

SURVEILLANCE AND CONTROL IN THE AGE OF INFORMATION:
A CRITICAL ANALYSIS OF THE TECHNOLOGY-POWER
RELATIONSHIP

A THESIS SUBMITTED TO THE
GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

EVREN KURT

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
IN THE DEPARTMENT OF
SCIENCE AND TECHNOLOGY POLICY STUDIES

FEBRUARY 2010

Approval of the Graduate School of Social Sciences

Prof. Dr. Sencer Ayata
Director

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

Assoc. 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.

Ins. Dr. Barış Çakmur
Supervisor

Examining Committee Members

Assoc. Prof. Dr. Erkan Erdil (METU, ECON) _____

Ins. Dr. Barış Çakmur (METU, ADM) _____

Assoc. Prof. Dr. Teoman Pamukçu (METU, STPS) _____

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.

Name, Last Name : Evren Kurt

Signature :

ABSTRACT

SURVEILLANCE AND CONTROL IN THE AGE OF INFORMATION: A CRITICAL ANALYSIS OF THE TECHNOLOGY-POWER RELATIONSHIP

Kurt, Evren

M. Sc., Department of Science and Technology Policy Studies

Supervisor: Ins. Dr. Barış akmur

February 2010, 155 pages

This study deals with the notions and practices of surveillance and control in the current society. By this means, it aims to discuss the relation between technology and power on basis of surveillance technologies witnessed in all domains of life. With the extensive use of new technologies as camera monitoring, biometrics, and smart cards, power holders get the opportunity and tools to monitor all actions and data of individuals. How this is achieved and for what purposes and the ideology behind the surveillance practices are the main issues of this study. In accordance with this goal, the use of surveillance technologies as a tool of power to provide rationalization in which everything

is visible, predictable, and controllable, to maintain social control, and to ensure the domination of power over the society is discussed through examining the applications of surveillance in Turkey and in other countries. Besides, the becoming of surveillance and control as natural and usual aspects of the current society in the eyes of people and their becoming a culture are also pointed out and analyzed in order to comprehend the location of these notions in everyday life. All these issues are discussed critically in order to analyze the role and ideological function of surveillance, in particular, and the relation of technology with power, in general.

Keywords: Surveillance, Society of Control, New Technologies, Power

ÖZ

ENFORMASYON ÇAĞINDA GÖZETİM VE DENETİM: TEKNOLOJİ-İKTİDAR İLİŞKİSİNİN ELEŞTİREL BİR ANALİZİ

Kurt, Evren

Yüksek Lisans, Bilim ve Teknoloji Politikası Çalışmaları Bölümü

Tez Yöneticisi: Öğr. Gör. Dr. Barış Çakmur

Şubat 2010, 155 sayfa

Bu çalışma, günümüz toplumunda gözetim ve denetim kavramlarını ve uygulamalarını ele alıyor. Bu sayede, yaşamın her alanında karşılaşılan gözetim teknolojileri temelinde teknoloji ve iktidar arasındaki ilişkiyi tartışmayı amaçlamaktadır. Kameralar, biyometri ve akıllı kartlar gibi yeni teknolojilerin kapsamlı kullanımı ile iktidar sahipleri bireylerin tüm eylemlerini ve verilerini izleme imkanına ve araçlarına sahip oluyorlar. Bunun nasıl ve hangi amaçlar için sağlandığı ve gözetim uygulamalarının ardındaki ideoloji bu çalışmanın temel konularıdır. Bu amaç doğrultusunda, her şeyin görülebilir, önceden kestirilebilir ve denetlenebilir olduğu bir rasyonelleşme sağlamak için, toplumsal denetim oluşturmak için ve iktidarın toplum üzerindeki hakimiyetini temin etmek için gözetim teknolojilerinin iktidarın bir aracı olarak

kullanılması, Türkiye ve diğer ülkelerdeki gözetim uygulamaları incelenerek tartışılmaktadır. Ayrıca, gözetim ve denetimin insanların gözünde günümüz toplumunun doğal ve olağan unsurları olmaları ve bir kültür haline gelmeleri, bu unsurların günlük yaşamdaki konumunu kavramak için ele alınıyor ve inceleniyor. Tüm bu konular, özelde gözetimin rolü ve ideolojik işlevini ve genelde teknolojinin iktidar ile ilişkisini incelemek üzere eleştirel bir açıdan tartışılmaktadır.

Anahtar Kelimeler: Gözetim, Denetim Toplumu, Yeni Teknolojiler, İktidar

To My Family,

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my supervisor, Ins. Dr. Barış Çakmur, for his invaluable guidance throughout this study. His advices, comments, and criticisms not only were helpful in the formation of the study and in the determination of the discussion points, but also caused me to think more creatively and critically.

Lots of words are not enough to express my indebtedness to my family. I am grateful to my mother and my father for their endless love throughout my life. Besides, my sister, Emel, and my brother, Emre, are two other persons who deserve special thanks for their encouragement and friendship.

Finally, I also wish to express my thanks to my friends for their moral support and useful advices during my studies.

TABLE OF CONTENTS

PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	vi
DEDICATION.....	viii
ACKNOWLEDGMENTS.....	ix
TABLE OF CONTENTS.....	x
CHAPTER	
1. INTRODUCTION	1
2. LOCATING SURVEILLANCE AND CONTROL IN THE CURRENT SOCIETY.....	11
2.1. Control through Surveillance.....	15
2.2. The Technologization of Surveillance.....	22
3. SURVEILLANCE UNDER THE NAME OF SECURITY.....	29
3.1. Public Safety and Policing.....	30

3.2. Visual Surveillance: An All-Seeing Eye.....	32
3.2.1. Workplace Monitoring.....	36
3.2.2. Street-Based Surveillance and MOBESE in Turkey.....	40
3.3. Surveillance through Biometrics.....	52
4. SURVEILLANCE AND CONTROL THROUGH PERSONAL DATA.....	59
4.1. Employee and Student Smart Cards.....	65
4.2. Consumer Surveillance: The Analysis of Loyalty Cards in Turkey.....	69
4.2.1. The Features and Functioning of Loyalty Cards: How Data are Collected and Used.....	78
4.2.2. Manipulation of Consumers.....	86
4.3. The Commodification of Personal Data.....	92
5. SURVEILLANCE AND CONTROL AS A CULTURE.....	98
5.1. Structures Promoting Surveillance and Control: Life Continuously Under Gaze.....	101
5.2. Surveillance in Popular Culture.....	107
5.3. Power and the Ideological Functioning of Surveillance and Control.....	114

5.4. Resistance to Surveillance.....	121
6. CONCLUSION	126
REFERENCES.....	137
APPENDICES	
A. FIGURES ABOUT VISUAL SURVEILLANCE AND SURVEILLANCE THROUGH BIOMETRICS.....	143
B. FIGURES ABOUT LOYALTY CARDS IN TURKEY.....	150

CHAPTER 1

INTRODUCTION

This study aims to examine the relation between technology and power in the contemporary society. In doing this, rather than a broader and open-ended discussion, I am going to analyze surveillance and control and their technologies which have been witnessed and discussed since the early twentieth century and, more extensively, since the development and widespread use of information and communication technologies (ICT) in the last decades.

My goal is to deal with the concepts of surveillance and control and their practices in the human life and in the social life in order to discuss technology and the ideology behind it. How surveillance practices are performed by power holders for what purposes is the principal question of this study. Why power holders intend to monitor all acts, actions, behaviors, and data of people in all aspects of life and how and why they aim to maintain continuous control over individuals and over the society are attempted to be answered through analyzing examples of surveillance practices carried out in Turkey and in other countries.

Before going into the deep analysis of surveillance and control and the relation between technology and power in this context, it is necessary and

useful to discuss technology and also the background of technology-society and technology-power relations. Thus, here, first of all, I am going to take into account the word “technology”, different theoretical perspectives to its role and function in the social and political arena, and the place of control in the discussion of technology. In addition to the discussion of technology in a theoretical manner, economic and social developments regarding technology throughout the twentieth century are also going to be mentioned afterwards. A short and particular history of this century is going to be presented subsequently through mentioning the notions and practices of Fordism, post-Fordism, and the information society.

Although technological tools, inventions and developments are almost as old as the history of mankind, the word technology does not have such a long history. Even primitive human beings used several tools and methods to survive. However, those technical equipments were devoid of science. This deficiency started to be removed with the emergence of science in ancient Greek. Likewise, the word “techne”, accepted as the root of technology, went back to the ancient Greek civilization. The word “technique” is also used, today, instead of it with similar meaning. It refers to specific tools, skills, and methods developed and used by human beings.

Technology, as we understand today, on the other hand, owed much to applied science beginning from the nineteenth century, rather than pure science of the past. Important scientific developments, such as electronics, have changed the structure and functioning of technology. Accordingly, technology has had a great role in the change and development of such as production, transportation, and communication. Technology, which was witnessed together with the Industrial Revolution, was different from its previous definitions. It has a broader meaning than that of technique. It can be defined as art, thinking and system of technique, developed by human beings. Similar to technique, it

is not a concept peculiar to the nature; that is to say, it is not an inherent component of nature. On the contrary, it was and is created and developed by human beings in order to survive in the nature and to control the nature; in short, it is a human creation.

Since the Industrial Revolution, the term technology has appeared in our social, economical and cultural life not only theoretically but also practically. It is obvious that technical developments have bettered our lives. That more comfortable houses have been built, that distances between locations have been shortened via car, trains and airplanes, and that people in different places have got into touch via mobile phones and the Internet are some examples of technological developments. However, the deterioration of the balance of nature through the hands of human beings via destructive applications of technologies is the other side of the coin, but it is not the issue of this study. Both human lives and social life have fed from technological developments positively and negatively; positively because our lives have been bettered through houses, cars, and several equipments, and negatively because technologies have resulted in unemployment and helplessness of people against huge technological developments. Here, the critical question is that who determines the direction of technological changes and that whether technology is free of external control.

There are several thinkers who discuss technology and its relation with society, economics, culture and politics from different perspectives. One sees technology as an independent actor determining all other fields of life while the other considers it as only a tool in the economic and social development. As pointed out by Mesthene (1971) while one sees it as “the motor of all progress” solving all problems in the social life and liberating the individual from any boundary, the other defines it as autonomous and uncontrollable, “robbing people for their jobs, their privacy, their participation in democratic

government and even, in the end, of their dignity as human beings” (Mesthene, 1971: 17).

In the study of technology, technological determinism is the item which has been mostly discussed. Technological determinism is an approach considering technology as an independent power, which determines social, economic and cultural life by itself. According to this, without any external control or social/cultural/political/economic determinant, technology itself is the driving force of change shaping the way of life in the society and the direction of society. As declared by Murphie and Potts (2003: 12),

“technological determinism tends to consider technology as an independent factor, with its own properties, its own course of development and its own consequences. Technological change is treated as if autonomous: removed from social pressures, it follows a logic or imperative of its own”.

At this point, it is necessary to declare that the studies taking technology into account as the motor of all change in the society are not analyzed by scholars under a single title called as technological determination. Some scholars make a distinction between theories of technology which regard technology as an autonomous force and those in which technological determination is the approach in the explanation of technology-society relationship. The approaches of autonomous technology and technological determinism are similar in seeing technology as the driving force of social change.

Street (1992: 23), for example, defines autonomous technology as that it “... claims technology acquires an independent momentum, which not only puts it beyond human control but also allows it to order all human activity, including politics”. Autonomous technology and technological determinism

both regard technology as the motor of all change; however, they have different perspectives in explaining the process of this determination. The latter differs from the former in that it

“...makes no particular claims about the ideological rationale provided by technology or about the extent of its impact. It does, however, contend that technology sets the conditions for the operation of the political system, including the political agenda, even if it does not determine the policy output” (Street, 1992: 30).

While considering suggestions of these approaches, it can be clearly declared that, in both theories, there is determinism in explaining the economic and social development without reference to society and social dynamics.

In this context, Feenberg (1991) makes another classification of theories of technology. He classifies theories of technology under three concepts: instrumental theory of technology, substantive theory of technology and critical theory of technology. He mentions the first two theories as two established theories of technology in which technological determinism is seen and technology is regarded as our destiny. In addition to and different from them, he explains the critical theory of technology as the third approach.

The instrumental theory treats technology as a means in the service of its users. Here, technology is defined as neutral; that is to say, technology, as pointed out by Feenberg (1991:5-6),

“...(1) is indifferent to the variety of ends it can be employed to achieve ...(2) is indifferent with respect to politics ...(3) embodies the universality of the truth ... hence, what works in one society can be expected to work just as well in another ...(4) stands essentially under the same norm of efficiency in any and every context”.

One example of instrumental theory is of Bell (1976). Bell describes the history of society on the basis of technological developments. He discusses three different periods of society: these are pre-industrial society, industrial society and post-industrial society. He employs agriculture in the analysis of pre-industrial societies as the defining factor of society; likewise, manufacture industry and factories in the analysis of industrial societies and service sector and information in the analysis of post-industrial societies. Like the neutrality feature of instrumental theory, “Bell necessarily contends that all societies are set on the same developmental journey” (Webster, 2006: 46). Technical and social progress, according to this view, follows a unilinear and fixed form of development.

Another scholar setting technology at the core point in the analysis of society is Castells (2000). While studying on the Information Age and the Network Society, he declares that “...without information technology, the Network Society would not exist” (Castells, 2000: 5). According to him, the acquisition and use of technology or the lack of it give chance or obstacle to societies to transform themselves. Through this approach, the extensive use of ICTs shapes one society’s becoming a Network Society.

The second theory of technology, for Feenberg, is the substantive theory. This theory, Feenberg (1991: 5) mentions,

“...attributes an autonomous cultural force to technology that overrides all traditional and competing values ... [It] claims that what very employment of technology does to humanity and nature is more consequential than its ostensible goals”.

What gives this theory the substantive impact is the claim of this theory that “technology is not simply a means but has become an environment and a way of life” (Feenberg, 1991: 8).

According to substantive theory, technology, as an autonomous factor, is a driving force in the development of societies regardless of existing political ideologies. Technological developments create a new social structure which has its own values different from the past. Ellul (1964), a substantive theorist, calls this society as technological society. Ellul uses the term technique in his writings and declares that “technique has become autonomous” and has become a “reality in itself” independent from any value and control.

Instrumental and substantive theories assert that we cannot shape or change the direction and development of technology. In both theories, therefore, technology is considered as destiny.

As for the third theory of technology, the critical theory, unlike instrumentalism, rejects the neutrality of technology since technology has a political role in the society. Technology, in the hands of power, has an ideological function in the maintenance of domination over the society. Like the fact that Critical Theory attacks the forms of rationality of capitalism, Feenberg’s theory, while rejecting neutrality, argues Marcuse’s (2002: xlvii) remark that “technological rationality has become political rationality”. According to him, technological rationality no longer merely exists in the field of machines and production, but also and more notably in the society through providing a visible, calculable, and predictable environment via new technologies. This helps power holders to provide domination over the society and to ensure their hegemony and dominant ideology.

Furthermore, critical theory of technology also opposes the fatalism of substantive theory through opposing the thought of technology’s becoming a way of life and a “reality in itself”. Likewise, it rejects the idea of autonomous technology of substantive theory. Technology, rather, is not an autonomous power, in its own, that determines the path of development and change in the society independent of any factor. Its dependence is on political structure,

culture, and society, in short, on human action. The change, direction and choice of society can be affected by human action rather than a single and autonomous variable, namely, technology.

In addition to remarks mentioned so far, it is the fact that when we are talking about technology, the word “control”, inevitably, has come into consideration. A clear statement about control is done by Bassett (2007: 85): “Control is ... never an unintended side effect of technology ... [T]echnology itself is all about control”. Several technologies were developed and used in the struggle against nature. Technology was used by human beings, one of the weakest living beings on the earth, as the primary means to survive and to control the nature.

Although this feature of technology, the control over nature, is still important, it is not the sole dimension of control. Throughout the history of humankind, the practice of control has not weakened, but varied and become not limited with nature. Today, we witness control in all domains of life. Control over workers and employees in the workplace, over children in the family, over students in the school, and eventually over all people in the everyday life are some forms of control in the current society, which are analyzed and discussed throughout the thesis. The principal tool of providing such forms of control over individuals and over the society is monitoring activities.

Within this framework, this study, in the following chapters, is going to deal with the practice of surveillance and control in order to point out and discuss the ideological functioning of technology for the sake and will of power. Throughout the study, examples of surveillance practices such as closed-circuit television (CCTV) monitoring, biometrics, the Internet, smart cards and chip technology, used by state agencies, private corporations and even by families and schools, are going to be analyzed to point out how

surveillance and control become ordinary and natural notions of our daily lives, how they become a culture, and how they serve to power in providing a rationality and in ensuring the domination of power over the society.

In the next chapter, I am going to take into account the theory and practice of surveillance in detail. Fordism and post-Fordism are one of the points of this chapter due to their close relation with surveillance and control. This chapter aims to characterize surveillance through dealing with its previous forms, its theoretical framework, and its technologization process. Not only historical, but also theoretical framework is going to be drawn in order to locate surveillance and control, and, thus, technology, in the contemporary society.

In chapter three, there is an analysis of surveillance and control in their fulfillment of the crime and risk prevention. In doing this, I am going to analyze visual surveillance and biometrics performed in the name of security. State agencies and corporations employ monitoring devices as CCTV systems to track acts and behaviors of workers, employees, and ordinary citizens. In addition to workplace monitoring, I am also going to take into account street-based surveillance. At this point, MOBESE system in Turkey, the system of street surveillance cameras is the particular issue of this study.

Beside the surveillance and control in the name of security, that in the name of efficiency and consumer satisfaction is the matter of the subsequent chapter, the fourth chapter. The particular subject of this chapter is the smart cards used by employees in their workplaces and students in their schools and is the specific form of smart cards, the loyalty cards of companies, used by consumers in their shopping. Through using these cards, data of card users are collected, stored, processed, used for capitalist targets. How this process is done and how the manipulation of consumers is achieved are the questions of

this chapter. The structure and functioning of smart cards in Turkey is going to be exemplified through several instances.

Chapter five is basically a discussion chapter on the basis of the issues analyzed in the third and fourth chapters. How surveillance and control become embedded notions of the human life and the social life, how they become unchallengeable aspects of everyday life, and how they serve to power ideologically are the main points of the discussion. Human beings are under constant surveillance and control by parents, teachers, managers, state agencies, and private corporations. This case starts in the childhood and continues during the whole life. Within this framework and through considering surveillance practices mentioned until this chapter, how surveillance and control become a culture is aimed to be answered here. Besides, surveillance and control and their implementations, analyzed throughout the study, are going to be discussed in order to point out the ideology behind them. How they are used by power and for what purposes are within the discussion. Another issue of this chapter is the resistance to surveillance. Social movement groups, internet-based organizations, and related associations, for instance, question and challenge the widespread and intensive functioning of surveillance; besides, they also inform people about privacy-eroding feature of surveillance practices.

Finally, in the conclusion, I am going to try to point out the direction of the change of the current society concerning the issues of surveillance and control. What kind of a social structure the surveillance-and-control society is transformed into and whether we are moving toward a totally-administered and -controlled society are going to be emphasized. Furthermore, what is to be done to strengthen the privacy of people and to eliminate the helplessness of them against the all-seeing and all-knowing eye of power is needed to be dealt with.

CHAPTER 2

LOCATING SURVEILLANCE AND CONTROL IN THE CURRENT SOCIETY

Control over nature had been the primary form of control achieved through using technology until the twentieth century. In addition to nature, the individual became the subject of control and, thus, of monitoring together with the technological developments and with the changes in the production field in this period. Workers in factories in the early twentieth century were the initial example of control through technology. Control over workers was explicitly witnessed with the applications of Fordism and Taylorist Scientific Management in the workplace.

Fordism was based on the assembly line in which every single worker had a very simple and specific duty in the production. Workers did not have any knowledge about and effect on the whole production process; however, they only dealt with particular part of production. Standard goods were produced through standard methods and processes by standard tasks of workers. Fordism was ruled according to Taylorist principles.

The aim of Taylorism was declared as to increase the efficiency and to eliminate the idle of workers. Time, at this point, was the notable point in

Taylorism and in the Fordist mode of production. The production process and the tasks of workers had to be finished at a given period; this pre-determined time-labor scale was expected to increase efficiency. Therefore, in order to maintain this, there was a strict control over workers followed by managers. Managers, by means of these Fordist-Taylorist principles, aimed workers and their actions and behaviors to be visible, calculable, and controllable. Therefore, these principles helped managers to provide a rationality in which there was nothing unpredictable under their authority.

Similarly and additionally, Fraser (2003), according to whom, Fordism was not simply a matter of economics, sees it as a governmentality embodied a distinctive political rationality which is widely diffused throughout the society “on the capillary level”, such as in factories, hospitals, prisons, and schools. She discusses the characteristics of this Fordist governmentality similar to that Foucault’s (1977) disciplinary society. Fordism, as mentioned by Fraser (2003: 163-4), has three defining features like that of Foucauldian discipline:

“...(1) Fordist discipline was totalizing, aimed at rationalizing all major aspects of social life ...(2) It was socially concentrated within a national frame ...(3) This mode of social ordering worked largely through individual self regulation”.

Workers were expected to regulate their acts and behaviors or, say, to control themselves in accordance with the rules of managers. This self-control case, not limited with workers, is also largely seen in Foucault, which is going to be discussed in the next chapter.

Transition from Fordism to post-Fordism has underlain today’s information-based societies. In the post-Fordist mode of production, there are differentiated products and flexible specialization, rather than standardization of Fordism. While Fordism regarded the worker as the part of the machine,

post-Fordism gives much more emphasis to the ability and knowledge of worker. Besides, service sector and white-collar workers have become important in economics in addition to manufacture industry and blue-collars. Market no longer only deals with production, but also consumption through advertisements. Another development is the globalization; there are transnational corporations, which are very strong economically and technologically as states and are very influential in the national and world market. The major item related with these changes is information. The acquisition and use of information, namely, ICTs, have become significant in this period both for institutional structures, as states and firms, and for individuals themselves. In addition to concept of post-Fordism, Bell (1976), for instance, calls this new society as post-industrial society in which the central role is given to information. Most scholars, such as Webster (2006), define it as the information society, which I will use throughout this study.

As for our main issue, the practice of control is also seen but extensively and systematically in the information society. The advance of control did not stop with the control over nature and the control over workers. In the information society, the whole society has become the subject of control and its inseparable partner, surveillance. “The power of technical control over nature ... is extended today directly to society” (Habermas, 1971: 56). What happens in the information society different from the past is the increase of control and surveillance via new technologies. Control is no longer limited with the aim of providing domination over nature and over workers. Surveillance and control are not limited within the boundaries of the labor process but diffuse to all aspects of life. Therefore, Lyon (2001) sees information societies as also surveillance societies. Here, all people in the society are potentially subject to surveillance. While there were discipline and correction through confinement in Foucault and in Fordism, surveillance

societies in the post-Fordist period deals with continuous control without confinement through tracking people in all fields of life.

This process is not performed by a single entity as the nation-state or the managers unlike the case of Fordist mode of production, but by several entities, such as states, small or large corporations, transnational firms, professional associations and even private households. In the current society, “rather than being concentrated in the hands of a few, disciplinary power appears nearly everywhere, dispersed, and fragmented” (Staples, 2000: 26). The dispersion of surveillance and control to every individual and to every field of life is achieved by means of information and communication technologies as computers, mobile phones, closed-circuit TV (CCTV) cameras, smart cards, satellites, GPS-based locational technologies, and the Internet. Thus, Marcuse (2002) is right in considering technology as a form of social control and domination. In order to strengthen their hegemony over the society and to maintain rationality in which everything/everyone is visible and controllable, power holders need to track individuals under the names of crime/risk prevention and efficiency.

This issue helps power to maintain rationality, which is one of the significant issues discussed in this study. As known, rationalization is not based on concepts as tradition, but on efficiency, predictability, calculation, and control in order to reach specified goals. It was and also is a principal aim of power in order to ensure domination over the society and to strengthen its authority vis-à-vis the civil society. Weber, who saw bureaucracy as the example of rationalization, considered rationality as the character of modern society. He considered the increasing role of predictability and control, which led to what he called the “iron cage” of bureaucracy, as the principal elements of rationalization. Besides, he “...regarded surveillance as a necessary accompaniment to the increased rationalization of the world” (Ball and

Webster, 2003: 11) where people are in the “iron cage” of laws, rules, and regulations.

The leading tool of rationalization, that is, of achieving predictability and control, is the tracking of such as workers and employees in the workplace, students in schools, consumers in shopping, users of the Internet and, comprehensively, all individuals in the society. Feenberg (1995: 11) states that “rationalization is our modern horizon¹, and technological design is the key to its effectiveness as the basis of modern hegemonies”. Here, technological design in this context comprises surveillance and its related technologies and practices which serve to ensure hegemonies of such as states and corporations. The authority still intends to keep people under control not merely through bureaucratization and rules and laws accompanying it, but through technological tools. Although means have changed, rationalization is still the main character of contemporary life. Thus, surveillance practices have been given much importance in order to reach a predictable and controllable environment.

2.1 CONTROL THROUGH SURVEILLANCE

From now on, upon this basis, I am going to point out and discuss surveillance and control, in detail, in the contemporary society. In today's world, state agencies and private corporations have the capacity to track

¹ This term “...refers to culturally general assumptions that form the unquestioned background to every aspect of life” (Feenberg, 1995: 10).

individuals and to record their personal data through ICTs, more concretely, through surveillance and control technologies, such as CCTV monitoring, biometrics, chip-embedded smart cards, and also the Internet. The monitoring of individuals is not a new phenomenon although it is considered together with the development information and communication technologies in the late twentieth and in the twenty-first centuries.

One of the earliest forms of watching was the neighborhood gaze in order to be sure whether neighbors are good people or they are harmful to the environment and to the common life. It was, and also is, necessary for the security of the community. In addition to such attempts for the safety of the social life, there was also the gaze of people in order to maintain and strengthen social order. In this case, people watched and controlled -as also seen in the current society- themselves and others in order to make everyone obey the rules, traditions, and customs.

Previously, the state agencies kept several records of individuals, and also the private companies did. For example, in addition to surveillance and control over workers, the voting lists, the tax files, and medical records of citizens were written down by related state officials. Besides, the employee numbers and their information were also recorded by both state agencies and private companies.

The turning point of keeping records of individuals was the computerization in the late twentieth century. The computerization of surveillance has given more capacity and power to monitor people. Before the computerization and digitization of surveillance and control, the monitoring and control activity were realized through face-to-face control. Besides, wiretapping, eavesdropping devices and other techniques of monitoring were used by espionage agents of the states throughout the history. Whether declared or not, the main aim was to prevent risks and to provide social order.

Although keeping records of citizens was largely witnessed in the nation states in the nineteenth and twentieth centuries, it is not peculiar to that period. For example, “recorded counts of population for conscription or for taxation occurred in ancient societies such as the Roman Empire” (Lyon, 2007: 30) in order to get and store information about people. By this way, people were categorized according to their wealth, education, social status, and other dimensions.

As for nation states, in addition to such measures of sorting of people, the census, registration of births and deaths, taxation records, voting lists, and data of criminals have been the forms of systematic surveillance over the society. As for the working life, monitoring for capitalist endeavors was such as recording workers and employees, and their wages and performances. Surveillance as we understand it today emerged with the nation states, modern bureaucracies, and the capitalist enterprises. On the other hand, the measures of surveillance and control in today’s world have become technological and computerized, and their use has gone beyond the abovementioned means.

What is different today from the surveillance in the previous times is the widespread use of technologies and the systematic and institutional structure and functioning of surveillance. Not only in the past but also in today’s world, security and social order are the initial goals of the states. Power always needs to know every event and to get information about every potential threat in the society. Otherwise, it is thought that struggle against risks and uncertainties would be impossible. In order to eliminate uncertainty and spontaneity and to be ready against potential threats, power needs an all-seeing and all knowing eye. This role is performed by surveillance and control technologies through providing a rationality which forms a visible, predictable, and controllable environment.

While a broad definition of surveillance is the close observation of a person or a group of persons, it does not meet the structure and features of surveillance in today's world. Lyon (2001: 2) defines surveillance as "...any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered". Surveillance, in this wise, involves the systematic monitoring of people in every field of life and the collection of data about all their actions and communications for the purpose of controlling and managing them by whether governmental agencies or private corporations in accordance with specified goals. These goals are the goals of capitalism, more broadly, of power, which work to cement people to the status quo and to enforce the domination of power over individuals and over the society.

The state has been the most influential figure and has had a considerable role in the practice of surveillance. States have used several measures to keep their citizens under gaze and control in order to strengthen its power and to maintain social order in the society. Other than ideological means as the media which are very influential in today's world, states, previously, mostly benefitted from the coercive functioning of state apparatuses as bureaucracy and/or army. These apparatuses of the state have surveilled and controlled the citizens according to the will of the state, of power, to ensure the hegemony and to augment domination of power over the society.

Such a case was taken into account by Orwell (1987) as a dystopia. In this regard, he portrayed, in his novel 1984, the most conspicuous picture in which total surveillance-and-control society was described. He narrated the state, the society, the individuals, and their relations in Oceania, one of three countries in the world. The State uses several watching and listening devices in order to keep people under its gaze and control. For example, there are eavesdropping devices hidden behind the pictures on the walls of people's

houses and hidden inside tree branches. There is also telescreen, a kind of a television, through which not only people watch and listen declarations of the State, of the so-called Big Brother, but also Big Brother watches every action of the person inside the house even if the telescreen is not open.

In Orwell's dystopia, a totalitarian state was described, in which all people are subject to coercive means of surveillance by Big Brother whether inside or outside their houses and have no chance to question and challenge the structure and functioning of power and of these measures. While considering the practice of surveillance described by Orwell, it can be claimed that today's society surrounded by new technologies goes beyond Orwell's dystopia in that current power holders have more opportunities and a lot of technologies, such as cameras, biometrics, smart cards, mobile phones, and satellites, to monitor people in all spheres of life.

Other than the abovementioned issues, the turning point in the discussion of surveillance and control is the Panopticon, the architecture of prison designed by Bentham (1995). In his design, the building is circular. The apartments of the prisoners, called as "the cells", are divided from each other; prisoners are deprived of communication among each other. There is an inspector, the guard, at the center of the architecture; the apartment of the inspector, called as "the inspector's lodge", is located in such a way that the inspector sees all prisoners and never turns back to any prisoner. Prisoners, on the contrary, although see the central inspection tower, cannot see the inspector and cannot know whether the eye of the inspector is on them at any given time. This "the see-being seen dyad" (Foucault, 1977) is an important point of the Panopticon in that "...the person to be inspected should always feel themselves as if under inspection" (Bentham, 1995: 43). Accordingly, Bentham's aim "...was to show how the exercise of power within the confines of the prison

system could be rationalized, with the intention of improving the reformation of the posited deviant natures of the inmates” (Innes, 2003: 115).

This “seeing-never being seen” feature of the Panopticon is significant because it leads to the fact that people under surveillance have to control and adjust their actions and behaviors under the constant gaze. The major effect of the Panopticon, thus, is “...to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power” (Foucault, 1977: 201). Foucault, who saw the Panopticon as a figure of political technology, applied the monitoring and disciplinary mechanism of the Panopticon to the general functioning of social life, to the society. In other words, “what for Bentham was a dream, for Foucault is the social reality par excellence of modernity” (Lyon, 2006b: 24).

According to him, the school, the family, and the workhouse, like the prison, are the institutions which aim and attempt to surveil and control their inhabitants, in accordance with the will of them, more concretely, of power, through enclosure and discipline (Foucault, 1977). The confinement is the critical feature of the Panopticon, thus, of the disciplinary societies. The main aim is to maintain social order and to reinforce the domination of power through disciplinary mechanisms as confinement and through controlling people and making them control themselves.

While Foucault presented a social reality, Orwell narrated a dystopia in which a totalitarian state, the Big Brother, monitored, controlled, and manipulated actions and even thoughts of people. Thus, “whereas Orwell’s vision could be viewed as a ‘possible but preventable future’ ... Foucault’s Panopticon often appears as imminent and inevitable” (Lyon, 1994: 204). This is because the institutions discussed by Foucault in the case of the Panopticon do not function in the same manner as in the case of the Big Brother in Orwell. While there is no chance of challenge in Orwell’s dystopia due to coercive

institutions as army and police, there is the chance of objection but also paranoia due to the comprehensive existence and functioning of surveillance practices in all fields of life.

On the other hand, disciplinary societies and the sites of confinement of Foucault were no longer the case of the twentieth century. The most influential criticism to disciplinary societies came from Deleuze (1992), according to whom, control societies are taking over from disciplinary societies. He asserts that “we are definitely moving toward control societies that are no longer exactly disciplinary no longer operate by confining people but through continuous control and instant communication” (Deleuze, 1990: 174). Paranoia of being constantly monitored has much been instilled into the conscious of people because there is no longer confinement to train individuals, but all-seeing eyes everywhere to surveil and control them continuously.

Confinement has no longer been the leading means of the institutions since late the twentieth century, since the development and extensive use of information and communication technologies. Rather than centralized disciplinary mechanisms which train individuals in order to create good -that is, good for the will of power- students, workers, and, finally, loyal and docile citizens, control societies have performed several forms of “free-floating control” (Deleuze, 1992) in all aspects of life in accordance with the same goal. For example, the education is not limited with the school-term period of children but expands to every level of human life; the media, for instance, are the area in which people are continuously being educated or, say, influenced and even manipulated through presenting standardized opinions and standardized forms of lifestyles.

2.2 THE TECHNOLOGIZATION OF SURVEILLANCE

In the twentieth and mostly in the twenty-first centuries, a major technological development has occurred, namely, information and communication technologies. The effect of them is not limited with the production field, not with the structure and functioning of manufacture. Today, computers, telecommunications such as mobile phones, satellites, and chip technology largely affect state agencies, private corporations, households, in short, our everyday lives. These technologies have permeated into our lives in such a manner that people do not envisage a life without technologies they use regularly and that they think they cannot live without such as their mobile phones and personal computers.

While technological developments have led to new opportunities for individuals and for the society through improving the conditions of human life and through improving the services provided by state and private agencies, they, on the other hand, have resulted in new problems such as the erosion of privacy. Both governmental agencies and private corporations, local or global, have got new opportunities to monitor people everywhere, while at work, speaking on the phone, using the Internet, shopping, and so on. By this way, individuals have faced with several applications through which authorities surveil them and their actions, even though concerning their privacy.

The first effect of the technologization of surveillance was witnessed in the workplace together with the introduction of computers. Computers and other forms of techniques such as door-opening and building-entering smart cards and CCTV cameras within the workplace have become inspectors, rather than solely a manager of Taylorism, in the gaze and control of employees. Other than Taylorist scientific management, technological management, based

on surveillance, has become the main character of today's capitalist enterprises (Lyon, 2004b: 165). Surveillance of workers is much more intensive with the technological means than that of the past. While "surveillance transcends traditional Taylorism" (Lyon, 1994: 126), it has become an important control mechanism of capitalism in the workplace. Briefly, the introduction and permeation of new technologies into the workplace extends managerial control and also the domination of power over workers and employees.

Due to such technological developments not only in the workplace but, more significantly, in all spheres of life, we have moved from physical surveillance toward electronic surveillance. By this way, not only certain people are tracked for specific purposes, but also even ordinary citizens are tracked in order to provide a rational social order in which everything is visible, predictable, and controllable and, thus, to provide domination over the society. This means new technologies are the accelerator and intensifier of surveillance.

Furthermore, beyond electronic surveillance, there occurs data surveillance. Clarke (1988) was the first defining this as "dataveillance", which differs from physical and electronic surveillance in that it deals with the monitoring of data of individuals. The governmental agencies and the capitalist business enterprises intend to achieve data of people because "risk assessment, prediction, prevention, and rational planning require personal information" (Marx, 2002: 18). Information and communication technologies give state and private agencies the opportunity of collecting, storing, and analyzing data of people. For example, as going to be largely analyzed in the following chapters, while surveillance cameras in the stores, airports, malls, and even streets are watching individuals physically, loyalty cards of supermarkets are monitoring their very personal information as names, addresses, incomes, purchases, choices, needs and, thus, their consumption and living patterns.

Through referring new technologies in the practice of surveillance, Gary Marx (2005) points out the notion of “the new surveillance” in the contemporary society, which has different features than the previous surveillance practices. “The new surveillance transcends distance, darkness, and physical barriers” (Marx, 2005: 769). Surveillance technologies no longer work in just a particular place for a specified period of time. On the contrary, cameras, mobile phones, the Internet, and smart cards, for instance, track people and their personal data anywhere and at any time.

Data of individuals are collected, stored, and retrieved through computers, and become reachable by private and public institutions at any time. In addition, the new surveillance “...has low visibility or is invisible. It becomes ever more difficult to ascertain when and whether we are being watched and who is doing the watching” (Marx, 2005: 770). On the other hand, although there are no captions saying “Big Brother is Watching You” as seen in Orwell’s dystopia, we know that there are surveillance devices somewhere in our lives watching us. Surveillance cameras functioning everywhere, credit cards used in shopping, biometric devices in the airports, the Internet, mobile phones, recording of phone conversations, the detection of one’s place via GPS technology or the IP address of the computer, etc. instill the feeling of being constantly watched everywhere into the conscious of people.

Although the new surveillance has a potential to function invisibly, such as chip technology, CCTV cameras are a visible tracking device. Authorities do not tend to perform monitoring completely invisible due to the fact that visibility leads to the self-regulation of individuals. Because surveillance and its technologies are with them or around them in all aspects of life and because they feel that they are potentially under gaze anywhere and anytime, individuals are expected to control and regulate themselves and to adjust their actions and. Rather than merely one’s controlling himself/herself,

such a self-control is a leading feature of the new surveillance. This form of control is also expected to result in the social control.

Moreover, the new surveillance

“...triggers a shift from targeting a specific suspect to categorical suspicion of everyone ... Between the camera, the tape recorder, the identity card, the metal detector, the tax form, and the computer, everyone becomes a reasonable target” (Marx, 2005: 771).

These and also other tracking devices as credit cards, loyalty cards of firms, chip technologies, mobile phones, locational technologies as GPS (Global Positioning System), and biometrics as face recognition systems are to surveil all individuals, not merely specific ones. Power considers everyone as a potential threat or risk in the contemporary society; thus, it aims to get more and more information about everything and everyone in the society.

Because all people are considered potential risks against the social order and against the dominant ideology, power holders intend to monitor them everywhere and every time in order to eliminate risks and uncertainties. In order to rationalize their affairs, states benefit from several measures such as surveillance cameras located in various points of cities, biometric devices as in airports or in official buildings, and smart cards used for building entrance or door opening in order to maintain rationality and to eliminate uncertainties in today's complex social structure. Together with the state's monitoring and controlling people, they surveil and control their own actions and behaviors due to “the fear of the Panopticon” (Foucault, 1977). That is to say, beside state surveillance over people, there is also self-surveillance and self-control pursued by people under the constant gaze over them.

In addition to this effort of the state, private enterprises also employ several surveillance devices in their businesses. Both tracking of employees mentioned previously and tracking of consumers are two targets of surveillance for capitalist endeavors. Corporations tend to monitor their customers for profit maximization and for the increase of their power. Here, they monitor expenditures of their customers; they collect, store, and process data of customers not merely for their specified commercial goals, but also for providing control and hegemony over individuals.

Measures used by them are surveillance cameras to watch customers, credit cards monitoring their overall purchases, and loyalty cards monitoring their detailed expenditures, the content of their shopping baskets. With these means, capitalism does not just monitor consumers and their personal data, but also influences, manipulates, and controls them and their actions, behaviors, choices, needs, and buying patterns through instilling them a standardized way of consumption and of living.

Both the government and the capitalist business enterprises serve to the same purposes and same end. Through benefitting largely from new technologies, they attempt to achieve rationality, to form social control, to provide domination over the society, to reinforce the hegemony of capitalism, of dominant ideology, and to form loyal customers and docile citizens for the well-being of existing social order and of power.

In accordance with these goals, two main discourses, security and efficiency, are used to legitimize the widespread existence and functioning of surveillance and control technologies in all fields of life. Whether in the public or private places, the existence of surveillance cameras and biometrics, for example, as a tool of power, conceals behind the discourse of security. Especially, after the terrorist attacks on September 11, the states have given much more significance to the security measures in order to fight against

crime. Not only the state buildings and airports, but also the shops, houses and even the streets are covered by surveillance measures, basically the CCTV cameras and recently the biometric-equipped cameras. By this way, the state has got the capacity to track every individual in the society and to avert potential threats and risks. The basic idea behind the surveillance and control technologies is to eliminate spontaneity and uncertainty and to maintain rationality. Power also needs obedient citizens in the formation of surveillance systems. This is done through putting forward the need of security against robbers, muggers, and terrorists. Therefore, people, largely, do not question and challenge these all-encompassing surveillance systems around us due to the need of security.

Likewise, institutions as schools, associations, and private corporations perform several mechanisms, such as smart cards and the Internet, to surveil, control, and manipulate the choices, actions, and behaviors of individuals under the name of efficiency and consumer satisfaction. Through using surveillance and control technologies, authorities can also track people, and collect and profile their personal data. By this means, they can get information about who the person actually is via biometrics, where he/she is at a given moment via CCTV cameras, and what his/her preferences and living patterns are via credit cards and smart cards.

The information about one's lifestyle is analyzed and used by state agencies to avert spontaneity and risks in social life and also by private companies for commercial purposes. The data of people can be collected, stored and analyzed whether in everyday life such as in supermarkets while they are shopping or in the Internet while they are just surfing. Databases can be formed according to individuals' profiles and used for persuasion and seduction of them in their shopping.

All these surveillance and control practices under the name of security or efficiency bring us the issue of achieving rationality and of providing domination over the society by the dominant ideology. In this context, in order to clarify the goals of power in the current society concerning surveillance, it is necessary to point out and analyze the practices of surveillance and control carried out by power holders, by whether state agencies or private corporations. After discussing surveillance under the name of security and public safety and mentioning the case in Turkey in the next chapter, dataveillance of consumers, employees, and students under the name of efficiency is going to be analyzed subsequently.

CHAPTER 3

SURVEILLANCE UNDER THE NAME OF SECURITY

Security is the mostly mentioned and the prominent discourse while considering the development of surveillance and control technologies. The nation states have carried out various technologies and practices under the name of providing more security to their citizens and to the society and of providing the security of their borders. This case is not a new phenomenon; the goal of security went back to earlier stages of nation states and also to the period of empires. Whether in the feudal period, in the empirical times or in the nation states, the power holders always had the attempt to maintain securer environments for the safety of people under their authority and, more considerably, for the well-being of the existing social order.

In the past, the security via military technologies and armed forces, namely, the police department for the social security and the army for the border security, were at stake in the discussion of the security discourse. In addition, there were also laws and regulations, having a deterrent character, regulating the social life, and maintaining the security against existing and potential criminals. In today's societies, only the armed forces and legislations that are the coercive means of power have become inadequate for the security and public safety in the eye of power holders.

Not only the state agencies, but also the private corporations have the tendency and apply policies to use several technologies, such as video recording technologies namely the CCTV (closed circuit television) systems, biometrics, and chip technology in accordance with the goal of security. The principal idea behind the use of such technologies is to detect crimes and criminals, to eliminate or at least reduce threats and uncertainties of the contemporary society and of the individual behavior, and to maintain a system where every potential threat to the existing order is predictable.

Before dealing with the functioning and the benefits of such technologies in the security discussions in detail and comprehensively, it is necessary to point out how and in what conditions we have moved from “risk society” (Beck, 1991) to “the law-and-order society” (Hall et al, 1978) in order to comprehend the character of contemporary society.

3.1 PUBLIC SAFETY AND POLICING

Maintenance of public safety through “reclaiming the streets” (Coleman, 2004) is seen as one of the prominent duties of states. The street reclamation can be pursued through eliminating such as the street robberies, mugging, rape, and vandalism. In short and more concretely, the elimination of the fear of crime is the precondition of the public safety. As discussed largely by Hall et al (1978), an increasing rate of crime inevitably leads to panic in the society; with the words of them, this is the “moral panic about mugging”.

In order to eradicate the panic about crime and the fear of being attacked in the streets, there has occurred “pre-emptive policing” (Hall et al, 1978) as a deterrent power, which works through observing the suspects in a particular place by officials and also by the private security. Besides, the individuals in the society, due to the fear of crime, are willing to the fulfillment of more practices and more extensive measures in the struggle against crimes and criminals.

This leads to the empowerment of state authorities and of their enactment capacity of harsher laws and policies. All of these, at the end, serve for the benefit of the existing system, for strengthening the power. In this context, rather than questioning and challenging the policies and regulations which actually constrain the human life under the name of security, people largely consider them useful and necessary.

It is the fact that “not only mugging, robbery and rape, but also the terrorist activities, political kidnappings and hijacking pave the way for the creation of the law-and-order society” (Hall et al, 1978: 300). Besides, it can be declared that moral panic about crime, which connotes fear and insecurity, has resulted in the creation of “law-and-order society”.

Beck (1992) emphasized that the aim of surveillance practices in such a society is not merely to prevent crime and danger, but more strategically to “avoid even conceivable risks”; here, every citizen is seen as a risk factor. Therefore, the surveillance practices and policing measures are or are aimed to be implemented over the public at large in order to be on alert against every potential threat to the social and political well-being. The law-and-order society and considering every individual as a potential risk have become globalized especially in the post-9/11 era. The terrorist attacks in the United States on September 11, 2001, comprehensively changed the states’ and the private corporations’ approaches not only to terrorism and to terrorist

organizations, but also and more profoundly to the issue of security and to the security measures concerning all individuals within a territory and also concerning the world.

This means that every individual all around the world is regarded as a potential threat to the security of states and to the public safety. Therefore, law-and-order measures are expanded to comprise the entire of countries and the whole world through cooperation of the states. In this issue, “the unknown and unintended consequences” (Beck, 1992) of the modern life are aimed and expected to be removed through tracking the individuals and through getting information about them via several practices of technologies. This is done under the name of security and of the struggle against terrorism through new technologies, which can be labeled as surveillance and control technologies, such as CCTV, biometric-based devices, smart cards with embedded chips.

3.2 VISUAL SURVEILLANCE: AN ALL-SEEING EYE

It is the fact that many people consider the surveillance through cameras, more concretely, the CCTV monitoring system, as useful and necessary in the fight against crime, violence and terrorism in the current society. Therefore, surveillance cameras have entered to our everyday lives, to every aspect of social life, without any comprehensive challenge or criticism. Today, everywhere around us is full of surveillance cameras functioning constantly and extensively.

The first CCTV system was established in 1942 by the Nazi Army in Germany in order to watch and control the process and to detect the technical faults of V2 rockets. In addition, the first CCTV camera system working in the public sphere and monitoring ordinary citizens was used in England with four security cameras during the parade of the Queen in 1956.² Furthermore, the CCTV cameras have been used in various types and in various purposes largely since 1960's. In 1961, video surveillance system was installed at a London Transport train station.³ Furthermore, in New York City, police cameras were installed at the Municipal Building in 1969.⁴ In addition, also in the 1970's and 1980's, they were largely used in, for example, in workplaces, in stations, in banks and in particular state buildings and also in stores afterwards, as a deterrent factor against crime and violence. Of course, the cameras and the monitoring practices of those times are not as technology-intensive as that of current times. These cameras worked in their own; that is to say; the video recording was not tied to other cameras, was not managed from a control room, or their records were not digitally collected, stored and processed.

With the great technological developments, basically, the developments of information and communication technologies, and with the aftermath of 9/11 events, the use of monitoring systems has become widespread all around world. Initially, the surveillance cameras have been used for the security of, for example, official buildings, airports, metro stations, stores, and malls; later, they have become a tool of surveillance over the individuals in the streets. Today, official and private areas are surrounded by surveillance cameras, some of which are equipped with biometric technologies, such as face recognition software. Streets of cities in various countries are monitored and recorded by

² <http://haber.gazetevatan.com/haberdetay.asp?exec=haberdetay&tarih=06.11.2006&Newsid=92233&Categoryid=7>

³ <http://www.notbored.org/england-history.html>

⁴ <http://www.notbored.org/nyc-history.html>

such cameras which are built in places where population density or crime rates are high in order to maintain public safety.

In this issue, new information and communication technologies have a big role and function to establish well-functioning monitoring systems. Gary Marx (2005) defined this as “the new surveillance” when compared with the previous surveillance practices, such as espionage agents and face-to-face control of criminals and suspects. “The new surveillance...has low visibility or is invisible” (Marx, 2005: 770) due to the fact that the human-effect in the monitoring practices has been lessened or removed. In comparison with other surveillance technologies, as biometrics or chip-embedded smart cards, CCTV is more visible. Thus, CCTV has a different character and structure.

This different character of the CCTV can be pointed out through referring Foucault’s statement “visibility is a trap” (Foucault, 1977). It is the fact that every individual can witness the existence and functioning of surveillance cameras whether in a mall or in an airport or even in a street. There occurs a feeling on individuals that a hidden eye behind the cameras is always looking at them and watching their actions. But they do not have any knowledge about when they are being watched. The cameras around them may record their activities at any time and there occurs a feeling of being surveilled constantly; thus, people feel themselves compulsory to control their actions and to adjust their behaviors in order to get rid of these all-seeing eyes.

Individuals’ tendency of controlling their activities is the result of the “fear of the Panopticon” (Foucault, 1977). A fear because people are subject to a constant gaze by an eye which is not seen by them, or, say, by an eye behind these cameras which is not seen. The surveillance technologies have the capacity to see without being seen, like the inspector of the Panopticon in the lodge. Hence, the feeling of being constantly monitored leads to the constant fear of being monitored at any time. Foucault gives importance to this

“seeing/being seen dyad” due to the fact that “it automatizes and disindividualizes power” (Foucault, 1977: 202). This automatic functioning of power has a considerable effect to reclaim prisoners in the prisons, to reclaim the robbers, muggers, and potential criminals in the streets, to supervise workers and employees, and to make every citizen in the society be docile under the domination of power, through using the surveillance-and-control capacity of cameras installed everywhere.

In short, it can be claimed that “CCTV is a general expression of power, a new technological tool of the disciplinary network designed to provide obedient citizens” (William and Webster, 1999: 125) Thus, everyone in the society, whether a criminal or an ordinary citizen, is expected to become subject to the all-seeing eye of the power, without any criticism or challenge. All-encompassing surveillance cameras have notable effects and function in the appearance of “docile bodies”, which are discussed by Foucault (1977) as the outcomes of the disciplinary societies. As mentioned above, self-control has occurred in relation to the constant gaze of power; therefore, “docile bodies” “under surveillance do not need to be regulated since they regulate themselves” (Koskela, 2003: 300) due to the fear of being watched at any time.

In order to deal with this abovementioned automatic functioning of power and people’s becoming passive surveillees and “docile bodies” is going to be understood more clearly after taking into account the particular fields and forms of surveillance. Out of today’s largely witnessed monitoring, surveillance cameras in malls, in workplaces and in the streets have come into consideration. Hence, these three items are going to be analyzed under the following headings.

3.2.1 WORKPLACE MONITORING

One basic example considered in the practice of visual surveillance is the CCTV cameras in the shopping malls. The malls are not only places of shopping, but they have also become the points of modern life, which means that they are also entertainment areas, meeting points, and community centers. A shopping mall is a place for shopping with various stores within it, for watching films in its cinema halls, for eating, and for wandering and spending time. Therefore, the corporations give much significance to the design and services of the mall. Such a big and comprehensive place of social life also needs security measures; and this is not ensured merely through employing security staff.

The malls in Turkey, for example, without any exemption, similar to that in other countries, are surrounded and protected by CCTV cameras, managed from a central control room. Unlike this similarity, the malls in Turkey and their monitoring activities are newly developed. The malls of developed European countries and of the United States are largely technology-intensive and even some of them have face recognition software embedded in the security-camera applications.

The cameras of the malls in Turkey are motionless and work without face recognition system. These surveillance cameras watch the individuals in the mall not only at the entrance, but also in several points of the mall. In brief, they are accepted as *sine qua non* of the modern malls. The cameras, which work and collect data continuously, are generally placed at the entrance, the intersection points and the crossroads of the malls. Their records are collected, stored and analyzed by the employees in the control room regularly.

The main reason of using these cameras is declared as the need of security; mainly, they are designed to fight against shoplifting, robbery, mugging and also other crimes. There is a goal to make the individuals feel themselves safe and secure. As mentioned by Helten and Fischer (2004: 332) in their work on video surveillance in Berlin malls, according to managers, “...the main objectives of the systems are to prevent crime (mostly theft and vandalism), to support prosecution and to guarantee the safety of the customers”.

In addition to the malls, CCTV surveillance is also and largely used inside the stores. These surveillance and control mechanisms should not only be seen as a measure against crime, but also as a managerial control over employees in the workplace. Workplace monitoring can be defined as the digitization of Taylorism; that is to say, there is not a manager as an inspector physically controlling employees in the workplace, but there is a digital eye, which is performed and directed by officials in a control room of the given corporation's main office, and surveils and controls every action of them.

The Silk&Cashmere Company is one of the firms tracking and controlling their employees through surveillance cameras continuously. This company has 44 points of sale throughout Turkey, in each of which, all actions and activities of about one hundred employees are watched and recorded by at least two cameras, installed within each store, during the working period. Gonca Turgay⁵, explains that the records are watched and analyzed in the main office of the company by four employees every day. By this means, it is stated that the faults and errors of employees and also their behaviors and attitudes to the customers can be easily monitored. Besides, Turgay also declares that when it is needed, one of the employees of the surveillance squad is sent to the

⁵ The General Co-director of the Silk&Cashmere Company

related store in order to solve the problem detected by cameras tracking the stores.⁶

In brief, information about every action of workers can be reached by the employers through the information and communication technologies, basically, the computers. Managers have opportunities to monitor and learn what is going on under their authority in the workplace and how the employees and workers do their jobs via auditing, monitoring, e-mail checking, and other several technically mediated forms of surveillance. Attewell (1987: 88), in this issue, declares that the “computer surveillance of clerical workers enables managers to consolidate their power over labor and to increase the pressure on employees to work fast” and to work with no or at least minimum fault.

Another field of monitoring employees is the smart cards used by corporations. There are several smart cards used by the employees of a company while they are entering their workplace or while entering a restricted place in the company building. In addition, some biometric measures are also employed and used together with these cards in order to control the entrance activities of particular places; for example, iris scan, fingerprint, hand geometry, and voice detection are some measures witnessed in some institutions, most of which are state agencies.

It can be useful, here, to give a specific example of using smart cards by employees in the workplace. At Middle East Technical University (METU), the administrative and academic staff and also the students are given ID cards. A microchip and an antenna are embedded into these cards to make them smart cards. At the start of 2002-2003 academic year, the smart card project was put into effect. METU smart card has two applications: While it is an e-wallet for the cafeteria, for example, it is also an e-ID at department buildings, PC rooms,

⁶ Hürriyet, İnsan Kaynakları, December 23, 2007, p.3 and http://www.silkcashmere.com/basin_haber_detay.asph=468

and three campus gates (A-1 gate nearby Eskişehir Highway, A-4 gate in the direction of 100. Yıl, and A7 gate on the Bilkent way) equipped with entry barriers and with 24-hour recording cameras. Elif Maviş⁷ mentioned that the ID cards of the personnel are designed to maintain security at the campus and to control the entrance to the campus and to particular buildings within the campus. There are passing systems that are run by the smart cards of the personnel and of the students at METU. There are two campus gate entries with barriers which are in operation after working hours and at the weekends; all students and personnel with a car sticker are authorized to open the barrier. In addition, the smart card system is also in operation in certain department buildings; specific personnel and/or students are authorized to enter these buildings after working hours, at the weekend, and during the holidays. Another passing system is implemented to enter the PC rooms; all the academic and administrative staff and the students have entry and exit authority to PC rooms at dormitories and department buildings without any time restriction.

As explained by Maviş, the system works as follows: in the central office, that is the computer center at METU, it is assigned who is authorized to open which gates within and outside the working hours. For instance, no student is authorized to enter the computer center building by using his/her ID card. In the same manner, the personnel of the civil engineering, for example, are not authorized to enter the building of the administrative sciences after the working hours. All such settings are determined and arranged by the central office of the computer center, and also arranged according to the decisions of departments' administrative officers. She also clearly states that the student or employee entering a building with a smart-card entrance is seen by the staff of the central office. By this way, when and how often which personnel or student enters which building can be tracked any time or periodically; these

⁷ The Manager of METU Smart Card Project

information are stored in the database for a period. Maviş emphasized that all these arrangements are carried out for the purpose of maintaining security and order. Furthermore, students and personnel can also check their activities and personal records, such as when they enter which building, how often they use PC rooms, etc. through the website.⁸ Furthermore, the smart cards are also used as a means of payment. E-wallet application for the cafeteria, the library, the sports center, the pool and the social lounge is the other feature of the smart card, through which transactions of card holders can be tracked. This feature of the METU smart card is going to be analyzed in the next chapter, rather than under the subject of security discourse.

3.2.2 STREET-BASED SURVEILLANCE AND MOBESE IN TURKEY

In addition to surveillance of employees in workplaces, another and mostly discussed form of monitoring is the surveillance of individuals in the streets, which is also defined as “neo-panopticons” (Mann et al, 2003). There are various surveillance cameras installed to monitor the streets and the individuals in the streets in various countries. This form of monitoring is a recent and also an increasingly developing phenomenon. While street-surveillance cameras are newly used in Turkey, they have been largely used in developed countries, such as, the United States, England, Canada and Japanese for years. Recently, biometric features are equipped inside these cameras; they

⁸ http://smartcard.metu.edu.tr/personal_records.jsp

are not merely watching devices, but also detecting tools including biometric measures such as face recognition system. For example, the cameras in London have the capacity to examine the faces of individuals and to analyze them whether there is a matching with databases of criminals. The first use of face recognition software was in the London Borough of Newham in 1998.⁹

The systematic and institutional use of street-based public surveillance cameras traced back to 1990's. Sherbooke and Sudbury were the first cities of Canada which implemented open-street CCTV cameras monitoring individuals in the streets.¹⁰ Furthermore, England was another country comprehensively founding street surveillance cameras in several cities. Newcastle, London, and Glasgow, Scotland are three of first cities monitoring their streets. As for the United States, Chicago street surveillance camera debut was in 2003 while New York and Los Angeles started to install street surveillance cameras in 2004.¹¹

The foundation and use of public CCTV cameras are materialized according to the policies and decisions of authorities under the name of public safety and security, but without the will or informed consent of the citizens. The mostly declared purpose of the system is the fight against crime. Street surveillance, which is extended to more cities and countries, is demanded and built by the authorities as "...a means to control crime and to maintain social order" (Lyon, 2003: 16).

Due to the widespread existence and permanent functioning of street-based CCTV cameras, individuals tend to feel that they are on constant gaze by the hidden eyes behind the cameras. There is one surveillance camera for one

⁹ <http://www.notbored.org/england-history.html>

¹⁰ http://goliath.ecnext.com/coms2/gi_0199-5119154/Open-street-camera-surveillance-and.html

¹¹ http://www.ibls.com/internet_law_news_portal_view.aspx?id=1804&s=latestnews

hundred-thirty individuals in the world; the record belongs to London, where an ordinary English citizen is monitored three hundred times a day by surveillance cameras.¹² This example indicates that the abovementioned feeling is not paranoia of the individuals. This feeling makes the individuals control their acts and behaviors in the public sphere due to “the fear of the Panopticon”. If you are aware of the fact that someone is continuously looking at you and watching your actions, you inevitably feel the necessity of adjusting your acts and behaviors. Likewise, if you are informed that you are being monitored by the surveillance cameras, you, unintentionally or not, check and control your behaviors.

In order to inform the citizens about the existence of the cameras, the public and private authorities make announcements via signs saying that there is a CCTV system monitoring and recording the area. “This area is monitored by the CCTV” or “You are on CCTV surveillance” signs warn the individuals that they are being recorded by cameras. These signs declare that the CCTV surveillance helps to “promote public safety and manage and protect your property” (Appendix A.1). This security discourse is due to the goal of the legitimatization of surveillance; in other words, security is the most successful discourse, in the hands of power, in the achievement of widespread existence and functioning of monitoring. Under the name of this discourse, people regard surveillance as beneficial and necessary in the current so-called risk societies. This also leads to the increase in the number of CCTV cameras in countries and their cities.

In this respect, Graham (2006: 147) mentions that “‘You are on CCTV Surveillance’ signs are everywhere these days; but these might soon be replaced by signs that say ‘Warning! You are entering an area which is NOT

¹² <http://haber.gazetevatan.com/haberdetay.asp?exec=haberdetay&tarih=06.11.2006&Newsid=92233&Categoryid=7>

covered by CCTV””. This is because of the fact that the authorities have a tendency to build more cameras in the streets on the one side, and the citizens demand more cameras to be built, on the other side, because they regard that these cameras are important tools of crime prevention, of policing, in the establishment of public safety and security. Such a social life wholly surrounded by cameras under the name of security leads to the individuals’ living harmoniously with the existing social and political order. This is because every act of citizens is potentially regarded as dangerous and risky to the order by power holders. In accordance with such a possibility, everyone in the streets, where there are cameras or, at least, signs saying their existence, controls oneself and adjust his/her behaviors.

The visual surveillance and, thus, control and discipline spread all over the society, from guards’ control over the prisoners to the managerial control over the employees, to the parents’ and authorities’ control over the students, and, finally, to the power holders’ control over the ordinary citizens. Such a “dispersal of discipline” (Norris, 2003) to all domains of social life and to human life is the indicator of the society of control. When the CCTV system is in question, it is the fact that “the spread of CCTV over city-center represents the most visible sign of the ‘dispersal of discipline’ from the prison to the factory and the school, to encompass all of the urban landscape” (Norris, 2003: 249). In other words, the CCTV cameras built in the streets are the clear symbols of the surveillance-and-control society.

Under the heading of street surveillance, it can be useful to take into account a newly developed tracking technology, called as Street View which is developed by Google, in order to understand the current case of surveillance in the social life. It is presented via the Internet under the name of entertainment; that is to say, it is enounced by Google that people all around the world can see different countries, cities, and places while sitting on their chairs via the

Internet. The main declared aim of this application is to present various areas of cities to the Internet users in different countries. On the other hand, besides seeing the places, it also gives all people having internet access the opportunity to watch other people, and their houses, cars, and also their activities at a particular time. Google declares that Street View contains imagery that is no different from what you might see driving or walking down the street.¹³

Google Street View differs from Google Maps and Google Earth in that it monitors the streets at the ground level by cameras built on the cars (Appendix A.2). These cars are equipped with cameras recording the 360° panoramic street-level views. Through the website of the Street View¹⁴, the individuals all around the world can track the parts of selected cities and their surrounding metropolitan areas (Appendix A.3). This system started in the cities of United States in May 2007. Until now, the Street View has expanded to hundreds of cities and towns of the United States, and to some parts of France, Italy, Japanese, Canada, Norway, Sweden, Holland, Portugal, Czech Republic, Denmark, Mexico, Australia, and New Zealand.¹⁵ Just through using a computer and an internet access, one can easily monitor the houses, buildings, parks, squares, cars, and also individuals in the streets of particular cities of these countries. The photo of an area is available in the website with a 360° panoramic view at the ground level; one can travel the streets as if he/she is in the car whether looking forward, backward, upward, right side, or left side just through using the mouse of his/her computer.

As mentioned above, Google Street View does not only take the pictures of common places of a city, but also the pictures of ordinary people in their daily lives and also such as their houses, without any permission. In this

¹³ http://www.google.com/intl/en_us/help/maps/streetview/privacy.html

¹⁴ <http://maps.google.com/help/maps/streetview/>

¹⁵ All countries and cities can be seen through http://www.google.com/intl/en_us/help/maps/streetview/where-is-street-view.html

regard, the system is open to be a surveillance tool of corporations for commercial purposes and of governmental agencies in monitoring their citizens. However, Google asserts that the photos presented through the web do not damage the private property and privacy of the individuals. In order to enforce this claim, Google, after broadcasting the photos, allows users to flag inappropriate or sensitive imagery for Google to review and remove the picture. Another application followed by Google to support this claim is that the faces of the individuals and whose photos are taken and the license plates are blurred by Google automatically so that the individual or the vehicle cannot be identified.

However, it is the fact that the Street View cars may take the photos of individuals at anytime and anywhere. For instance, cameras of these cars sometimes capture a man trying to enter a house through climbing over the garden gate and the viewers do not have any knowing whether he is a burglar or just a resident losing his keys (Appendix A.4). Such examples of pictures broadcasted by Google via the Internet can be varied. In short, people are captured at anytime in their daily lives. Therefore, this service of Google is criticized due to its infringements of the privacy of those whose photos are taken and due to its capacity of being a mobile Big Brother.

However, people do not consider Street View as a threat against their privacy and they mostly do not interested in its surveillance capacity; they, on the other hand, regard and use it as an entertainment item. Internet users watch the photos taken in various countries and cities; in addition, they share these photos with other people in the cyberspace such as Flickr, Facebook, Twitter, messenger applications, and their personal web pages. Rather than opposing the existence and the uncontrolled functioning of surveillance cameras or discussing their disadvantages against privacy, individuals mostly consider them as an ordinary item of the social life. This application of Google is a clear

example of street-based visual surveillance and of presenting its place in everyday lives of individuals. Not only the CCTV cameras built in various parts of the cities, but also the mobile cameras, as in the case of the Google Street View, monitor all people and their activities at any time without any distinction.

As for the street surveillance in Turkey, the case of monitoring the streets is relatively a new phenomenon. The first surveillance cameras tracking the streets were installed in İstanbul in 2005. The CCTV system of İstanbul and also of other cities in Turkey is called as MOBESE (Mobil Elektronik Sistem Entegrasyonu / Mobile Electronic System Integration), and is a recent system when compared with those in the developed countries. As mentioned above, the first city in Turkey surveilling the streets via the CCTV cameras was İstanbul. Since 2005, several places of İstanbul have been monitored by 570 MOBESE cameras placed around the city. These cameras are located in areas, especially, where the population density and crime rates are high. They also have the capacity to record what is monitored. The recordings of the cameras are watched and analyzed by the officials at the main office within the İstanbul Police Department (Appendix A.5).

Most of the cameras are monitoring the streets of such as Eminönü, Beyoğlu, Kadıköy, Beşiktaş, and Şişli, where there is a high density of population. 370 cameras are placed inside the city, that is, in the streets where people spend their times. On the other hand, the rest of the cameras are watching the bridges and critical points of motorways around İstanbul; the main goal of the latter is to monitor the traffic jam and to monitor and control the cars in the traffic. These cameras have the capacity, for example, to detect the suspicious and stolen cars and to report them to the central office through tracking the license plates of cars (Appendix A.6).

In addition to İstanbul, authorities aim to build MOBESE systems in other cities as well. As declared by officials of the Ministry of Internal Affairs, this system has been built in 49 cities so far; on the other hand, in the rest of the cities, the installation processes are going to be finished and these cities are going to be surrounded by MOBESE cameras in the year of 2010.¹⁶ Some of the cities currently having the MOBESE system, beside İstanbul, are Ankara, Tekirdağ, Antalya, Konya, Muğla, Diyarbakır, Kayseri, Sivas, Elazığ, Çorum, Mersin and Rize. According to Beşir Atalay, the Minister of Internal Affairs, some cities' lack of MOBESE system is a deficiency; therefore, the system is aimed to comprise all cities in Turkey.¹⁷ As seen, the authorities intend to cover all around Turkey with surveillance cameras so that the eyes of the Big Brother can reach every part of the country and every individual.

In addition to the officials, the citizens also demand, or, at least, do not object to, the cameras built everywhere. In all cities, people regard the camera surveillance over the streets as a precondition of public safety and security. Former questions dealing with the existence of the CCTV cameras as “Are these cameras harmful to our privacy?” are displaced by the questions like “Why don't we have cameras everywhere?”. One indicator of this case is the citizens' increasing demands of CCTV cameras. In this issue, a General Director of a security systems company mentioned that the sales of cameras increased with a rate of 40% in 2007 after the recent crimes which had been caught by the surveillance cameras and after the news declaring the abilities of these cameras presented via the mass media.¹⁸ Likewise, the speeches of the officials and the news of the television channels and newspapers, concerning the fact that the cameras are useful against the criminals, have important effects on people's increasing demand of cameras.

¹⁶ <http://www.showhaber.com/228015/guncel/mobese-31-ilde-daha-hizmete-girecek.html>

¹⁷ Hürriyet Ankara, August 1, 2008, p.1

¹⁸ <http://www.haber7.com/haber/20070123/Dink-cinayeti-kamera-satislarini-patlatti.php>

Hereof, a statement of the İstanbul Police Department can be given as an example. The officials declared that, in 2007, there was a decrease of 30,38% in the crime rates in İstanbul; according to them, the biggest role in this decrease belongs to the MOBESE system.¹⁹ In the same manner, it is declared that, in Konya, where the MOBESE system started in March 2008, there has been a considerable decrease in the crime rates by means of MOBESE cameras since 2008²⁰; similarly, the Antalya police department announced a decline of the crime rates resulting from MOBESE cameras²¹; in Rize, likewise, the officials pointed out that thirty crimes have been detected by MOBESE cameras in a month after the system was installed²².

Discussions about crime-decreasing feature of street surveillance cameras have also been made in London. There are about 10.000 CCTV cameras fighting against crimes in 32 London boroughs; however, 80% of crime remained unsolved according to the data of 2007.²³ Another data in this issue, which is also admitted by the police department, is that only one crime is solved by each 1000 CCTV cameras per year in London²⁴; this means that street surveillance cameras do not work as effectively as declared by authorities.

Another fact, reinforcing the questioning of the benefits of surveillance cameras, is that we regularly witness a crime -not just traffic accidents- committed in front of CCTV cameras through the mass media. Almost every

¹⁹ http://www.polis.web.tr/article_view.php?aid=17335

²⁰ <http://www.haberk.com/haber/21035/mobese-suc-oranini-dusurdu-haberi/>

²¹ http://bilgiedinme.antalya.pol.tr/index.php?option=com_content&task=view&id=741&Itemid=51

²² http://www.semthaber.com/haber_detay.php?haber_no=60334

²³ <http://www.thisislondon.co.uk/news/article-23412867-tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved.do>

²⁴ <http://www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html>

day, there are several news concerning CCTV cameras on television channels and newspapers. For instance, a crime recorded by a MOBESE camera in the street (Appendix A.7) or a capture of arson of a car (Appendix A.8) is broadcasted to the masses via TV, newspapers, and the Internet. These are signs of the fact that CCTV cameras do not stop crimes and criminals. However, the mass media in Turkey present such news in that MOBESE cameras function effectively for security and that they are useful to detect criminals; this also makes individuals think that surveillance cameras are useful and necessary for public safety.

Such news, presenting crimes and criminals in such a manner, lead to the fact that people consider CCTV cameras as essential and useful for security. Accordingly, they feel themselves safe when the areas around them are covered by cameras. Goldsmith (2006) criticized this feeling as “safety in prison”. Similar to the fact that the prisoners feel safe due to the sheltered building with security guards and inspection tower as in the Bentham’s design of Panopticon, the citizens are expected to feel themselves more secure with the existence of CCTV cameras. Particularly, they think or expect that these cameras in the streets prevent the crimes; however, the cameras do not work as a pre-emptive policing device but as a detection tool in the post-crime period. That is to say, the criminals do not quit, for instance, mugging or robbing; they even commit a crime in front of the cameras through such as hiding their faces (Appendix A.8).

The cameras do not merely function as a tool to prevent crime as a pre-emptive policing tool, but also as a tool of “social ordering strategy” (Coleman, 2004) or of “social orchestration metaphor” (Lyon, 2001). This feature of surveillance cameras means that because people conceive that every action of them is tracked and recorded by these cameras, they feel themselves compulsory to control and adjust their behaviors and actions in the social life

under the constant gaze of eyes behind the cameras. By means of such a self-control mechanism, social order can be maintained effectively without any coercive means of power. In relation to this, Foucault (1980: 155) declared that

“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”.

In this issue, the media have a considerable role in accepting the cameras as necessary items in the social life and, thus, in maintaining self-control among individuals and maintaining the legitimization of the extensive functioning of street surveillance cameras. The media, through their news and programs presenting surveillance devices as a favorable item, have a notable effect in this legitimization. As the surveillance system is an increasingly developed tool of the power, in accordance with the “social ordering strategy”, power holders do not want individuals under their authority to question and challenge the system.

Consequently, the power needs to get the consent of the citizens in this attempt of legitimization. Here, the most significant role, again, belongs to the media, which work as a consent-obtainer. The mass media, through their programs, indoctrinate that surveillance systems are for the maintenance of security, public safety and the social order. Rather than questioning the pros and cons of monitoring systems, individuals mostly consider them as necessary. In this respect, the media have more notable and determinative role and function in people’s giving consent to surveillance cameras than the state agencies have.

Consent given to the CCTV surveillance over the streets means also the consent given to the gaze of power over all individuals. This also means that authorities do not need coercive means any more in order to ensure the social

order, to provide social control and domination over the society. The CCTV cameras, particularly, the MOBESE cameras in Turkey that are our concern, are the basic tools in this issue. Therefore, the power needs self-control and consent of individuals in order for the surveillance system to function more properly.

According to Hall et. al (1978), the consent does not arise spontaneously, but is organized through powerful institutions, one of which is the media, as mentioned above. That the cameras detect the criminals and that some examples of this case are presented by the media present us why people do not challenge the existence and widespread functioning of MOBESE cameras and why they do not question whether their privacy is eroded. It can be useful to give some examples about the role of the media in legitimizing the comprehensive use of MOBESE cameras. In addition to traffic accidents presented by the media every day, there are several crimes recorded by these cameras in various cities of Turkey. For example, the arsonists setting the cars on fire in İstanbul were monitored by the MOBESE cameras.²⁵ In addition, as presented by the media and declared by the authorities, the MOBESE cameras recorded the terrorist bombing in Güngören, İstanbul, in 2008.²⁶ Such examples of various crimes recorded by MOBESE cameras and presented by the mass media can be varied.

Unexceptionally, after every event of crime, the authorities state that “the records of the MOBESE cameras are going to be analyzed” and the media announce that “the officials are going to make a statement after the examination of the records of MOBESE cameras”. These cases result in the fact that individuals ask, at first, whether there is a MOBESE camera in the area where the crime occurs.

²⁵ <http://www.hurriyet.com.tr/gundem/7921321.asp?gid=48&sz=7646> and <http://www.milliyet.com.tr/2008/01/01/siyaset/asiy.html>

²⁶ http://www.ntvhaber.org/haber_detay.asp?haberID=3537

These abovementioned cases that are the broadcastings of the statements of the authorities, the programs of TV channels and the presentations of the mass media serve to the power holders in the legitimization process of surveillance through affecting and manipulating people in their giving consent to monitoring and in their formation of self-control. By this means, social control can be provided and domination of power over the society can be ensured more effectively and comprehensively without any coercive means of power.

3.3 SURVEILLANCE THROUGH BIOMETRICS

Biometrics has been added to the surveillance technologies, especially, to CCTV monitoring systems, in order to make the system more efficient and effective. Some forms of biometrics used in the surveillance practices can be listed as follows: fingerprint technology, iris scanners, face recognition software, voice detection systems, and DNA analysis. With the use of biometrics in the field of surveillance, the human body becomes the source of the surveillance rather than the site of the surveillance; that is to say, “surveillance is turning decisively to the body as a document for identification, and as a source of data for prediction” (Lyon, 2001: 72).

Through using the data obtained from the human body in order to monitor and control the activities of individuals, biometrics technology is used, for example, in border security, the airport screening, in employee tracking, and even in the street-based surveillance. Biometrics, especially, comes into

consideration in the detection of criminals and suspects. In order to do this, the states establish databases formed through collecting information of their citizens and of the individuals entering the country. There is an increasing tendency in the collection and storage of information of individuals, whether citizens of the given country or foreigners, especially, after the 9/11 terrorist attacks. Accordingly, databases are formed through collecting personal information of individuals. The name and photograph of an individual are already in his/her passport. In addition, these data are digitally stored in databases together with person's fingerprints in some countries such as England and the United States. Biometrics is, today, extensively used in these countries as an embedded feature of surveillance and control particularly for border security and is used as a measure against crime, mainly, terrorism.

The countries have used biometrics especially in airports as a tool for identification and verification purposes. It helps the state agencies such as in the airport tracking to identify who the person is, whether there is a match with those stored in the database, and, besides, to verify whether the person is actually that he says he is through such as face recognition systems and fingerprints.

This system is largely used in the visa applications while entering a country in order to maintain the border security. Such surveillance practices are generally seen necessary in the fight against fraud and terrorism, and in the control of illegal immigration. When the security discourse is in question especially in the post-9/11 period, the privacy has gained a secondary importance. Individuals are in a tendency that they do not have any chance to oppose so-called security applications while doing check-in in the airports. This is because of the fact that whether they consider these applications useful in the fight against crime or they see them as a precondition to enter the country.

While there is such a tendency, biometrics is increasingly becoming principal tools of state and private agencies. Unlike other tracking practices, biometrics provides much more accurate and correct information about people to the power holders. While surveillance cameras monitor a specific place and individuals in there, biometrics-added surveillance cameras also identify individuals and verify their identities through, for instance, face recognition software. Thus, biometrics is much more useful for power to eliminate uncertainties or, say, for rationalization. The more rationality permeates into social life, the less uncertainty and unpredictability occurs. Although it is also valid for other surveillance technologies, biometric applications give the authorities much more opportunity to categorize individuals, which is defined as “social sorting” by Lyon (2003), whether they are criminals, or suspects, or potential threats, or harmless.

Such a categorization among people is expected by power holders to be useful in the elimination of risks and uncertainties in the social life, and, thus, in the maintenance of rationality. The motto of such a tendency can be as “social sorting for social order”. In order to provide social order,

“abstract data, now including video, biometrics, and genetic as well as computerized administrative files, are manipulated to produce profiles and risk categories in a liquid, networked system. The point is to plan, predict, and prevent by classifying and assessing profiles and risks” (Lyon, 2003: 13).

Rationality, today, which is promoted by surveillance technologies, makes these planning, predicting, and preventing issues more achievable through databases in which every sort of information of people can be stored.

In order to eliminate risks and uncertainties, the states are inclined to build more biometrics-equipped surveillance technologies because such

systems work more accurately in identifying and verifying the data of individuals. Therefore, there has been a huge growth in the biometrics market. In year of 2000, expenditures for biometric systems was about 66 million US dollars worldwide, which comprised fingerprint scanning, hand geometry, iris and retina scanning, face recognition, and voice and signature verification technologies.²⁷ On the other hand, the size of the market reached to 2 billion dollars in 2006²⁸, and to 3 billion dollars in 2008²⁹; which means that the worldwide market grew 3.030% in eight years.

The US government, as an initial example, gives much significance to the security issues, and, thus, the biometrics measures. In the post-9/11 period, the US government has built a program, called as US-VISIT (United States Visitor and Immigrant Status Indicator Technology), which declares that it helps federal, state, and local government decision makers accurately identify the individuals they encounter and determine whether they pose a risk to the United States.³⁰ It, for example, involves the collection and analysis of biometrics -digital fingerprints and photograph- of travelers in their visa issues. This program is expected by authorities to prevent identity fraud, criminals, and immigration violators. Since 2004, photographs and fingerprints of the international travelers willing to enter the United States have been collected and stored due to the security concern (Appendix A.9). Furthermore, in 2007, the US government started to use ten-fingerprint scanners collecting ten fingerprints from international travelers³¹ (Appendix A.10).

²⁷ <http://www.findbiometrics.com/Pages/feature%20articles/anatomy.html>

²⁸ <http://www.securitypark.co.uk/security-market.asp>

²⁹ <http://www.itpro.co.uk/604920/biometrics-market-to-double>

³⁰ <http://www.dhs.gov/files/programs/usv.shtm>

³¹ http://www.hurriyetusa.com/haber/haber_detay.asp?id=15165 and http://www.dhs.gov/files/programs/gc_1194553866460.shtm

As for the biometrics practices in the European Union, the member countries formed a European fingerprint database, called as the Eurodac system which entered into force in 2003, for comparing the fingerprints of asylum seekers and illegal immigrants. The system functions to control and to identify them, and to determine whether the immigrant entered the Union territory unlawfully.³² Besides, the first integration of biometric features in passports and travel documents, also known as e-passport, was implemented in the EU in 2004; the facial image and fingerprints of the person are stored in a chip inside the passport/travel document.³³ Such e-passports, with an embedded chip and antenna in it, are increasingly preferred by other countries due to its ability of preventing risks concerning security through identifying and verifying individuals.

In addition to such chip technologies for surveillance purposes, there are also several software programs, analyzing the biometric features of individuals, which are used in surveillance practices. Several large-scale or small-scale companies are developing biometric products, such as, FaceIT, TrueFace, I-Scan, SpeakEZ, Cybertouch, NR Identity, Voice Print, etc. (Van der Ploeg, 2006). FaceIT ARGUS is one of the most popular face recognition systems and is produced by a US-based company, the Identix Corporation.³⁴ When a CCTV camera captures a face of an individual, FaceIT analyzes the face and compares it with the database whether there is a match or not.

The system works as follows: FaceIT creates 3D image out of an individual's digitized 2D photograph. It generates a faceprint that is unique to each individual, and through using a series of different algorithms, the system examines whether there is a match between the 3D image created digitally and

³² http://ec.europa.eu/justice_home/key_issues/eurodac/eurodac_20_09_04_en.pdf

³³ http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/114154_en.htm

³⁴ <http://www.identix.com/pages/71-facial-screening>

the image of a person tracked by the CCTV camera (Appendix A.11). The developer company of FaceIT declares that “FaceIT can find human faces anywhere in the field of view and at any distance, and it can continuously track them and crop them out of the scene, matching the face against a watch list” (quoted in Graham and Wood, 2003: 236).

A new technology is also in practice in the surveillance of individuals: RFID (Radio Frequency Identification) tags. RFID is, mainly, used for tracking the objects, such as manufactured goods, pharmaceuticals, containers, and vehicles, during transportation from the point of departure to the point of arrival. It gives owners of the objects or the officials the opportunity to monitor and to control their objects during the transportation process. RFID tags are very tiny chips and can be installed into or onto any object easily and secretly so that no one can easily notice the existence of the RFID tag which has a surveillance capacity (Appendix A.12). They consist of a chip which stores the data of the given object and a tiny radio antenna which can receive and transmit a radio signal. Every object having an RFID tag is given a unique RFID tag number, which is not similar to any RFID tag number. In addition to the hidden placement of tags, there are also hidden readers, receiving the information stored in the RFID tag. The tags can be read from a distance through radio signals. By this means, the data stored in the tag are read by the readers where they exist. Data read by the reader, then, are sent to the computer, with which the RFID reader was attached.

RFID technology was, previously, only related with commercial issues; it, now, goes beyond its initial usage. Recently, RFID tags are placed, for example, into ID cards, passports and visas so that the individual having an RFID-embedded passport, for instance, can be monitored while does not notice he is being tracked (Appendix A.13). RFID tags inside the passports contain the information of person's name, date of birth, place of birth, digital

photograph, and a digital face recognition template; these data are transmitted to the operating computer via the RFID reader when RFID tag receives a radio signal from an RFID reader (Wilson, 2007: 213). By this way, when a person, carrying an RFID-embedded ID card or passport, enters a zone checked by the RFID reader, he/she is monitored until he leaves the zone of the reader.

RFID readers are generally placed in specific areas, such as airports, stations, official buildings, and even stores. RFID readers in such places work constantly and search RFID tags in order to track those having an RFID tag in their pockets. When the reader detects an RFID tag, it informs the main control point and transmits the data of the individual, which are received from the tag, to that center. By this means, the officials track the individual during the time he is in the RFID-reader zone, analyze and profile his/her data. This technology is used for security matters by state agencies such as in the identification of people through data transmitted by the RFID tag and in the comparison of them whether there is a match with the database of criminals and suspects. The potential of use of this technology by private corporations for commercial purposes is going to be mentioned in the next chapters.

In addition to considering surveillance and control under the name of security, another mostly used discourse is the efficiency, or, say, consumer satisfaction and service improvement. In the following chapter, this case is going to be discussed through analyzing the surveillance of personal data of employees in the workplace, students at the school, and of consumers in their shopping. In doing this, smart card technology and loyalty cards of firms and their practice in Turkey are going to be analyzed comprehensively.

CHAPTER 4

SURVEILLANCE AND CONTROL THROUGH PERSONAL DATA

State and private agencies, or, say, power holders, employ not merely face-to-face surveillance, visual surveillance, and direct control in order to make everything visible, predictable, and controllable, and thus, to maintain rationalization and social order, but also chip-technology-based surveillance practices gathering personal information of individuals. As discussed by Lyon (2007), we have moved from face-to-face surveillance to “file-based surveillance”. In such a form of surveillance, beside people’s actual acts and behaviors, their personal data, for instance, their names, occupations, habits, consumption patterns, and lifestyles, are also monitored through basically chip-embedded smart cards. A person’s using these cards in workplaces, schools, and in shopping means that his/her personal data and activities are potentially open to the gaze, control, and manipulation of power holders.

While doing shopping, for example, not only consumers’ data of expenditures, but also their preferences, needs, likes, and dislike are subject to the surveillance of firms. The main question, here, is how and for what purposes personal data of people are collected and used. The surveillance of individuals, mainly, consumers, here, is pursued in order to not only monitor

their transactions, choices, needs, and habits, but also control and manipulate them. In addition to this specific commercial goal, the overall goals are to achieve rationality through reducing uncertainty and spontaneity and to ensure domination over the society.

Several technologies and practices are developed and employed through using new technologies by state and private agencies in order to get and collect data of people. One technique gathering personal data and working as a surveillance mechanism, also emphasized in the previous chapter, is chip-embedded ID cards. They are a tool which is used by states in the identification of individuals, in the verification their identities, and in the track of their activities in order to rationalize the state affairs.

Every action of citizens, such as in banks, ministries, tax agencies, and passport applications, can be watched by state authorities and can be stored in databases. A similar application started in Turkey in 2002, which is called as MERNİS (Merkezi Nüfus İdaresi Sistemi / The Central Population Administration System). In this system, ID cards of Turkish citizens are not chip-embedded smart cards for now; however, a central population database was formed and each citizen was assigned a single and unique citizenship number. This number, which is written on ID's, is used compulsorily in citizens' every relation with ministries, municipalities, banks, hospitals, tax offices, social security institutions, and courts. Instead of names, these numbers are used while paying taxes, opening an account in a bank, getting a credit card, registering residences, and being treated in a hospital, for example. In short, names are replaced by citizenship numbers in all state affairs concerning administrative and economic issues. By this means, institutions can track individuals, and their residences, wages, incomes, tax payments, etc. through databases established according to these data. Such issues help states in the

rationalization of their affairs and of the relationship between citizens and administrative and economic institutions.

In addition to such ID's, and chip-embedded ID's and passports, there are also other forms of smart cards used by private corporations to surveil their employees and by managers of schools to surveil students. Furthermore, there are also loyalty cards improved and employed by companies to spy on customers and their transactions in the course of shopping. In these cases, data of individuals are collected, stored, and processed by means of chip-embedded smart cards and also, of course, computers. Beside smart cards, the other area of collecting personal data is the Internet. Computer users are sometimes surfing the websites, sometimes doing shopping in the cyberspace. Websites have technological capacity to get information about the user through tracking the IP address of the computer; for instance, how often he visit which websites, what he buys, which websites he has a membership, and what movies he watches can be monitored in the cyberspace.

Through using these techniques which monitor people's consumptions, transactions, habits, and lifestyles, companies get the ability to form databases. Firms, whether a store or a website, establish databases so that they not merely can learn consumers' acts and activities, but also manipulate them. Because of such a feature, databases have become a surveillance mechanism. Regarding this fact, Poster defines databases as "Superpanopticon", which is defined as "a system of surveillance without walls, windows, towers, or guards" (Poster, 1990: 93), or as "a system of surveillance that transcends physical and institutional structures" (Goss, 2002:180). Unlike the guards and physical surroundings in Bentham's Panopticon, no surveiller, here, physically watch and monitor people; yet, databases do.

Every day, we, as consumers, are exposed to advertising messages sent to our mobiles phones and/or our e-mails. In this regard, the common question

asked by most people is “how did they get my name / my phone number / my address?”. For example, when a woman gets a message about a campaign of cosmetics, she can ask “how did they know I am female?”. The answer to these and similar questions is databases, which are established through storing our personal information and transactions. The firms, as the actors of Superpanopticon, know not only their customers’ names or phone numbers by means of the membership forms of loyalty cards filed out by customers, but also whether they have children, whether they have pets, and whether they have specific interests and habits through tracking their shopping baskets and analyzing their transactions which are gathered via loyalty cards.

In order to achieve this, data surveillance, or say, dataveillance (Clarke, 1988) has become a notable tool of capitalism to maximize profits and to increase efficiency. Stores and the Internet are the main areas in which people submit their personal data and data of transactions to the firms. As an outcome of such tools, corporations have regarded consumers not as individuals but as “databased selves” (Simon, 2005) or as “digital personae” (Clarke, 1988) from which data they need are collected. The individual is considered by firms as a digital identity which is composed of numbers and data through isolating from the personality.

In this chapter, hereafter, how surveillance and control work through using personal data gathered via smart cards and the Internet is going to be mentioned. Basically, surveillance over employees, over students, over consumers, and over the Internet users is going to be discussed and analyzed through also considering some examples realized, particularly, in Turkey. Herein, smart cards monitoring students and employees, loyalty cards monitoring consumers in their shopping, and technologies monitoring people in the cyberspace are going to be explained and discussed critically. Surveillance through personal data is going to be dealt with through mentioning particular

examples of smart cards in Turkey. In addition to the examination of the working process of smart cards, the goal behind the smart card practice pursued by institutions is also going to be analyzed. The purposes of, such as, efficiency, profit maximization, and manipulation of consumers are the main discussion points of this chapter. Besides and more notably, the overall goal of power holders, the ideology behind surveillance practices, and dataveillance's becoming an ideological tool of power are also mentioned in this chapter and largely discussed in the final chapters.

The examples of dataveillance of students and employees, taken into account in this issue, are the METU ID card used by both employees and students within the boundaries of the campus and the smart card at METU College used by students in the school as a means of payment. I made interviews with Elif Maviş³⁵ for METU ID card and with Erdem Şahin³⁶ for METU College smart card. From these interviews, I got information about the structure and functioning of smart cards and how and why personal data are gathered and stored.

As for loyalty cards, more concretely, loyalty cards, used by consumers in their shopping, I made interviews in-depth with ten officials from six different companies. The club cards of firms I researched and am going to point out are Migros club card and Koçtaş club card which take place within the Paro program³⁷, CarrefourSA card, Beğendik club card, Praktiker card, and Öğütler card. Furthermore, I examined a recent development in the loyalty card system. It is that banks have established joint card programs with firms. In such programs, companies share their customers' data with banks. There are, so far,

³⁵ The Smart Card Project Director of METU

³⁶ The Smart Card Project Manager of Sofra A.Ş. at METU College

³⁷ It is a program, in which different companies as Migros, Koçtaş, Ford, Opet, etc. work together, provide joint campaigns to their customers and in which a joint customer database is formed and shared by these companies.

three examples of such cooperation in the Turkish market. One is the Money Card in which Garanti Bank, on the one side, and the companies, namely, Migros, Tansaş, Şok, and Macrocenter, on the other side, work together and process and use the common consumer database. Another joint card program of Garanti Bank is Forum Bonus Card. In this program, Garanti Bank and Forum malls in Turkey are the partners. The other example of joint program is the Carrefour Axess, in which the partners are CarrefourSA with its stores all around Turkey and Akbank, the owner of the Axess credit card. In three cases, the banks store and process data of customers achieved through these cards.

I researched the working process of loyalty-card system through visiting some branch offices of stores. The firms and their branch offices I have visited are Migros in Ankamall, Maltepe and Beşevler; Koçtaş in Ankamall; CarrefourSA in Armada and Cema; Beğendik in Kocatepe; Praktiker in Bilkent; and Öğütler in Kolej, Maltepe and Gimat. The interviews about Migros club card, Koçtaş card and other club cards in the Paro program were made with Kına Demirel³⁸, Serenat Çakır³⁹, and Teoman Vural⁴⁰. As for Beğendik club card, the interviewees were Ata Beğendik⁴¹ and Şebnem Yıldız⁴².

In Praktiker, Ülkü Demiroğlu, from the department of Customer Relations, is the official who explained me the features and working process of Praktiker card. Furthermore, I made interviews about CarrefourSA club card with Mine Şenel⁴³ and Hasret Akar⁴⁴. Moreover, those I got information about

³⁸ The Director of Migros Club Card Department

³⁹ The Customer Relations Manager of Ankamall Migros

⁴⁰ The Service Department Manager of Ankamall Koçtaş

⁴¹ The General Director of Beğendik

⁴² The Director of Beğendik Club Card Department

⁴³ The Manager of Armada CarrefourSA

⁴⁴ The Manager of Central Counters in Cema CarrefourSA

Öğütler club card are Ömer Öğüt⁴⁵ and Garip Elmalı⁴⁶. According to these interviews and researches, dataveillance practice in Turkey is going to be analyzed in order to point out how and why corporations attempt to surveil and control individuals.

4.1 EMPLOYEE AND STUDENT SMART CARDS

The most common use of smart cards is the identity cards used by employees in public and private institutions while entering the workplace. For example, some employees can be authorized to enter a particular room in the workplace. Managers both in governmental agencies and in private corporations intend to know every event in the workplace and every action of their subordinates. These door-opening smart cards, through which rationalization in the workplace is achieved, serve managers to watch and control everything under their authority. Identity cards, which also function as smart cards when a chip is placed into or onto them, are used to track and control the activities of employees. These cards, which are attached to a computer system, have the capacity to inform the managers when employees enter the workplace and which employees are where during the working period and when and how often they enter different parts of the workplace.

Smart cards and RFID tags used in the schools are a more recent example when compared with smart cards used in the workplace by employees.

⁴⁵ The Director of Computer Center of Öğütler

⁴⁶ The Manager of Kolej Öğütler

School managers tend to use these technologies in order to monitor the actions of students. Other than using physical-surveillance techniques, information technologies as chips and computers are mostly applied to get information, for example, whether and when the student enter and leave the school building.

Two examples of monitoring students by school authorities can be given from the United States. One is that, in Texas, children wear RFID tags to alert school authorities and police when they get on and off the school bus (Lyon, 2007: 17). Another example is Enterprise Charter School in Buffalo, New York, which started to use RFID tags for their students in 2003. Enterprise was the first school in the USA to require compulsory RFID tags to attend the school. When the RFID tags are scanned at the entrance of the school, the readers record and store the data such as the students' photos, dates of birth, and enrollment details as they enter the school building (Albrecht and McIntyre, 2006: 173).

An example of smart card in Turkey is seen at Middle East Technical University (METU). The identity cards of both students and employees are also designed as smart cards in order to be used in various activities in the campus. As mentioned by Elif Maviş, the smart card project of METU has two features: one is the e-ID to maintain security and the other is e-wallet to use ID card as a means of payment. In the previous chapter, the features and functioning of METU ID card within the security framework were explained. E-wallet application is the subject of this chapter. This application is implemented in commercial issues within the campus. The cafeteria, the library, the students affairs office, the faculty club the social lounge, the computer center, the pool, the sports center, and the Baraka gymnasium are places where academic and administrative staff and students use their ID's as an e-wallet, instead of money.

After matching their identity cards with their bank accounts, they can, for example, pay the bill at the cafeteria, pay entry fee for the sports center, pay the printer fees at the computer labs, and pay fines for overdue books in the library with just their ID's. The smart card system does not comprise the private enterprises in the campus, but only the foundations of the Presidency. By this way, as also pointed out by Maviş, data about transactions of students and employees and about activities they deal with in the abovementioned places are collected and stored in the central office of the smart card project. In more detail, what a student or an employee buys, what he/she consumes, which sport activities he/she deals with, and when and how often he/she uses these services can be easily seen and monitored through databases established accordingly.

Maviş points out that while all data about all students and employees are seen in the main office, the relevant units have the opportunity and authority to examine and analyze the data concerning their unit. For instance, as for the social lounge, the director of this unit can watch who prefers to eat which foods and how often students and employees use the lounge. Director of one unit cannot see the data related to other units; on the other hand, the central office has the power to see every transactional event of each unit. In addition, students and personnel themselves have the chance to check their expenditures. Through the website of the smart card system⁴⁷, they can see, for example, when they eat what in the cafeteria and in the social lounge, what they spend in a specific date, and when they go to the sports center or to the pool. All these data are also subject to surveillance of managers who analyze databases of card holders. As stated by Maviş, data obtained from the commercial activities of students and employees in the presidential units are used to better the commercial activities of units within the campus, and no data is shared with any private company. Through analyzing transactions, preferences, activities,

⁴⁷ https://smartcard.metu.edu.tr/personal_records.jsp

and habits of card holders, the Presidency or one of its units rationalizes its activities and its relations with students and personnel through making everything under their authority visible and predictable.

Beside METU ID card, another smart card application which is only used by students is the smart card of METU College. At METU College, as described by Erdem Şahin, students are given smart cards in their registrations to the school in order to be used instead of money in the canteen and cafeteria. The initial goal is to use these cards as a device of payment in the expenditures of students. Whether the students themselves or their parents load some amount of money to their smart cards via the card reader located at the school. And the card is scanned by readers in the canteen and in the cafeteria while the student is buying foods. Therefore, students do not need to carry money. Şahin explains that all transactions of each student made throughout the week, month, and year are stored in the database of the school management. By this means, officials of the smart card project can monitor expenditures of each student in a particular day or periodical, for example, what he/she buys frequently, how often he/she uses the cafeteria, and what spending habits he/she has. These data about students' daily and monthly expenditures are stored in order to form a database of students.

These data of each student can also be shared with the parents of the student when demanded by the parents. Parents have the chance to learn all consumption habits of their children from the school managers or from an e-mail. This informing process functions according to the demand of the parents; that is to say, there is not an automatic sending of data to the parents. However, it is the fact that most parents demand to be informed about expenditures of their children⁴⁸; the function of this surveillance system is up to that point. The subsequent behaviors of the parents to their children are outside the scope of

⁴⁸ From the interview with Şahin, Erdem

the system. It can be concluded that such a smart card system, which is employed to replace money in expenditures, becomes a surveillance and control mechanism of parents over their children.

By this way, they have become informed about what their children buy and what kind of expenditure habits they have. They whether try to discipline their children's actions and transactions if necessary or just want to be an all-seeing eye over them without interfering them. Gary Marx (2005) defines such monitoring tools which are used to monitor the kids as "electronic leashes". Not only such smart cards, but also RFID tags, cell phones, GPS (Global Positioning Systems), and computer guarding programs are also used as electronic leashes. These technologies notify the school authorities and/or parents where the kid is, what he/she buys, which websites he/she visits, what consumption patterns he/she has, and so on. By this way, parents can surveil their children and control them even at a distance.

4.2 CONSUMER SURVEILLANCE: THE ANALYSIS OF LOYALTY CARDS IN TURKEY

Capitalism, or, say, power, in general, wants and aims to know everything occurring in the society in order to take policies for the well-being of the social order. Therefore, power holders, both state agencies and private corporations, perform several tools, as mentioned in the previous chapter, such as CCTV monitoring and biometric-based technologies in order to gaze people under the name of security. And they use these technologies to maintain social

order and strengthen their power at the expense of civil society, beside the goal of security.

By this way, power has got tools to become aware of every event and to monitor individuals in order to eliminate uncertainties in the contemporary society. However, this is not considered adequate and satisfactory by the power. It is the fact that power holders “want to know not only what you are doing and saying, but also what you are likely to do or say next” (Lyon, 2001: 56). For this issue, corporations have employed some other forms of surveillance technologies as credit cards and smart cards, collecting people’s personal data in the commercial field, so that they can get information about not only physical characteristics and actions of individuals, but also their likes, dislikes, needs, preferences, and living patterns.

As far as such data of individuals are learned, it has become possible to control them, to manipulate their needs and choices, and, finally, to make them be obedient to the existing order, similar to the “docile bodies” of Foucault (1977). Power wants all citizens to be under constant surveillance and control and to be in harmony with and not to challenge the existing order. In addition to visual surveillance and biometric surveillance, discussed previously, another notable field of surveillance is commercial to create docile bodies which are under permanent control. Commercial is regarded as a notable field of monitoring because it is the field that every individual deal with; everyone is, more or less, in the sphere of consumption.

As mentioned by Goss (2002: 193), “to stand outside the sphere of consumption ... is to stand nowhere at all in contemporary society”. Thus, power gives much significance to commerce in monitoring and controlling people. People do not need to do much thing; just their existence in the commercial field leads to the surveillance by the power. Their every information about their transactions, preferences, lifestyles, etc. are subject to

surveillance through whether credit cards or loyalty cards of companies employed for the use of their customers. In short, as stated by Fox (2001: 251), “simply by participating in modern commerce, individuals are significantly eroding their own privacy”. Companies track and watch individuals in the modern commerce in order to manipulate and control individuals, their behaviors, choices, needs, and so on.

The first step of controlling individuals is to identify them. Hence, firms have introduced techniques to surveil and manage consumers. The most well-known techniques are credit cards of banks and smart cards performed by supermarkets for the use of their customers. Through these cards, firms have got the possibility to get information about expenditures, needs, choices, consumption patterns, and, thus, lifestyles of consumers so that they produce and market their items and advertise them according to the information gathered from consumers.

In the previous title of this chapter, it is mentioned that the daily/monthly expenditures of METU College students are monitored and collected through using smart cards and that these data are shared with parents. However, rather than such a specific case, surveillance over all consumers is the point of discussion, here. The first tracking technology applied, which monitors the transactions of consumers, was the credit cards of banks. These cards reveal some issues such as what the card user buys from where. On the other hand, all items of the expenditures, that is, the content of the shopping basket, are not seen through credit cards. For example, banks can monitor how much the card user pay for the supermarket shopping, but cannot see what products he/she buys.

In order to satisfy this necessity of the firms, loyalty cards are introduced for the supermarket customers. Through these cards, all expenditures of each customer using loyalty card in their payment and all

goods they buy are monitored. These data are more important for the firms than those obtained by credit cards due to the fact that needs and consumption patterns are watched via loyalty cards.

Several firms have employed their loyalty cards for their customers. Out of them, club cards of Migros, Koçtaş, Opet and Ford are going to be considered and analyzed together because these firms are the members of Paro system. This is a system in which different firms share their customer databases and follow common policies. A Migros club card user, for example, can also take advantage of and benefit from the campaigns of Koçtaş. He/she can use his/her existing card in another Paro company as if he/she has a club card of that company. The current list of the members of the Paro program is as follows⁴⁹:

- Migros
- Koçtaş
- Opet
- Ford
- Fiat
- Arçelik
- Beko
- Aygaz
- Mogaz
- Koç Allianz
- Avis
- Setur
- Divan
- Demirdöküm

⁴⁹ All members of the system are announced on the website of the program, <http://www.paro.com.tr>. The list of members is updated if there is a new member or if there is a leaving from membership.

- Nokia
- Burger King
- Sarar
- Arstil Furniture

In addition to these companies, recently, World Card, the credit card of Yapı Kredi Bank, has entered the Paro program. This means that World Card user can get benefit from campaigns of the abovementioned stores, Furthermore and more importantly, Yapı Kredi Bank can reach and follow customer databases of Paro companies, and use them for its commercial purposes. Before going into the deep analysis of the loyalty cards, I think it is useful and necessary to give some information about loyalty cards.

According to the information gathered from the interviews and researches, it is witnessed that the first and most common loyalty card used in Turkey is Migros club card, which has been in the market since 1998. It has almost a historical background like that of bank credit cards. In order to get information about both Migros club card -the leading loyalty card in the market- and credit cards, it can be useful to point out the number of people having these cards. Migros started loyalty-card system in 1998; at the end of that year, Migros had 900.000 card owners. This amount can be considered satisfactory in the first year of the system. In the next year, 1999, the number of card owners reached to the amount of 2.500.000 with an increase of 177%. Such an enormous increase might be due to the fact that Migros was the first firm providing several economic benefits, especially, discounts, to its customers having the club card; people, in order to be a special customer through getting opportunities the non-card-owner customers do not utilize and to economize their purchases through discounts, might become the member of Migros club card. In 2008, up to August, the owners of Migros club card have

reached to 13.000.000, which means that there is an increase rate of 1.444%, in ten years.⁵⁰

In the same period, between 1998 and August 2008, the total number of bank-credit-card owners has reached from 7.118.358 to 41.574.759.⁵¹ As can be seen, while the increase rate of the Migros-club-card owners is 1.444%, that of credit-card owners is 584%. The main reason of this difference between these cards is that while the cards, in the former case, are given to all customers of Migros without any stipulation, the banks do not give all their customers credit cards. The only condition of getting a loyalty card is to fill out the membership form; the next step is to utilize the benefits of the card. On the other hand, the applicant of a credit card has to meet several conditions, such as a salary, demanded by the bank in order to get the credit card.

Migros club card and its long-term use have paved the way for other firms to develop their own loyalty cards for their customers. Every year, a lot of new customers have been added to the members of loyalty cards of firms in order to benefit from the cards' opportunities, such as a rebate. Recently, a lot of firms, such as almost all supermarkets, gas stations, and large stores, provide loyalty cards, or, so-called club cards, to their customers.

While the number of card users gives us an idea about the use of loyalty cards in Turkey, the percentage of customers using a card in their payment on the counters is the other significant information pointing out the significance of loyalty cards in the commercial field. For example, on the counters of Migros,

⁵⁰ The numbers of Migros-club-card owners have been gathered from <http://www.migros.com.tr/tarihce.asp> and from the interview with Demirel, Kına, the Director of Migros Club Card Department.

⁵¹ These data have been gathered from the reports of BKM (Bankalararası Kart Merkezi / The Interbank Card Center): <http://www.bkm.com.tr/istatistik/raporlar1.html> and http://www.bkm.com.tr/istatistik/pos_atm_kart_sayisi.asp

80% of customers use their loyalty cards while shopping⁵²; on the other hand, this ratio is about 75% in Beğendik⁵³ and in CarrefourSA⁵⁴ while it is 70 % in Öğütler⁵⁵. These rates explicitly reveal that the using of loyalty cards among customers is high. Therefore, it can be claimed that about 70-80% of customers of stores are comprehensively under the constant gaze of firms. This means that millions of people are under surveillance of companies in the commercial field while they are shopping daily or periodically in their stores all around Turkey.

These high amounts of the use of loyalty cards stimulate banks to be interested in this field. As mentioned previously, there are three cards, namely, Money Card, Forum Bonus Card and Carrefour Axess, in which banks and large stores work together. Actually, first two of these three cards are the credit cards of Garanti Bank and the third one is of Akbank. On the other hand, they function not only as a credit card, but also as a loyalty card. This means that owners of these cards benefit both from the advantages of the credit card, its monetary exchange value, and from the advantages of the loyalty card, such as discounts and campaigns in shopping.

The holder of Money Card uses his/her card in Migros, Tansaş, Makrocenter and Şok while shopping not only as a loyalty card which supplies some economic benefits as discounts but also as a credit card of Garanti Bank. This means that data of customers, basically, his/her personal information and consumption patterns, are subject to surveillance and, thus, manipulation of these firms and the bank. Customers of 251 Migros stores, of 281 Tansaş stores, of 9 Macrocenter stores, and of 709 Şok stores throughout Turkey

⁵² From the interview with Çakır, Serenat

⁵³ From the interview with Beğendik, Ata and Yıldız, Şebnem

⁵⁴ From the interview with Şenel, Mine and Akar, Hasret

⁵⁵ From the interview with Elmalı, Garip

(which means thousands of people from different ages, sexes, educations, and locations) are potentially the surveillees of Garanti Bank.⁵⁶

The other joint card program of Garanti Bank, Forum Bonus Card, also contains a large amount of customers, like Money Card. Here, customers of seven Forum malls in Turkey and of firms in these malls use this card and become subject to the surveillance of Garanti Bank. These seven malls are Forum İstanbul with 130 different firms working in the forum, Forum Ankara with 72 firms, Forum Bornova, İzmir, with 81 firms, Forum Aydın with 48 firms, Forum Mersin with 131 firms, Forum Trabzon with 81 firms, and Forum Çamlık, Denizli, with 62 firms.⁵⁷ Through this card, Garanti Bank can learn every product in the shopping basket of each customer of these firms. While shopping, Forum Bonus Card is read by the counter; thus, the personal information embedded in the card and content of the shopping basket of the customer are stored in the database via computers. By this way, Garanti Bank can track the expenditure habits, likes, and dislikes of customers.

As for Carrefour Axxess, the same abovementioned working process is in use for this card in CarrefourSA stores. Customers use their cards in their shopping in 25 CarrefourSA stores in 12 cities in Turkey.⁵⁸ CarrefourSA card is different from Carrefour Axxess in that while the former is only a loyalty card that provides such as discounts, the latter, additionally, provides the opportunities of a credit card such as hire-purchase.

Loyalty cards and these three credit cards in the disguise of loyalty cards are considered by customers as discount cards, other than as a tracking

⁵⁶ More information about campaigns of Money Card and detailed information of stores can be reached via the website, <http://www.money.com.tr>

⁵⁷ Whole list of malls and the firms in these malls, name by name, can be seen in <http://www.forumcard.com.tr/program-ortaklari.aspx>

⁵⁸ The whole list of CarrefourSA stores in Turkey can be seen in the website of the firm, <http://www.carrefour.com.tr/magazalar.asp>

device. This is because, as mentioned by Ata Beğendik, when customers see discount rates on certain items only valid with the loyalty card, they want to get and use the card to benefit from its economic advantages; they are not interested in and do not question the functioning and characteristics of the cards they use regularly. On the other hand, in the viewpoint of the firms, loyalty cards are put into use in order to maintain loyalty between the customer and the firm. Accordingly, firms make promotions, lottery drawings, etc. to reward their customers who prefer shopping in their stores and to maintain and strengthen that loyalty.

On the other hand, the basic and foremost reason of using these cards is the surveillance of consumers. All transactions of each consumer can be watched and processed by firms via loyalty cards. Firms have the chance to form databases of their customers, particularly, customers' data of identities, addresses, expenditures, preferences, and so on. It is the fact that, simply by using these cards, ordinary people as consumers have become the subject to surveillance. Before explaining how consumers are monitored by cards in detail, it is useful to mention the fact that there is not an obligation for people to obtain and use loyalty cards.

As can be witnessed in stores, the use of loyalty cards is not compulsory; people voluntarily, according to their will, use these cards in their shopping. Firms try to make their cards attractive and inviting through several practices such as rebate and promotion. Thus, people, in order to get use of such economic opportunities, obtain and use loyalty cards; moreover, they have got different cards of different firms because they want to take advantage of rebates and promotions of all supermarkets and stores. In all stores having loyalty cards, it can be seen that a lot of items have dual prices, one of which is the current price for all customers and the other is the lower price for club-card users. Hence, in order to get rid of higher prices and to decrease their

expenditures, people ‘voluntarily’ decide to use the loyalty card of the store in their shopping.

However, such a so-called noncompulsory use of cards is basically pseudo-voluntariness. This is because “...even if the consumer knows that information is being collected, the choices are either participation or the default punishment of a higher price” (Elmer, 2003: 237). The system works as follows: whether stay outside of the system and pay higher prices or participate to the system and utilize promotions. In this regard, it can be claimed that firms implicitly asks their customers making them to be under surveillance for some economic benefits. In other words, power includes individuals to the functioning of the surveillance system not through coercive means, but through such economic rewards. As mentioned by Whitaker (1999: 141), “the Panopticon rewards participation”. If you are the part of the system, or say, if you just consume and are obedient and faith to the power, you will be rewarded. In this manner, “firms reward consumers those in the surveillance process through such as rebate” (Elmer, 2003: 232) in order to make them not to question and challenge the functioning of the monitoring practice.

4.2.1 THE FEATURES AND FUNCTIONING OF LOYALTY CARDS: HOW DATA ARE COLLECTED AND USED

As mentioned above, customers get and use the loyalty card of a firm willingly in appearance; more concretely, there is not an obligation of being a card owner. But, a hidden obligation, thus, pseudo-voluntariness, takes place

through providing commercial benefits such as rebate to the customers who have and use the loyalty card. In spite of such an “illusion of voluntariness” (Davies, 1998: 237) pointing out this incentive to ‘opt-in’, consumers do not have a complaint about the surveillance of their transactions. Moreover, they are pleased and satisfied of achieving several benefits obtained through using the card, such as promotions in their shopping, loyalty drawings in certain days, gifts sent to them by firms in special days as New Year’s Day or Mother’s Day.⁵⁹ Such policies pursued by firms conceal the surveillance potential of loyalty cards. This potential is more considerable and useful for firms other than the aim of satisfying consumers.

It can be useful to point out clearly how surveillance mechanism works in the stores in order to make clear the structure and functioning of loyalty cards and the relation between consumers and the firms. The monitoring process starts with filling out the membership form of the loyalty card; each firm has its own application form and determines the content of it. They want their customers to give necessary personal information. There are common points in the forms of all firms: Membership forms of Praktiker (Appendix B.1), Migros (Appendix B.2), Money Card (Appendix B.4), CarrefourSA (Appendix B.5), Beğendik (Appendix B.6), and Öğütler (Appendix B.7) ask questions to the customer about his/her name, sex, address, phone number, marital status, occupation, and income. Besides, through the form, companies also aim to get information about whether the customer has his/her own house or car. In addition, hobbies and preferences are aimed to be learned via the application form; for instance, Praktiker (Appendix B.1) and CarrefourSA (Appendix B.5) ask their customers which fields (bathroom, garden, construction materials, electronics, decoration, etc.) they are interested in. Here, one can ask why the firms concern on my house or car or my interests. The answer lies on the fact that firms aim and want to get all information about

⁵⁹ From the interview with Beğendik, Ata

their customers in order to form customer databases. By this way, firms can classify their customers in various segments, such as those having their own houses, those with an income above a certain limit, and those interested in electronics. Firms, accordingly, follow differentiated policies, specific promotions, and targeted advertisements to various segments of customers. This case is going to be discussed and analyzed more in the following pages under the heading of the ‘manipulation of consumers’.

All these data filled out by customers are recorded by officials of the firms in their computer systems. Every new membership form filled out by customers is registered to the database system in a single or in a few days.⁶⁰ By this way, all current personal data of every customer who have the club card of the firm can be seen in a few seconds. The managers can easily learn how many married customers they have, how many customers with children they have, how many customers of them have high incomes to buy expensive products, and so on. In addition, firms can also get information on the fact that which branch offices of the related firm have more customers and that which stores sell certain products more; for example, which stores sell mostly vegetables, or cosmetics, or electronics, or luxury goods can be learned by managers.

Furthermore, although these data are necessary, they are not enough for the firm to monitor and analyze the needs, preferences, and habits of the customers. In order to maintain this, firms need to track all daily and periodic expenditures of customers. While the first stage of the surveillance of consumers is the membership form of loyalty clubs, the second one is the use of these cards in counters. In order for firms to monitor consumers, loyalty cards have to be scanned by the reader equipped in the counter. When the

⁶⁰ This is explicitly declared in the interviews made with Ögüt, Ömer, the Director of Computer Center of Öğütler, and with Yıldız, Şebnem, the Director of Beğendik Club Card Department.

customer comes to the counter to pay the price of the items he/she buys, first he/she gives his/her loyalty card to the cashier, then the products inside the shopping basket.

Abovementioned customer information maintained in the commercial field can be classified under four types of data: geographics, demographics, psychographics, and consumer behavior (Goss, 2002:174). Geographics include region, market area, address, and population density; demographics include age, sex, income, occupation, education, and housing status; psychographics include social class, and lifestyles; and, finally, consumer behavior include usage rate, loyalty, and attitude to specific products. All these data take place in databases of the firms.

Through analyzing these data, managers of the firms can identify the customers and track their personal and transactional data. Not only amount of their expenditures, but also all products they buy exist in the system. Hence, the managers can monitor data of customers, such as name and address of customers, their frequency of shopping, their amount of expenditures daily, monthly or annual, which stores they frequently do shopping, all the products bought by them, certain items and brands preferred by the customer, and so on. By this way, each firm has formed its own database in which their customers and customers' data are stored and processed. Every time the customer uses his/her card while shopping, new information related to the customer are added to the database.

During my interviews, I have witnessed and examined roughly the customer database of Öğütler.⁶¹ When a name or membership number of a customer is typed up in the system, personal information and all transactional data of the customer are watched in every detail. All products he/she has

⁶¹ From the interview with Ögüt, Ömer, the Director of Computer Center of Öğütler

bought in a specific day and during a period can be seen on the computer screen of the manager. Another feature of Ögütler card is that not only managers but also the customer can also watch his/her transactions via the website of the firm⁶² through entering his/her customer number and password given by the firm. Other firms do not have such an application; they only see data of their customers themselves as a form of centralized data storage and processing. In the case of Ögütler, the question of whether the third parties such as hackers can get the database of the firm stored in the Internet remains unanswered. Firms, whether shared with customers or not, collect and store personal and transactional data of their customers only if they use loyalty cards while paying the price of the purchase.

However, what happens if the customer does not use his/her card while paying the price of the shopping basket? The answer is simple: no data concerning the customer can be gathered. Only data achieved are the amounts and types of products sold during the working period. This is a problem for the firms because they want more data in order to rationalize their activities. Therefore, they intend to make their customers use their cards constantly. To achieve this, they seduce customers through providing economic benefits such as discounts and promotions.

The most common tool is the dual-pricing strategy. All firms I researched (Migros, Koçtaş, CarrefourSA, Beğendik, Ögütler, Praktiker) have dual prices in certain items. Dual pricing is in practice in all stores having loyalty clubs without exception. Daily or weekly discounts are applied to different products. By this way, people regard loyalty cards as useful and profitable for their budget. Because different items are in discount in different days, customers are forced psychologically to use the card in their every

⁶² <http://www.ogutler.com.tr>

shopping. In addition, firms give much significance to this policy which results in the being a member of the loyalty club and in the use of the cards regularly.

Unlike other supermarkets, Praktiker carries out differentiated prices not only among those who have the card and those who have not, but also among existing card users through considering their amounts of spending. A new member of the Praktiker card has a Classic card. When his/her annual expenditure has reached 4.000 TL, his/her card turns into a Gold card; when exceeds 10.000 TL, the card becomes a Platinum card. Every new card has more advantages than the previous one. Likewise, Gold-card users obtain more discounts than those having Classic card, and higher rate of discount is provided to the Platinum-card users than to the Gold-card users.⁶³ This means that the more you spend, the less you pay than the other customers.

Furthermore, obtaining points after every shopping is another practice pursued by firms. Customers, only if they use their loyalty cards, get points determined according to the amount of their purchases. These points are used as money stored inside the loyalty cards; when points reach to a certain amount, the customer can buy products with their points. Points used by customers mean free-of-charge shopping.

All firms I have researched provide this benefit to their customers. Customers of Migros, for example, get points through their expenditures which are called as “Paropuan”. The customer can spend his/her Paropuan whether in Migros or in other firms of Paro program as Opet, Ford, Burger King, Koçtaş, etc. whenever and wherever he/she wants. It is seen that customers regularly control the amount of their points and spend them from time to time.⁶⁴ Although there is a free-of-charge shopping in the eyes of customers, firms do

⁶³ From the interview with Demiroğlu, Ülkü, from the Customer Relations of Praktiker

⁶⁴ Customers learn their points via through the websites of firms and from counters. In addition, customers of Migros can learn it via ‘kiosk’ located in the stores of Migros.

not regard this case as a sale free of charge. Moreover, managers regard points as new sales. They think that “giving 5% of the purchase as a point to the customer means selling this amount of several products to this customer”⁶⁵. Thus, this does not lead to a loss for the firms. In contrast, it results in not only the maintenance and enforcement of loyalty between the customer and the firm, and but also the selling of more products. There occur more sales because whether or not the customer needs to buy anything, he/she does shopping in order to spend his/her points rather than spending the money inside his/her pocket.

Another notable feature of the loyalty cards is that consumers give written or implicit consent to the surveillance of their transactions. Such a statement may be considered incorrect or unbelievable at first sight. One can ask why a person gives consent for being the subject to surveillance. However, the fact is not simple as such.

All firms use printed membership form to be filled out by the customers in order to get and benefit from the loyalty card. When the customer signs the form, he/she accepts all the statements and conditions written on the form. Moreover, there is not a possibility to reject the terms of the form. It is a pre-acceptance without any way of rejection or challenge. It is accepted by the customers that firms can monitor and process the transactions of him/her.

In the membership form of Praktiker card, it is written that “I give permission that content of my shopping can be watched by Praktiker” (Appendix B.1). And the customer is wanted to sign this form without rejection. Likewise, in the membership form of all Paro program companies, there is a part with a title of “Declaration of Membership and Consent”. According to the terms written under this title, the customer accepts their

⁶⁵ Form the interview with Beğendik, Ata

personal data to be collected, processed, and shared with other firms of the Paro program (Appendix B.3). For example, if you have the Migros club card, it means that you are also the member of the Paro program; thus, your personal data, your transactions, and analysis of your shopping details are shared with firms in the Paro program such as Koçtaş, Arçelik, Aygaz, and Sarar.

Furthermore, CarrefourSA is another firm that gets permission and consent of their customers in the collection and storage of their data. According to a sentence on the membership form, the customer gives permission that CarrefourSA can share all his/her personal information with other people and/or companies (Appendix B.5). The similar case is seen in the membership forms of Money Card (Appendix B.4) and Praktiker (Appendix B.1). The critical point, here, is that the customer has no option to reject the case of being monitored. In the abovementioned three forms, the firms do not ask whether the customer accept the surveillance or not with a ‘yes-no’ question; but they, in a manner, force customers to be the subject of the continuous surveillance. The rejection of being monitored means the rejection of using the loyalty card of the firm.

The customer has two options while filling out the form: whether he/she signs the form and accepts the terms which result in customer’s being monitored or he/she does not sign the form and does not get the card. In this case of a choice, in order to achieve economic benefits of the cards and through considering their budgets, consumers tend to sign the membership form and make their data be monitored, stored, and processed without questioning the functioning and characteristics of the loyalty card.

As mentioned by Van den Hoven and Vermaas (2007: 285), “the main moral principle in the area of personal data...is the principle of informed consent”. However, we cannot witness informed consent in getting and using the loyalty cards. On the contrary, here, there occurs a compulsory consent due

to the fact that customers do not have the chance to opt-out of being monitored while at the same time using the card and utilizing its benefits. To reject the terms and conditions of the loyalty card means to reject using the card and, thus, to be devoid of economic benefits as discounts. On the other hand, while the abovementioned firms (Migros, Praktiker, and CarrefourSA) get the permission of customers (however, this is not an informed consent in which customers are well-informed about the whole process) to collect and process transactional data of them, other firms (Beğendik and Öğütler) collect data of card users without any written information about the existence of surveillance capacity of their loyalty cards on their memberships forms.

Although there is not a statement on their forms about customers' giving permission to the surveillance of their transactional data, they also collect, store, and analyze transactions of their customers. Every single item bought by the customer is recorded in database as information about him/her in order to be used by firms for commercial purposes as profit maximization and administrative purposes as efficiency and rationalization. How firms use these data to control and manipulate the choices and needs of consumers requires particular interest.

4.2.2 MANIPULATION OF CONSUMERS

One of the main processes in dataveillance by firms is the attempt of “sorting between customers who are worth pursuing and retaining for their business and others who are unprofitable to the corporation” (Lyon, 2007:

186). Sorting is one of the basic features of surveillance. Thus, in the commercial field of surveillance, firms sort their customers according to their several data such as income, frequency of shopping, amount of expenditure, and specific products bought.

Likewise, Gandy (1993) mentions “the panoptic sort”, which points out the sorting of people according to their data. As mentioned by him, three stages are pursued in the comparison of individuals with others: identification, identifying individuals in their personal data; classification, involving the assignment of individuals to conceptual groups on the basis identifying information; assessment, representing a particular form of comparative classification (Gandy, 1993: 15-17). In applying these stages in the process of dataveillance, we can point out the working of the system as such: At first, data of customers are collected and stored in databases; by this way, personal and transactional data can be seen and tracked. After the collection and storage of consumers’ data, firms make classifications and categorizations among customers through taking into account their incomes, purchases, choices, and so on. Besides, analyzing these data in order to compare customers with others is another stage of dataveillance.

With the classification and analysis of customer data, firms have the necessary information to make advertisements in order to influence, persuade, and even seduce them. This is basically targeted advertising provided to certain segments of customers. In Praktiker, for instance, Classic-card users, Gold-card users, and Platinum-card users, which are classified according to the amount of their expenditures, are informed about different promotions and campaigns via messages and e-mail.⁶⁶ But, the categorization and targeted advertising do not go beyond. That is to say, several segments of customers are not formed according to their choices, preferences, and consumption habit; and, thus,

⁶⁶ From the interview with Demiroğlu, Ülkü

various campaigns are not provided to such differentiated segments of customers. In other firms, as mentioned by the officials in interviews made with them, they do not categorize and classify their customers; they present same promotions and advertisements to all customers using loyalty cards.

On the other hand, this surveillance system has such a technological structure that it gives the firms the opportunity to sort and categorize each customer among others and to pursue targeted advertising in accordance with types and content of their transactions.⁶⁷ Some examples can be given as follows to clarify targeted advertising: If a customer regularly buys cosmetics, the firm can make a promotion on, such as, a certain brand of lipstick or perfume only for that customer and notify the customer via communication means. Likewise, if a customer generally prefers to buy a certain brand in shopping, the firm can notify the customer when a new item of that brand has been produced.

Such examples point out the targeted advertising or promotion for specific segments of customers, accompanied by a tempting offer or privilege. This case is defined as “categorical seduction” by Lyon (2001). In addition, Webster (2006) terms another form of surveillance and control of segmented customers as “categorical exposure” in order to mention the comprehensive functioning of surveillance technologies and of advertising in that they give no chance other than to behave and live according to the conditions submitted to them. Thus, companies, as a power holder, provide a consuming and living sphere to the individuals, to the consumers, in which they are under the constant surveillance and control of power through technologies as loyalty cards and several tools as advertisements or promotions functioning to surveil, manipulate, and control the individuals.

⁶⁷ From the interview with Beğendik, Ata

Policies as discounts, promotions, lottery drawings, and advertisements clarify the fact that consumer data are increasingly "...valued and sought as a means of creating customers for products" (Lyon, 2004a: 140). In order to sell their products, firms intend to manipulate and seduce customers concerning their choices, preferences, needs, and habits. Generally, people tend to buy a product only if they need it; however, their demand and choice of certain products and brands can be manipulated through advertisements, promotions, and discounts. For example, if a customer regularly buys biscuit rather than chocolate, the firm can hardly or never make the customer buy chocolate. But the firm can make a targeted promotion to seduce the customer that a packet of biscuit and a packet of chocolate can be sold combined with a special discounted price. In addition, the firm, through advertising, can aim and try to make him/her buy a certain brand of biscuit or buy biscuit more frequently via specific advertisements or promotions; for example, if the customer buys two packets, the third packet would be half-priced. Therefore, it is true that "advertising does not create demand...but molds it and steers it in certain directions that work for the benefit of producer" (Jhally, 1990: 15).

Under the influence, manipulation, and seduction of advertising and other forms of persuasions, consumers do not largely make their own choices and take their own decisions in shopping. In most cases, real choices of consumers do not take place. Dickson (1974) makes a distinction between real choices and apparent choices. He discusses that the apparent choices of, for example, a car, appears in relatively unimportant items, such as shape, color, or texture of car seats whereas the real choices, such as price, mechanical reliability or ecological impact are obscured and lie outside the control and choice of the consumer (Dickson, 1974: 88-89).

Similarly, the consumers, today, do not need to or do not have the chance to question the price and content of the product, how it is produced, or

whether it is ecological friendly, which comprise real choices. However, Dickson's consideration on apparent choices which are regarded as under the control of the consumer has changed with today's technological developments. That is to say, corporations aim to control and direct all choices and preferences of consumers not through, of course, coercive means, but through persuasion, influence, and seduction achieved especially via advertising and promotions by firms.

According to these issues, it can be claimed that consumption which is dealt with consumer is not determined and shaped by solely the consumer himself/herself. But, as stated by Marx (1971), production produces not only the object and the manner of consumption, but also the desire for consumption. And corporations carry out surveillance technologies and other following policies, mentioned above, in order to control, direct, and manipulate their choices, needs, and desire for consumption.

These all abovementioned considerations present us Marcuse's (2002) "one-dimensional man" in the contemporary society, whose behaviors and actions are manipulated, directed, and controlled by power, and who choice and consume only that which is given to him/her. In Marcuse, one-dimensional man lost the ability to dissent those provided by power and to control his/her own decisions and actions. One-dimensional man, within the framework of this study, has come into being through effective and comprehensive functioning of surveillance and control technologies.

Regardless of the fact that they really need to buy a certain product, consumers are influenced and manipulated to do shopping through several advertisements, discounts, and promotions applied by the firms. For example, if a certain product or a certain brand of a product in the supermarket is rarely bought, the firm has the power and tool to analyze the database of their loyalty-card users and identify the customers who would potentially be the consumer

of that product through monitoring their transactions. Additionally, the firm can carry out targeted advertisements to the related customers to make them buy the product; or, the firm can make a promotion specific to those customers, such as a special discount or another product, which is frequently bought by those customers, attached to the given product.

In the light of these and some other examples, we can clearly declare that consumers are manipulated and controlled by corporations through using the abovementioned technologies and techniques. Thus, most of the corporations, today, utilize surveillance technologies as chip-embedded smart cards and perform several techniques influencing and manipulating the choices and needs of consumers in order to realize their capitalist endeavors and to enhance their power. They aim and try to make consumers desire things which they do not really need; these are the false needs due to the fact that they are mainly the needs of capitalism rather than consumers (Marcuse, 2002). Unlike this reality in capitalism, consumers' free choices and real needs do not take place because their choices, needs, and living patterns are formed by those provided and presented to them by power holders.

One has to or is forced to define and satisfy his/her needs through the products presented on shelves; but, he/she has no power and chance to get full, complete, information about products. As discussed by Jhally (1990: 24), other than the complete information which involve information about how goods were made and who produced them, consumers get information about the uses of products.

Consumers give their decisions on shopping and on buying products through taking the information into consideration provided by corporations via advertisements. Furthermore, corporations do not see general advertisements addressing all consumers sufficient in persuasion of consumers; they also carry out targeted advertising and promotions, as mentioned above, to direct specific

customers of supermarkets toward specific products and to manipulate their needs and choices.

4.3 THE COMMODIFICATION OF PERSONAL DATA

Another issue that has to be considered in the discussion of loyalty cards of firms and the analysis of dataveillance is the commodification of personal data. While talking about commodification, the issue which comes into consideration at first is the selling of data from one firm to another firm. However, there is not a company only dealing with the storage and processing of personal data in the market. This statement is not valid in the cyberspace, on the other hand. The Internet gives companies more opportunity to watch internet users. This should not be reduced to merely e-commerce. “The growth of electronic commerce ... introduces cybersurveillance” (Lyon, 2001: 145); the increase and comprehensive spread of cybersurveillance over all internet users result from computer technologies, such as cookies. While some technologies as spyware and phishing work to steal personal information of individuals such as credit card numbers, cookies generally function to collect surfing habits of the individual though there are also cookies that aim to get personal data.

When the internet user visits a website, a cookie is sent to his/her computer's hard disk by the website. Cookies located in one's computer store information about surfing habits, such as which websites he/she visits and how often he/she visits, and send these data to the related company; thus, they give

extensive tracking capacity to companies in the cyberspace. Through cookies, websites can collect data on individual's actions, preferences, likes, dislikes, and needs. Some websites declare their privacy policies and inform the internet users and visitors about cookies and about information they collect. For example, Yahoo and Google announce in their web pages under the title of "privacy policy" that they transmit cookies to the user's computer so they track the websites visited by him/her, and that they do not share his/her personal data with the third parties or sell to them.⁶⁸ In addition, Yahoo, for instance, gives chance to their visitors to opt-out in order to get rid of being tracked. When the internet user downloads "opt-out" cookie, located on the page of Yahoo⁶⁹, to his/her computer, the tracking activity stops.

Other than these companies, there are also other companies only dealing with the tracking of individuals in cyberspace as a commercial activity. zBubbles, for instance, is a program that works for Alexa, a subsidiary of Amazon. This program, like other similar programs, "offers shopping advice and simultaneously collects data about the computer-user's files and surfing habits to send back to profiling and marketing companies" (Lyon, 2004b: 179). As for other major internet companies, Doubleclick⁷⁰ collects surfing data from 6400 locations in the Internet; likewise, Engage has detailed surfing profiles on more than 30 million individuals in its database (Lyon, 2001: 145). Such companies, through using particularly cookies, track individuals in the cyberspace, their surfing habits, thus, their hobbies, likes, preferences, and needs, in order to make them be under the control and manipulation of companies.

⁶⁸ <http://info.yahoo.com/privacy/us/yahoo> and <http://www.google.com.tr/intl/tr/privacy.html>

⁶⁹ <http://info.yahoo.com/privacy/us/yahoo>

⁷⁰ Google bought Doubleclick in May 2008. Since then, the company has worked under the managerial umbrella of Google.

In regard to the firms having loyalty clubs, which are considered above, along with the fact that they establish databases through monitoring their customers via loyalty cards, they declare they do not sell or share customers' personal information with other companies. All personal and transactional data of customers are stored and processed in the database of the firm, as mentioned by officials of the firms researched⁷¹. However, Paro program, which comprise loyalty cards of Migros, Arçelik, Nokia, Ford, etc. has a different structure. All data about a customer of one company, say, Migros, are shared with other Paro companies in the system. For example, Ford can get information about and monitor those who buy car accessories in Koçtaş or Migros watch data of the customers of such as Arçelik, Nokia, and Burger King. In the membership form of Migros club card, customers give an automatic permission for their personal data to be shared with other Paro companies when they sign the form in order to get and utilize loyalty card of Migros. Beside such consent, Migros, like other companies in the Paro program, also gets the consent of the card user to share his/her data with third parties without disclosing the name of the customer, according to the terms of "the declaration of membership and consent" (Appendix B.3).

In addition to such a commodification of personal data, another form of commodification takes place when the customers buy something. As mentioned by Van den Hoven and Vermaas (2007: 286), "every time they come to the counter to buy something, they also sell something, namely, information about their purchase or transaction", which is called as transactional data. To exemplify this case, it can be mentioned that loyalty card of the firm is the tool through which and the area in which a form of trade between the customer as a producer of data and the firm as a consumer takes place.

⁷¹ From the interviews in Beğendik, CarrefourSA, Praktiker, Ögütler

In order to talk about a commodity, as Marx (1971) takes into account production, consumption, distribution, and exchange as the stages of the process, the stages of production, consumption, and exchange can be regarded as the stages of the commodification of data. Personal data are produced by the individual, which are produced throughout his/her living period and are composed of likes, dislikes, needs, choices, habits, consumption patterns, and lifestyles of him/her. In addition, his/her data are not stable, but they change or become different day by day together with the changes in the life of the individual. On the other hand, the consumer of personal data of customers is the companies that monitor, collect, and store those data. In the consumption process, companies consume these inexhaustible products. They are inexhaustible because after every use of customer data, such as reducing the price of specific items sold in the supermarket, the data do not lessen or lose its value and usage.

In Marx, commodity fetishism is related to exchange value. He did not discuss mystification in the use value, but in the exchange value. This is because people do not get complete information behind the commodity; for example, who produces it, what rights are given to the workers, under which conditions they work, where and how it is produced, and whether there is an exploitation in the production process are not largely and completely known by consumers. However, in the case of dataveillance via loyalty cards, the use value of the commodity becomes mystified; the companies do not declare for what purposes the consumer data are used other than the declared purpose of efficiency. Here, the meaning of the collection of personal data in the hand and in the use of companies is not obvious for consumers to comprehend.

The use of personal data which comes into consideration at first and also mentioned by managers of the companies is the efficiency and the satisfaction of consumers. Therefore, customers expect from companies to

provide better services, to alter their policies according to the demand of customers, to submit more products, and so on. However, behind the discourse of efficiency, there occurs monitoring, persuasion, control, and manipulation of consumers according to the desire and goal of the companies and, thus, according to the will of power. This is not declared by firms as such; on the other hand, consumers are expected to believe that the collection of their data is for their benefit and is for the betterment of services provided.

The third stage in the commodity of data, as mentioned above, is the exchange process. Customers, while buying any single item, sell information on their purchases. Here, the question is what the amount paid for the sale of personal data is, or, say, what the price of personal data is. The price is sometimes a specific amount of discount in the item bought in the market, sometimes a lottery drawing got through the amount of purchase, or sometimes a gift attached to the item bought. To be more clear and in short, customers sell their personal data to firms in the exchange of some economic benefits such as a rebate or some other promotions. They see no harm in selling their information via loyalty cards in the payment for a discount in their expenditures.

Most people do not regard these cards as a surveillance mechanism, but as a discount card⁷², and do not wonder about and question their inner functioning behind the functioning of reducing the price of items. Besides, they do not, mostly, need to or waste time to scrutinize and oppose the conditions of the membership forms of the loyalty cards, through which they give consent to the collection, storage, and process of their personal data. This is because the permission is given by the customer whether through a short sentence as in the case of Praktiker (Appendix B.1), or through long sentences and items as in the forms of Paro club cards (Appendix B.3), or through a sentence in small letters

⁷² From the interviews in Migros, Praktiker, Beğendik, CarrefourSA, Ögütler

as seen in the forms of Money Card (Appendix B.4) and CarrefourSA (Appendix B.5), or through implied consent which is not written down in the form signed by the customer as in the case of other firms (Beğendik and Ögütler). Two alternative actions of a customer have come into consideration whether to use loyalty card in the payment, and to benefit from its advantages, and, thus, to sell his/her personal information, or to get rid of using the card and of being monitored in order to protect his/her information.

Through the commodification of data, individuals are included to the system of surveillance in that they have become the subject to surveillance just through using loyalty cards in their purchases. Companies make them use these cards continuously in their every shopping and sell their personal data not through coercive means, but through persuasion and seduction via economic benefits. This is to reduce uncertainty and maintain rationality, in which everything is seen and predictable, in the contemporary society.

Both visual surveillance under the name of security and dataveillance in the commercial field, particularly, are tools in the hands of power for its goals. Power holders, through using these means, want all individuals to be under their constant gaze and control. In addition, they attempt to make them be obedient citizens in accordance with the existing social order and the dominant ideology. In order to clarify this issue, structures in the legitimization of surveillance and the ideological functioning of surveillance and control are going to be discussed in the following chapter on basis of the cases pointed out and analyzed in this chapter and in the preceding chapter.

CHAPTER 5

SURVEILLANCE AND CONTROL AS A CULTURE

In the light of the cases analyzed in the previous two chapters, it can clearly be stated that in all domains of life we are monitored and controlled through several surveillance technologies. Tracking of employees, CCTV surveillance in stores, malls, buildings, and streets, biometric surveillance, and monitoring of consumers in the commercial field are some forms of surveillance and control in today's society. Managers monitor their employees and workers, school authorities their students, parents their children, police department the citizens on the streets, corporations their customers, and, to sum up, power holders the individuals in the society. These fields of surveillance have been achieved whether through visual surveillance as CCTV monitoring over the workplaces and streets, or through biometrics, or through chip-embedded smart cards.

The answer of why surveillance is carried out by institutions is the goal of seeing everything in the society and of controlling people in accordance with the well-being and effective functioning of dominant ideology, of capitalism. States, in order to increase their power, use the discourse of security, as discussed in the chapter three. Besides, private corporations, as analyzed in the chapter four, in order to increase their profits and their corporate powers,

benefits from the discourse of consumer satisfaction and manipulate consumers. It is the fact that security is the most successful discourse in the legitimization of surveillance and control. In addition to and more important than the discourses of security and consumer satisfaction, the surveillance mechanisms are put into effect to surveil and control people for the benefit of power.

That is to say, the aim is to make all people be obedient citizens or be “docile bodies”. In particular, the ‘good’ worker, the ‘good’ student, the loyal consumer, and the obedient citizen are the goals of power, which are achieved not through coercive means, but through persuasion, seduction and exposure via surveillance and control technologies. Thus, these technologies “...are employed, not to enrich human life, but to maintain the state’s surveillance and control of its slave citizens” (Staigler quoted in Murphie and Potts, 2003: 106). They are slaves not, of course, physically, but through being obedient to the dominant ideology and the all-encompassing functioning of power; they consume, behave, and live according to the criteria presented to them by power holders, whether government agencies or private corporations.

People live in such a circumstance where there is little or no objection to the tracking activities in everyday life; in contrast, they prefer utilizing the benefits provided to them rather than challenging and questioning the existence and widespread functioning of surveillance and control technologies. It is basically the target of power holders that they aim to make surveillance and control be regarded as the usual, necessary, and beneficial components of contemporary societies. This is because of the fact that people do not challenge the conditions and elements which are embedded in their private lives and in the social life.

Accordingly, surveillance is required to be legitimized in order to eliminate potential challenges and oppositions. It is possible to achieve this in

today's society because surveillance and control have been seen in the lives of people since their childhoods. That is to say, 'ideological state apparatuses' (Althusser, 2002) such as the family and the school are influential in the becoming of surveillance and control usual and natural notions in the social life. Not only in the childhood, but also in all other spheres of life, people are subject to surveillance by several institutions that function ideologically according to the will of power.

Furthermore, popular culture is another field in the legitimization of surveillance. Through TV programs, movies, and even computer games, surveillance enters into the lives of people as a common issue or as an advantageous and necessary notion. These all bring us the fact of ideological functioning of surveillance and control. Through monitoring individuals and their actions and lifestyles, power aims to reduce uncertainty and eliminate risks, thus, to maintain rationality in which everything can be predictable. Power needs compliant individuals in order to achieve its goal. However, as mentioned by Foucault (1980), there is resistance if there is suppression; thus, challenges are always possible where the individual exists.

According to the abovementioned issues, in this chapter, it is going to be analyzed the ideological functioning of surveillance and control after discussing the ideological state apparatuses concerning surveillance and control and the concept of surveillance in popular culture as sources in the legitimization of surveillance. Finally, resistance to, opposing movements against, surveillance and control are going to be dealt with in order to point out the efforts and attempts of escape from being monitored.

Under these headings in this chapter, I want to discuss the ideology behind the notion and practice of surveillance mentioned in the previous chapters. This discussion places on the ground of studies analyzed in the third and fourth chapters. Main discussion points are how surveillance and control

become embedded notions of the human life and the social life and how rationalization, social control, and domination are provided and strengthened via technologies and practices of surveillance.

5.1 STRUCTURES PROMOTING SURVEILLANCE AND CONTROL: LIFE CONTINUOUSLY UNDER GAZE

Althusser (2002) makes a distinction between state apparatuses and ideological state apparatuses, both of which work for the well-being of the social order and for the sake of power. While goals of both apparatuses are similar in that they aim to strengthen the bonds between people and power according to the will of power, ideological state apparatuses differ from state apparatuses in their functioning. The former function ideologically whereas the latter uses coercive means in the practice of controlling and recruiting people.

State apparatuses which function to monitor and control people are, for example, army, police, courts, and prisons. They use several coercive means that are based on laws made by the legislative or regulations and instructions executed by the government and bureaucracy. People under their authority have to obey the rules and regulations of these institutions. Censor and sentence are two of the coercive measures pursued by these institutions. Besides, as analyzed by Foucault (1977) in his study on Bentham's Panopticon, confinement is another tool in disciplining and training the individuals and masses. Not only the prison, according to Foucault, but also the army, the factory, the school, and the mental hospital attempt to discipline and reform the

inhabitants of these institutions through confinement. The Panopticon, according to him, "...serves to reform prisoners, but also to treat patients, to instruct schoolchildren, to confine the insane, to supervise workers, to put beggars and idlers to work" (Foucault, 1977: 205). Here, Foucault's consideration on the Panopticon involves soul-training; that is to say, fields of Panopticon instill the feeling of being continuously monitored into the conscious of individuals who are subject to confinement, and, accordingly, people under constant gaze by the guards or other authorities have to control their actions and behaviors due to the eye watching them at any time.

The turning point in this issue is that Foucault's notions of confinement and disciplinary measures, which work coercively, have left their places to the notion of "continuous control" and "instant communication", which are suggested by Deleuze (1990), in monitoring and training people without any physical enclosure. Other than the institutions of confinement in Foucault and the state apparatuses in Althusser, there are also institutions, which function ideologically and attempt to surveil and control people in all fields of life without measures as confinement.

Althusser's ideological state apparatuses are influential and determinant in the legitimized and unchallenged practice of surveillance and control in the society. Althusser mentions the family, the school, the workplace, and the media as the structures which give priority to ideology in their functioning to control and train people in accordance with the will of power.⁷³ They work to indoctrinate the individual and the masses with the fact that surveillance and control are usual issues and are necessary and beneficial in contemporary society. They function to make the practice of surveillance and control be

⁷³ Althusser's ideological state apparatuses are not, of course, limited with these institutions. He discussed these apparatuses in the fields of religion, education, family, political parties, unions, communication as TV, and culture as art (Althusser, 2002: 33-34). Certain structures, but not all, are taken into account in this study to analyze surveillance and control in the social life.

acceptable, desirable, and unchallengeable in the social life. Thus, it can be claimed that these institutions are affective in the legitimization of surveillance and control. Besides these mentioned institutions, other structures that have to be taken into account in this context are in the commercial field, the mall and the supermarket; they have a role and an effect in the placement of surveillance and control into the daily lives of people.

In the light of the discourse that people rarely or never challenge or oppose the circumstances and the elements in which they grow and live, surveillance and control are aimed to exist and function in every part of their lives. It has to be stated that the practices of monitoring and control are not recent issues and are not peculiar to the current society. Throughout the history, children grow under the control of their parents and the school; furthermore, people are subject to prohibitions and punishments of legislations, religions, traditions under the name of being a good child, good person, and good citizen. What is at stake in contemporary society is that surveillance and control are technology-laden and are less visible and not coercive.

Children, today, for example, grow in an environment surrounded by surveillance cameras. Thousands of cameras begin to watch them when they leave their houses. Not only streets, but also parks, metro stations, airports, malls, and inside and outside of buildings and stores are places where children, like every person, face with and are subject to cameras and eyes behind these cameras. On the other hand, technological surroundings concerning surveillance and control around children are not limited with cameras.

One of the most significant structures benefitting from other surveillance technologies in the formation of the culture of surveillance and control is the family. “Massive socialization begins at home and arrests the development of consciousness and conscience” (Marcuse, 2002: 250). There occurs less or no way for children to question the life and conditions in which

they grow. Parents, in order to control and train their children, always want them to be under their gaze. In this wise, new technologies give them the chance to watch their children even at a distance. To put it differently, children are subject to parental surveillance via new technologies, which are called as “electronic leashes” by Gary Marx (2005). “There are locational technologies that use GPS (Global Positioning Systems) and GIS (Geographic Information Systems) in conjunction with wireless telephony providing much more powerful potential” (Lyon, 2003: 17) for the use of parents. Through such electronic leashes, parents have got the means of checking where their children are.

Parents do not only have the tools to monitor physically their kids, but also have tools to track transactions, consumer behaviors, and preferences of them. This issue can be exemplified through the smart card used at METU College. As explained by Şahin, all students at the College use the cards given to them by the school in their payments in the canteen and cafeteria. All purchases made by them are recorded in databases and shared with their parents. In this manner, parents have got the chance to get information on their kids’ expenditures and, thus, consumption patterns. Thus, they can control and train their children, according to their own criteria.

Surveillance that children face with is not limited with the experiences of cameras surrounding them and electronic leashes in the hands of their parents; the school is another structure in the practice of surveillance and control. School is the apparatus which indoctrinates the students with functioning of dominant ideology, of power, under the discourse of being good student and good citizen. In the light of such an Althusserian consideration, it can be mentioned that surveillance and control in schools function both materially through compulsory RFID tags and smart cards monitoring students,

and ideologically through the indoctrination of the thought that surveillance and control are common and ordinary issues in human life.

Becoming an adult or graduating from the university or lesser degrees leads to another institution's entering into the life of the individual. Whether in a factory or in an office, he/she cannot escape from managerial control. The managers tend to use several measures, such as face-to-face control, which decreases due to new technologies, cameras, and software programs tracking web surfing and e-mail traffic of the employee. Besides, smart cards are another device to monitor his/her actions, activities, as well as his/her expenditures, as in the case of smart cards at METU, which are used by all employees within the boundaries of the campus.

Apart from the family, the school, and the workplace, there is another structure which exists in every period of human life, similar to surveillance cameras in every field of social life: the media. The media function to legitimize the widespread existence of surveillance technologies in all spheres of life through their news and programs, as stated in the third chapter within the context of MOBESE cameras in Turkey. Almost all Turkish TV channels, after a terrorist attack, for example, broadcast the records of cameras or declare that the criminals are going to be identified after analyzing the MOBESE records in order to imply that street-surveillance cameras are very effective and notable policing tool in the struggle against crime.

In this manner, it can be declared that the media are the place of the manifestations of power. They function ideologically according to the will of power. Surveillance and control technologies are presented as necessary and beneficial through the broadcastings of television. After almost every crime, such as robbery, mugging, or terrorist attack committed in a store or in a public place, images and records of cameras are broadcasted via televisions and also the Internet to the masses so that people would think there are all-seeing eyes

watching us anywhere and anytime. Such broadcastings function to make people think that surveillance devices are everywhere, perform continuously, and capture every single item. Thus, besides their function of monitoring and detecting criminals in order to maintain security and promote public safety, surveillance cameras' "social ordering strategy" (Coleman, 2004) is also influential and important. Power, through the abovementioned ideological functioning of the media, makes people control their actions and behaviors owing to the idea and feeling of potentially being monitored constantly by all-seeing eyes located everywhere in order to form compliant individuals in harmonious with the will of power.

The mass media, namely television channels, newspapers, and the Internet-based media, present to the public "...the centralized formation of opinions and styles of behavior" (Williams, 2005: 4). Television, through its broadcastings, has an effect in the adjustment and even in the manipulation of behaviors and opinions of the masses and, thus, in the legitimization of surveillance technologies. While surveillance is a tool to control individuals and the masses in the hands of power according to its will, ideological functioning of television inculcates to the viewers the thought that surveillance is necessary in the struggle against crime and that surveillance works for our security and public safety.

In addition to abovementioned structures, malls and supermarkets are one of the most notable areas which train individuals to accept the existence of surveillance as a common issue. This is because malls, especially, are the places not only of shopping, but also of entertainment, meeting, and wandering of people in the current society. A lot of people spend much of their time - when they have leisure time or when they need to do shopping or when they just want to kill time- in these places. Several surveillance techniques have come into being together in these commercial areas.

Surveillance mechanism, here, starts with the guards, who are located at the entrance and in certain points of the mall and the supermarket and who are continuously watching individuals and are also checking their bags. Furthermore, cameras installed in various points of the mall are another eye on individuals. Moreover, supermarkets, whether inside or outside a mall, have another monitoring tool, the loyalty cards, monitoring all transactions of individuals using the cards. People do not see any harm in the existence of such tools against their private life, personal information, and privacy; on the contrary, they continue living under the surveillance of them without any challenge or objection, and they get used to these surveillance technologies whether under the name of privacy or of consumer satisfaction.

After abovementioned analysis of the role of structures functioning ideologically according to the will and benefit of power, it is useful to discuss the role and function of popular culture in the legitimization of surveillance. This is because of the fact that it implies the advantages and benefits of surveillance and control to the masses and that it has a considerable effect in “controlling individual consciousness” (Held, 2007).

5.2 SURVEILLANCE IN POPULAR CULTURE

Popular culture, through movies, TV shows, series, and even games, leads to the emergence of individuals who are subject to the indoctrinations of dominant ideology, of power; this is because popular culture introduces standardization and pseudo-individuation to human life (Horkheimer and

Adorno, 1996). To clarify, products of popular culture present us standardized forms of opinions and lifestyles which are imposed according to the will of power. As also pointed out by Marcuse (2002: 52-53), “a rising standard of living is the almost unavoidable by-product of the politically manipulated industrial [or, say, information] society”. Power wants individuals and the masses think, decide, and live in accordance with these standard forms. To concretize, in almost all TV series, for example, in Turkey, the existing social relations, the existing relations of production, the specified function of woman in the society, the superiority of social order over liberties and over challenges are broadcasted and presented in the same manner, in the viewpoint of dominant ideology. Furthermore, such indoctrinations of popular culture “...impede the development of autonomous, independent individuals who judge and decide consciously for themselves” (Held, 2007: 106). This case is the cause of pseudo-individuation which means that the individual is open to the manipulation of the popular culture, thus, of power. Besides, this is the individual who does not criticize, challenge, and/or question these manifestations of power which function to create obedient people.

In addition to such outcomes of popular culture, it also has an effect and function in the “production of consent” (Hall et al, 1978). In order to get the consent of the masses, fields of popular culture function ideologically in the legitimization of surveillance technologies. In movies, TV shows, and series, several surveillance techniques are used in order to present that these techniques are usual issues in the current society and that people can potentially be tracked at anytime and anywhere. Mathiesen (2006), in this issue, points out another notion in the discussion of panopticism concerning the media: synopticism. While panoptical surveillance means that the few watch the many, synopticism means that the many watch the few. He mentions that the media have this synoptical structure through which manifestations of the few, of power, are reached to the many. In this context, reality TV shows are

one example where synopticism is witnessed. The masses watch behaviors and even personalities of one or more individuals. Thus, as declared by Mathiesen, we live in “the viewer society” where the many see the few. Mathiesen takes into account the complementary relation between the media and the surveillance technologies; he sees the functioning of the synoptical surveillance, of the programs via the media as “means or potential means of power in society” (Mathiesen, 2006: 48).

There are reality shows on the TV, the examples of the viewer society, which are designed on the basis of the practice of surveillance. Various formats of Big Brother in various countries are one of the basic examples concerning reality shows in which viewers watch all actions, behaviors, speeches, and, thus, personalities presented to them. For instance, TV shows as various Big Brother programs in different countries, such as “Biri Bizi Gözetliyor” in Turkey, portray, in a way, the relation between the mass media and the concept of surveillance. They all imply us that surveillance is a natural and usual phenomenon in the human life and in the social life, that it does not erode privacy as seen on the screen, and that there is no reason to question the existence and functioning of the surveillance practices in our actual lives.

Similar case is also seen on TV programs, the so-called reality programs broadcasted during the daytime, which present private lives and personal problems of individuals and families. Such programs and viewers’ excessive interest on them introduce that this form of surveillance is similar to neighbor surveillance witnessed in all societies. People, interested in the lives of their neighbors, accordingly, show great attention to these programs. In this respect, there occurs the notion of “scopophilia” (Lyon, 2006a), or, in particular, the voyeur gaze, which means the love of looking. What is the difference of today’s scopophilia in the case of synopticism from that in previous times is its technology-intensive feature; the boundaries of

neighborhood gaze have extended so much that people can witness private lives of other ordinary people via the mass media.

Besides, surveillance of crimes is another form of TV reality-shows. In the USA, as studied by Doyle (2006), TV formats as Crimestopper and reality series as Crimewatch, Crime Beat, Eye Spy, and Police! Camera! Action!, have considerable and affirmative effects on people's approach to the practice of such as surveillance cameras. These and other reality-shows mentioned above have an effect in the surveillance's extensive penetration into our lives in that people are ensured to regard surveillance as a usual and unchallengeable element of the current society.

“Reality TV accustoms the audience to perpetual surveillance and self-surveillance and contributes to the installation of ideological norms within each subject. Knowing that everyone is potentially being observed by surveillance cameras and therefore taking care to monitor behavior so that it conforms to the norms expected in the normative culture represented by reality TV program discourse amounts to the internalization of surveillance” (Bignell, 2005: 136).

This internalization paves the way for the consent of the masses to the all-encompassing practice of surveillance and for its legitimization.

People's giving consent to and the legitimization of surveillance is also tried to be maintained extensively through the movies. Movies, as one of the leading areas in popular culture, treat the subject of surveillance tools in the fight against the crime and also the subject of the surveillance as a common element in the society. Out of Turkish movies, Mustafa Altıoklar's *Beyza'nın Kadınları* is an example using the MOBESE cameras in İstanbul. In the movie, the police captain watches the images of MOBESE cameras and analyzes the records of them in order to find the suspect. It is shown that MOBESE cameras

monitoring the streets of İstanbul is an effective tool against criminals and suspects. The presentation of cameras for security is largely seen in Hollywood movies. They, in this context, designate that the surveillance cameras are essential and beneficial devices working for the benefit, the security, of the people. David Fincher's *Panic Room*, for instance, is one of them. The movie is about a privately-owned CCTV system in a house, used by the inhabitants against potential criminals, such as thieves. Surveillance cameras, in the movie, are built in order to see every part of the house. This is a movie declaring the place of surveillance tools in our private lives.

Another movie dealing with not only surveillance cameras but also other various surveillance technologies against criminals is Tony Scott's *Enemy of the State*. It does not about the private use of surveillance devices, but about -as understood from the name of the movie- the use of surveillance against a so-called enemy of the state. In the movie, the guilty -according to the evaluation of the authorities- are tracked through several technologies, namely, CCTV cameras with face recognition software, locational technologies as satellite monitoring, and other various tools. In addition, public surveillance used for the detection of criminals is also witnessed in Joel Surnow's and Robert Cochran's *24*, a TV series. Surveillance technologies from CCTV cameras to mobile phone records and to satellites are presented as the tools beneficial for the well-being of the society.

Paul Greengrass's *The Bourne Ultimatum* is another movie in which surveillance cameras and other tracking devices are tools against crimes, criminals and are tools in the establishment of social order in the hands of authorities. In the film, Jason Bourne, the suspect in the eye of watchers, is followed through surveillance cameras in several cities and places in these cities in order to find out his/her location and to get information about his/her actions. More broadly, the film shows that any individual can be followed

through surveillance cameras in public places such as train stations and even the streets. The current case and use of cameras are described explicitly in the film: Their use is mostly defined as the means of struggle against crimes, criminals, and suspects. In addition to such a policing measure, these surveillance devices also work to enhance social order and to maintain a society and individuals in harmonious with the existing order. Authorities expect people to control and adjust their acts, behaviors, and even thoughts while the eye of power is on them. This expectation results from the surveillee's "fear of the panopticon" (Foucault, 1977) due to his/her permanent visibility driven by Big Brother, that is, by power holders. Such films point out that authorities, more concretely, watchers, use surveillance technologies, particularly, cameras, to find out and track so-called suspects. Here, there occurs a tendency that one should not worry about these technologies unless he is guilty. However, the misleading point is that fear society is emerging in which individuals are worrying that every action of them are potentially under surveillance and control. This is the steps of total surveillance society which is depicted by Orwell.

In regard to this issue, Steven Spielberg's *Minority Report* goes further than abovementioned movies. It describes a total surveillance society in which all people are under constant surveillance and control. And authorities want to control the future in addition to the current time. While potential crimes are foreseen by three psychics called as precogs, every current action of individuals is seen by authorities through, for example, iris-scanning devices. These devices, located everywhere such as on the subway, have the capacity to identify all individuals. Iris, thus, has become the ID of the individual, which means that one's escape from tracking is only possible through removing his/her eyes, as witnessed in the movie. In addition, as presented in the movie, people continue their daily lives with iris trackers all around the city as if these devices are natural parts of their lives; for example, they are iris-scanned for

identification not merely in workplaces, public transportations, or official buildings by biometrics-equipped cameras, but also in their own houses by spider robots at any time. The issues handled in this movie can be regarded as the signs of an Orwellian State, in which the Big Brother has a considerable and effective technology and power to spy on their citizens everywhere and every time, and to control them constantly. Here, it is implied that people feel themselves weak and desperate against the surveillance and against the power behind the surveillance structure. In the movies, surveillance system which has an all-seeing and all-knowing power is not only the fact of the science-fiction, but is also presented as the realities of our daily lives. Such and other several movies, TV shows, and series imply that surveillance exists in the current society for public safety and for the benefit of all people. Live safety through surrounded by cameras and live safety under the constant surveillance of power, in short, live “safety in prison” (Goldsmith, 2006). Besides, they also imply that living with surveillance devices around us is not an exceptional case of the human nature, but is a usual condition of the current society.

Another form of surveillance is that the computer games provide an opportunity for individuals to explore and experience surveillance. One of the most common games is SimCity, created by Will Wright. Users of various formats of the game around the world have the power to design a city, in which everything is decided by users. They watch, control, and direct every action of Sims (the name of the citizens in the game). Besides, users can also design a house and a way of life inside the house, through which everything concerning the private life of game characters is watched and determined by the designer. In this “simulation of a surveillance-and-control society” (Lyon, 2001), users become surveillers rather than surveillees and they experience the fact of being an all-seeing eye that watches and controls everything in the society. Related with this issue, Lyon (2001: 52) asks a question whether there are really godlike operators in our lives who can control the city and people through

using a mouse and a keyboard. This question can be answered through referring extensive surveillance technologies in our lives from computers, surveillance cameras, and telecommunications to satellites, smart cards, and biometric methods. The answer, in my opinion, is that there are godlike watchers which tend to rationalize the social life through monitoring all our actions and data via these technologies in order to ensure social control and domination of power over the society.

What happens finally is that the status quo is reinforced, potential objections and challenges are minimized, and self-control of people due to the fear of the all-seeing and all-knowing eye is maintained through the effective functioning of the products of popular culture. They “...serve to enhance political control and to cement mass audience to the status quo” (Held, 2007: 88) through “controlling individual consciousness”. Through the effective functioning of not only popular culture but also other institutions in the social life, surveillance and control have introduced our lives as usual, natural, and routine elements of human life and of contemporary society; thus, it has become a culture in our lives.

5.3 POWER AND THE IDEOLOGICAL FUNCTIONING OF SURVEILLANCE AND CONTROL

Surveillance is performed whether by government agencies or by private corporations under the names of, respectively, security and consumer satisfaction or service improvement. While the former uses surveillance

cameras and biometric methods, as explained in chapter three, in order to maintain security, private corporations, specifically, stores, as exemplified in chapter four, employ smart cards to increase the satisfaction of their consumers. What lies beneath these goals, that is, the ideological functioning of surveillance and control, is the main point of discussion. As also seen in the aforementioned chapters, surveillance and control technologies, in the hands and in the service of power, have become a tool to control the individual and the masses.

Power holders, in the current society, aim and endeavor to maintain rationality in that everything can be predictable and, thus, uncertainties and risks in the society can be reduced. Power wants to know "... not only what you are doing or saying, but also [and more significantly] what they are likely to do or say next" (Lyon, 2001: 56). In order to get rational decisions concerning the government of people, power holders need to know what is happening in the society, who the citizens are, what they are doing, and what they will potentially do. It is an essential feature of rationality for power to maintain or strengthen its domination over the society.

In this sense, through using new technologies extensively in every field of life, technological rationality is achieved, which "...reveals its political character as it becomes the great vehicle of better domination" (Marcuse, 2002: 20). Rationality, desired by power holders, ensures the reinforcement of power and its domination over the society. "The substance of domination is not dissolved by the power of technical control; on the contrary, the former can simply hide behind the latter" (Habermas, 1971: 61). Although this control of individuals and the masses serves to the increase of domination, its repressive character is removed from the conscious of people, especially, through the discourse of security. With such discourses, whether of security or of consumer satisfaction, comprehensive surveillance and control over society is

legitimized; this legitimization of the control of power leads to the legitimization of domination, as well.

Although surveillance technologies in our everyday lives are the symbols of domination, people do not regard them as instances of the domination of power or as an extension of repressive character of power. However, they consider them as tools to live more comfortable; for example, surveillance cameras around us are regarded as a means for the improvement and the augment of their security and of public safety rather than as a means for power to increase its domination. To exemplify, as also discussed in the third chapter, TV channels, unexceptionally, broadcast the records of MOBESE cameras related to a crime and the speeches of officials on the abilities of the cameras in the post-crime period. Such cases result in the fact that people would see these cameras as a necessary policing measure against the crime. Through these cameras and other tracking tools as biometric methods, the state has got the power to monitor what people do, and where they are frequently.

Another surveillance technique monitoring the actions of the individual, in the legitimization of domination, is witnessed via smart cards used in workplaces by employees. As explained by Elif Maviş, employees and students of METU are monitored via their ID cards, which also function as a smart card, within the boundaries of the campus; the card is used to enter the buildings having an electronic passing system and is used as a payment device in several activities within the campus. Which buildings the employee visits outside the working hour, how often he/she is in his/her office at weekends, which facilities he/she enjoys, what kind of a transactional data he/she has, in short, his/her actions, habits, and expenditures are tracked through this system.

The system is pursued to maintain the security and to better the services provided to the employees.⁷⁴ Behind these discourses, there is the aim to make everything visible and predictable through eliminating uncertainties. Surveillance practices concerning not only people's jobs, but also their very personal data are legitimized under the name of security and employee satisfaction. What is welcomed and legitimized is not merely the existence and functioning of the all-seeing eye, but also its increasing power and domination over people.

The other discourse used in the legitimization of surveillance and control and of the domination over the society is the efficiency and consumer satisfaction. This case witnessed in the commercial field is that private corporations, namely, stores, as discussed in the previous chapter, get use of these technologies in order to rationalize the working process and the their relation with customers. They do not track individuals physically as in the case of cameras, but track their purchases, choices, needs, and lifestyles. These data are very influential to learn both what people are actually doing and saying and what they will potentially do or say next. They are gathered, stored, and analyzed through loyalty cards used by consumers in shopping.

Customers are compelled to use loyalty cards in their shopping, not through coercive means, but through persuasion and seduction of the benefits of these smart cards. Companies provide several advantages, such as discounts and promotions, to their customers who use these cards. In order to mostly benefit from these discounts and, thus, due to economic reasons, customers do not hesitate to use loyalty cards and to share their data with the related companies. They do not regard them as an infringement to their privacy, but as a tool bettering their budgets. However, personal data in the hands and in the service of corporations have become a tool of control over people.

⁷⁴ From the interview with Maviş, Elif

Because they have the information on individuals' very personalities, companies, as a power holder, can manipulate and direct the consumption habits and even lifestyles of them, in accordance with the benefit and will of power. A standardized way of consumption and lifestyle is presented to the individuals. It is aimed to take the individual and the masses under the control of power. This is not maintained through coercive means as in Orwell's dystopia, but through persuasion, seduction, and exposure, as mentioned previously.

Corporations aim and attempt to use other various measures with RFID technology, as dealt with Albrecht and McIntyre (2006), other than loyalty cards, in order to rationalize the system in their workplace. One is the "Automated Monitoring of Activity of Shoppers in a Market" invented by NCR (National Cash Register Company) in December 2003. According to this application,

"when an unsuspecting does lift an item from a shelf, say a can of corn, the system kicks into surveillance gear, timing precisely how many seconds the shopper holds the item before either putting it back on the shelf or placing it in her shopping basket...The invention determines whether each item is located in one of three positions, namely, in the basket, on the shelves or neither in the basket nor on the shelves" (Albrecht and McIntyre, 2006: 64).

Another invention is related with RFID-tagged items used by consumers. It is an invented by IBM and called as "Identification and Tracking of Persons Using RFID-Tagged Items". It is used to learn identities and other information about consumers in a particular shopping place.

RFID readers, hidden in certain points of the store, can scan the RFID tags placed into or onto the object used by the consumer; accordingly, the system is notified about information of this consumer. Then, for example,

“if the person is carrying a man’s wallet, the store advertisement system may be configured to advertise razor blades and shaving cream while the person is passing through a particular display device in the store” (Albrecht and McIntyre, 2006: 68).

These are potential means, in addition to other aforementioned means as cameras and smart cards, to monitor and control people in their daily lives and, thus, to maintain a rationalized and managed world. The critical point, here, is to make these technologies and the notions of surveillance and control acceptable, desirable, and welcomed by the society. Due to the fact that they are tools in the hands of power to ensure its domination over the society, power holders want people to welcome these notions. Both governmental agencies and private corporations work hand in hand to emphasize the benefits and importance of monitoring and to present surveillance and control as usual and natural features of contemporary society, which should not be challenged. These result in the penetration of surveillance and control into lives of individual with little or no challenge.

Another item that has to be mentioned in this matter is the attempt of self-control, as analyzed by Foucault (1977) in his analysis on Bentham’s Panopticon. In clear, the existence of surveillance and control technologies in all fields of life instills the thought into the conscious of people that there might be someone at any moment watching over us. This feeling leads to the fact that people need to control and adjust their actions and behaviors “due to the fear of the panopticon” (Foucault, 1977). It is implied that power sees the individual at any time, whether while walking through a street or while doing shopping, so that this potentially constant visibility affect self-control of individuals. Thus, the major effect of surveillance and control technologies, as stated by Foucault (1977: 201) concerning the Panopticon, is “...to induce in the ... [individual] ... a state of conscious and permanent visibility that assures the automatic functioning of power”.

The functioning of power is strengthened through making people be in harmonious with the existing social order and with the dominant ideology. On the other hand, the inner structure of power ensuring domination over the society does not change. Technology, particularly, surveillance and control technologies, in the hands of power, are the tool in the increase and deployment of social control and domination over the society. Rationality, on the other hand, maintained through these technologies, "...protects rather than cancels the legitimacy of domination" (Marcuse, 2002: 162).

What is at stake, in terms of the will of power, is not a blank surveillance and control over the society, but the maintenance of rationality and the legitimization of domination. Surveillance is aimed to function effectively and efficiently by power to monitor, control, and administer all spheres of life and all individuals in the society, in which uncertainties and risks are accepted as usual characteristics. Thus, the initial goal is to eliminate or, at least, diminish uncertainties and to make actions and behaviors of individuals visible and predictable in accordance with the goal of rationality.

In this issue, all-seeing and all-knowing eye of power via surveillance and control technologies, from surveillance cameras to biometric devices and satellites to smart cards serve to power in an ideological fashion. These technologies and their functioning in such a manner indicate "...a rationalized, automated, totally managed world" (Horkheimer quoted in Held, 2007: 73), where domination of power is still prevailing over the society.

The surveillance-and-control society, in which power increases its domination over the society via new technologies, is the society where the signs of the Orwellian society exist and where there occurs little or no place to escape from being monitored. Thus, it can be declared that technologies promoting surveillance and control in the current society and their widespread

functioning in all domains life are very effective tools of power holders for the sake and will of dominant ideology.

What determines the relation between the society and power, as a surveillee and inspector, is not the technology itself, but the power relations behind it and its ideological functioning according to the will of power. Behind several discourses as security and service improvement, although surveillance technologies also function according to these goals declared by the government or the private corporations, they, on the other hand, mostly function to keep the individual and the society under control, that is, under the domination of power. The critical point which needs to be questioned is not the opportunities of new technologies improving the living conditions of people, but the problems serving to the power through confining people in the disguise of freedom.

5.4 RESISTANCE TO SURVEILLANCE

As analyzed up to now, it can be concluded that surveillance and control have so penetrated into our lives and consciousness that it is mostly conceived we have no choice but to adopt it. Power aims to continue and reinforce its power and domination over the society through keeping people under constant surveillance and control in all fields of life. Furthermore, it is expected for people to live in safety and in comfort without questioning the means leads to their so-called security and satisfaction: Just enjoy your life, do not bother

about the all-seeing and all-knowing eye on your personal life and on your personal information.

On the other hand, although power aims to minimize and even eliminate challenges to surveillance and control, it is the fact that there is always resistance where there is power (Foucault, 1980). Removing one's potential questioning and resistance, wholly, from his/her conscious is hardly or no possible. No possible because it is contrary to the nature of human, who always wonder and question everything concerning his/her life, throughout the history. Hardly possible because people, somehow, are willing to become "docile bodies", in accordance with the will of power, through providing so-called comfortable and safe world to live in and providing economic benefits.

Several attitudes of people toward surveillance and control technologies are witnessed. Holtzman's (2006) analysis on people's attitudes toward the privacy problem can be applied to their approaches to these technologies. He declares that

"people can employ five strategies to tackle the privacy problem. Each requires adopting a role, or combination of roles, and playing out the associated attitude. The characters are: the ignorer, the avoider, the deceiver, the curmudgeon, and the vigilante" (Holtzman, 2006: 254).

These characters are largely witnessed in the monitoring practices, basically, in cyberspace and supermarkets; the latter is one of the main concerns of this study. Besides, these characters are also witnessed in other fields of surveillance individuals are subject to. Ignorers do not pretend there is a problem about the effects of surveillance; they deny negative results of it. They regard tracking cameras located everywhere and other technologies as useful for the society without any criticism. The avoider, on the other hand, is aware of the fact that, for example, credit cards and loyalty cards have a

capacity to track his/her transactions; thus, they prefer paying in cash and getting rid of the economic benefits of loyalty cards. However, it is not much seen in the current society in which individuals consume and live through giving priority to their budget. As for the deceiver, he is who pretends himself/herself as someone else. Holtzman (2006: 256) exemplifies a deceiver in the cyberspace in that “with a few clicks of the mouse, you can digitally transform yourself from an educated forty-year-old woman living in suburbia to an elderly man living on social services”.

In addition, in the case of loyalty cards in Turkey, customers can potentially give incorrect information about them on the membership form, such as wrong phone number or even name; yet, it rarely happens that almost all loyalty-card users submit correct information.⁷⁵ Furthermore, “to be a curmudgeon, just say no. Refuse every unwarranted request for information and begrudgingly acquiesce only if necessary” (Holtzman, 2006: 258). Finally, the vigilante is much obsessed in sharing his/her information with other people. He considers every attempt of surveillance as an infringement to his/her privacy. Other than these different people approaching to the practice of tracking whether in a positive or negative manner, there are also anti-surveillance movements pursued, largely, by civil right activists and consumer groups. One of the most common groups is the Surveillance Camera Players⁷⁶. It is a group of players, which was formed in November of 1996 in New York. They define themselves as “...a small, informal group of people who are unconditionally opposed to the installation and use of video surveillance cameras in public places”⁷⁷. They frequently perform acts in front of surveillance cameras in order to inform and warn people about the surveillance

⁷⁵ From interviews with Beğendik, Ata, the General Director of Beğendik, with Şenel, Mine, the Manager of Armada CarrefourSA, and with Ögüt, Ömer, the Director of Computer Center of Ögütler

⁷⁶ <http://www.notbored.org/the-scp.html>

⁷⁷ <http://www.notbored.org/10-year-report.html>

cameras which have a function of eroding our private lives. They present and also declare that streets, owing to the existence of surveillance cameras operating continuously, have become stages (Schienke and Brown, 2003). Whether on the street or in a private place, the cameras are tools watching and recording private lives of individuals without their consent or persuasion.

In addition to New York Surveillance Camera Players, there are also players in Arizona and California, the US, Italy, Germany, France, Sweden, Lithuania, Spain, Holland, and Turkey. They regularly perform acts in front of the cameras sometimes coordinately or sometimes autonomously. Surveillance Camera Players in İstanbul, Turkey, call themselves as NOBESE, referring MOBESE the name of the state-surveillance cameras in Turkey, and define themselves as those who are not happy with being monitored and with the fact that people's every action is attempted to be kept under control.⁷⁸

As consumer surveillance, the most effective working anti-surveillance movement is CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) which was founded in October 1999 by Katherine Albrecht.⁷⁹ The advocates and volunteers of CASPIAN are mainly against RFID chips and loyalty cards of supermarkets which monitor personal and transactional data of consumers. They have nicknamed tiny chips embedded into the loyalty cards as “spychips” because of their surveillance potential (Albrecht and McIntyre, 2006). These devices, as analyzed previously, carry data as who the customer is, what he/she frequently buys, how much he/she spends periodically, what his/her preferences are, etc. to the managers of supermarkets. CASPIAN also reveals and listed the supermarkets, in the US,

⁷⁸ <http://www.izleniyoruz.net/php/index.php>

⁷⁹ <http://www.nocards.org/>

according to whether they monitor their shoppers, in order to inform people which supermarkets are tracking them and their purchases.⁸⁰

In addition to these movements, there are also other anti-surveillance movements working to defend private lives and personal information of people against intrusions of governmental agencies and private corporations. Privacy International (IP)⁸¹ is one of them, which a human rights group, formed in 1990, as a watchdog on surveillance and privacy invasions by governments and corporations. The American Civil Liberties Union (ACLU)⁸² is an organization, founded in 1920, which declares to protect the freedom of people, freedom from unwarranted government intrusion into people's personal and private affairs. Furthermore, the Electronic Privacy Information Center (EPIC)⁸³ is a public interest research center, formed in 1994, which has a goal to focus public attention on emerging civil liberties issues and to protect privacy of individuals. Such anti-surveillance movements inform the society on the intrusion of surveillance technologies into our private lives and on the erosion of our privacy. The use of surveillance over people to control them and to reinforce the domination of power is aimed to be reduced and even removed. In order to achieve this, the individual should be one who wonders and questions the surveillance practices around him/her in all domains of life.

⁸⁰ <http://www.nocards.org/list/supermarketlist.html>

⁸¹ <http://www.privacyinternational.org/>

⁸² <http://www.aclu.org/index.html>

⁸³ <http://epic.org/>

CHAPTER 6

CONCLUSION

This study takes its position as that technology is neither a neutral nor an autonomous factor in the development of society, but is an ideological tool of power to provide social control and domination over the society and also to provide rationality. However, it has to be declared that this position of the study does not refer to a negative approach to technology. It does not exclude or ignore the role of technology as a means of economic development and betterment of everyday life through the use of such as automobiles, household appliances, mobile phones, computers, and the Internet. On the other hand, my concern here is not to point out the benefits of technological developments, but more notably to discuss the ideology behind the practices of technology, particularly, of surveillance and control.

It is the fact that several technologies have been employed, in the last decades, not merely to improve economic and social development, but also and more notably to increase surveillance and control over individuals and over the society. While, previously, the criminals and suspects were subject to being tracked, today, whole society has become the subject of surveillance and control practices. Being innocent and harmless does not necessarily lead to the escape from being surveilled.

Current form of surveillance, which is systematic and institutional and carried out by several national, transnational, and local institutions, includes every individual and every aspect of life. This dispersed and intensive character of surveillance via new technologies has resulted in the decrease of direct control and of repressive character of domination. In other words, technology has helped power to decrease its coercive character. In addition, it also functions to provide rationality where everything is visible, predictable, and controllable through constant gaze.

The idea behind the discussions emphasized throughout the thesis is to point out this relationship of technology and power, in general, and to analyze how surveillance and control function as an ideological and a rationalizing tool of power in today's information societies. As mentioned in previous chapters, technologies as CCTV monitoring, biometrics, smart cards, and the Internet are employed by state and/or private agencies under the name of two discourses: one is security and the other is efficiency.

The security discourse suggests that tracking devices are applied in the struggle against crimes and risks threatening human life and social order. Considering monitoring practices as such a policing tool is largely supported by authorities and declared to individuals. Visual surveillance, discussed in the third chapter, functioning via cameras built in stores, buildings, schools, airports, and streets is the most used tracking technology. It works as an all-seeing eye, as the digital Panopticon, in every field of life.

The critical point is that not only their functioning and recordings, but also just their existence has a function to obtain obedient citizens or, say, "docile bodies" for the will of power. That is to say, people are expected to control -and they mostly do- their actions and adjust their behaviors due to the fear of cameras that are anywhere around them and that may watch them at any time; the existence of cameras, whether recording or not, lead to the self-

control of individuals. On the other hand, as pointed out in the third chapter with several examples, an objection, which can be posed at this point, is that we are facing with news about crimes, accidents, and other several events, such as a detection of a criminal, recorded by a surveillance camera on TV channels and newspapers every day. This means that cameras as tracking devices do not solve the security and safety problem suggested and expected by authorities. However, this case has not decreased the importance of cameras as a policing tool in the eye of public at large because their this feature is expected to ease security problems in the society.

The second discourse, efficiency and consumer satisfaction accompanying it, largely discussed in the fourth chapter, considers surveillance over such as employees, students, and consumers via smart cards as a means to improve efficiency and services provided. Visual surveillance becomes not sufficient for power; it also aims to get information about individuals' personal information, such as beside their names, addresses, and jobs, also their habits, likes, dislikes, and lifestyles.

These data are collected and stored through credit cards and, more effectively, loyalty cards, which are largely analyzed in the fourth chapter, used by consumers in their shopping. By this way, personal information, habits, consumption patterns, and, thus, lifestyles have become subject to surveillance of several institutions as private corporations, state agencies, associations, school authorities, and parents. This monitoring practice is carried out under the name of efficiency, consumer satisfaction, and of improvement of services that are declared by authorities.

The significant point in both items, surveillance under the name of safety and efficiency, is the unquestioning approach and acceptance of individuals. People, for example, do not question the structure, features, and working process of loyalty cards they regularly use in their shopping. They

regard these cards as discount cards which provide discounts in certain products in the store, without knowing or caring their tracking capacity. There is not an informed consent in this case given by customers, in which they are well-informed about the whole working process of these cards.

As mentioned in the fourth chapter, the membership forms of these cards get the consent of the card user through a short sentence which is generally disregarded and not read by the customer. He/she makes, unwittingly, all his/her personal data to be subject to surveillance in exchange for economic benefits as discounts and campaigns; hence, this can be defined as a purchased consent.

As for surveillance cameras, similarly, people mostly regard them necessary and useful for the public safety and for the security of their living. On the other hand, they do not have enough information about the functioning of such as street-surveillance cameras recording everything in the streets and about the use of their records. In both issues, Gramscian sense of consent clarifies this case more properly in that individuals give consent to surveillance and its institutions through living with them compatibly and in an unchallenging manner through accepting them as embedded and usual components of their lives and of the society.

Surveillance and control and their technologies and practices are regarded by most people as a necessity and precondition of today's so-called risk societies due to the increasing demand of security. Together with the introduction of these technologies into our lives, we have faced with several technologies surveilling us and all our actions. Children grow up with cameras around them, students are always under the control of their parents and school authorities, employees work with several monitoring measures used as a managerial control and, overall, all individuals live surrounded by cameras and other forms of surveillance every day and every time. In addition to being

monitored by the cameras, their personal data are gathered and stored by others while they are using credit cards, mobile phones or loyalty cards of supermarkets, or while surfing in the Internet. Personal data of individuals may easily be reached by anyone; we do not know who use these data how and for what purposes.

Within this framework, people, mostly, do not challenge the existence of these technologies and their extensive and intensive functioning; besides, they do not question whether their privacies are eroded. This is because concepts of surveillance and control are usual parts and sine qua non of human life and of contemporary society in the eyes of people. As discussed in the fifth chapter, from childhood to schools, from schools to workplaces and to daily lives in the streets and even at home, surveillance and control and their technologies are along with us. They have become a culture in the current society.

In addition to people's living together with surveillance and control, another issue analyzed in the study is the idea and reason behind the practices of them. Power holders, both state authorities and private corporations, give much importance to the functioning of tracking technologies. In order to strengthen their power and to ensure the well-being of capitalism, the authorities aim to see, know and predict every potential threat against the social order and to maintain efficiency through taking everything under their authority under control.

What threatens power most is the unknown and uncertainty. Therefore, the principal target is to reduce and, if possible, eliminate them. If there is nothing unknown and unpredictable, there is nothing to worry about. Capitalism is supposed to work more efficiently and effectively if uncertainties about the market and about consumers decrease. For instance, only if preferences and habits of consumers are learned through their data via loyalty

cards, certain commercial acts, such as targeted advertisements, can be performed by corporations to manipulate and direct their choices and consumption patterns. Thus, power intends to get more and more information to strengthen its power vis-à-vis the civil society. As seen, information has become the notable notion in the practice of surveillance and control. All surveillance and control practices mentioned throughout the thesis serve power through providing as much information as possible about individuals.

This case introduces us rationality where spontaneity and unpredictability have no place. Because new technologies give capacity and power to prevent this spontaneity, power holders establish and operate more surveillance practices in order to form a rational system and to strengthen this rationality and, thus, to ensure domination over the society. Several technologies are used sometimes to prevent crimes, to detect and deter criminals and suspects, sometimes to persuade or seduce consumers in their shopping, but always to strengthen social order and provide social control through surveilling individuals. Rationality is achieved in the current society more functional and effective than its previous forms through providing efficiency, surveillance, predictability, and control via new technologies.

Such a society reminds Orwellian society in which a total surveillance state and a totally-administered society exist. Technical barriers to an Orwellian society are being surmounted with every new technological development. It can be declared that we are rapidly moving toward a society or, actually, we are in such a society in which all information, actions, and behaviors are monitored and controlled and in which power is omnipresent and omniscient via extensive functioning of surveillance technologies. On the other hand, there are also social groups and activists, mentioned in the preceding chapter, which challenge existing surveillance practices and which inform individuals that these practices function against our privacy. They try to warn

people that technologies as smart cards and surveillance cameras are eroding our privacy and working as a control mechanism of power holders.

Beside technology's being a tool of power, domination and forms of hegemony can also be removed by democratization. In the process of democratization of practices and institutions promoting surveillance, control, and, thus, domination, the foremost role belongs not primarily to certain laws and rules forcing authorities to be transparent and accountable and giving individuals several rights, but, more effectively, belongs to awareness, initiative, and participation of individuals. These notions and their effective practice by individuals and social groups in all aspects of life are determinant in the struggle of democracy, in the struggle against undemocratic practices of surveillance and control and against domination over them.

As seen throughout the study, all surveillance practices are developed and employed without any participation of individuals and civil society. Mostly, they do not have any knowledge about the structure, functioning, and outcomes of these practices. They only consider them as beneficial and necessary for public safety and for better services; on the other hand, they do not worry about their privacy or question how several technologies monitor them for what purposes. This means that surveillance and control are performed by power holders from above in an undemocratic manner; people do not have any right or impact in the working processes of monitoring and in the formation and use of databases created through their personal information.

Only if democracy permeates to all aspects of social life such as through participation of individuals in policy-making and in practices of surveillance and through control mechanisms of civil society supervising applications of state and private agencies, we will, then, talk about democratic institutions promoting participation rather than social hierarchy, salvation from domination, democratic society, and individuation. The path of

democratization starts with wondering and questioning what is going on concerning human life and the society. For instance, only if one questions and challenges technologies tracking all his/her acts and activities, then, questioning the ideology behind surveillance practices, questioning rationalization, questioning domination, and questioning hegemony of power can be possible.

Civil society should be more active and effective in forcing public and private authorities in order to make them accountable and transparent in their acts and activities. This leads to the fact that the processes concerning the functioning of surveillance technologies and the collection, storage, and use of individuals' data will be subject to a control mechanism and will be more democratic. In order to achieve this, the attempts of questioning and challenging of individuals and social groups are needed.

Therefore, the principal duty is assigned to individuals themselves and to the civil society, more concretely, social groups. The starting point in the effort to make the system more democratic and, thus, to remove domination is to raise awareness throughout the society. Public awareness should be generated, at first, about the structure and functioning of tracking applications. For example, while surfing the net, we should be aware of being tracked via our IP addresses and cookies; or while shopping with a smart card, we should be aware of the fact that our personal data are collected and used by firms.

Individuals should be aware of the fact that cameras are continuously watching and recording them everywhere, that their personal data are collected through smart cards and anyone can reach these data, and that the Internet is a cyberspace in which their data, such as their preferences and habits, are open to tracking of states, corporations, associations, and even any internet user. Only then, the individual can question the happenings in his/her life and in the

society. This can also pave the way to question and challenge domination, control, and rationality used by power to continue and ensure its hegemony.

Here, the challenge expected to be pursued by individuals has two sides. On the one side, people should question the surveillance technologies and their intensive functioning in all fields of life as a tool to obtain data of individuals for the use of power holders. On the other side, more notably, they should struggle against the ideology and power relations, which intend to provide domination and social control in the disguise of security and efficiency, behind the practices of surveillance and control. This refers to the struggle against a totally-administered society and their institutions promoting domination over the society. Because domination, whether coercive or not, impedes the development of free and independent individuals, the main challenge should be directed to the domination of power. Only by this means, democracy can be placed in the social life with its required concepts and institutions, and with independent individuals.

It is the fact that Foucault's Great Confinement still exists but without physical barriers and without coercive functioning of power. The Panopticon in the contemporary society no longer needs to confine people in order to discipline them and to instill the dominant ideology into their conscious. Today, with several technological means, particularly, those mentioned in this study, power is everywhere. It not only monitors individuals and their actions and behaviors such as in workplaces, schools, stores, the Internet, etc. to obtain every information about them, but also tries to control and manipulate their actions, behaviors, choices, and lifestyles in order to make people "docile bodies" for the well-being of existing social order and for the sake and will of power.

Large scale technological developments and their widespread functioning in the hands of power holders intensely lead to the emergence and

strengthen of the thought that there will be no alternative way of living and no alternative form of society free of technologically-mediated surveillance and control and, thus, free of domination of power over the society. Within this framework, whether all-encompassing functioning of technology everywhere will lead to the emergence of a society in which people become helpless and hopeless individuals who only act, consume, and live according to the manipulations and directions of power or will lead to the emergence of a society in which everyone lives equally, happily, and comfortably without poverty, crimes and wars is an answerless issue.

In both cases it is seen that technology continues its effective and extensive functioning in the hands of power together with people's positive or neutral approaches to its being an ideological tool of power regardless of its privacy-eroding character. Therefore, another alternative should be pursued and another form of social structure should be maintained in which technology does not serve to power holders in ensuring their domination and hegemony over the society, in which individuals and the society are not controlled and administered according to the will of power, and in which the use of technology does not impede the development of free and independent individuals. What is needed in order to achieve this are the efforts and activities of people through questioning and challenging the ideological functioning of technology as a tool of power and also challenging the domination of power ensured by new technologies.

Every new technology, functionally, becomes a surveillance means in the hands of power holders, both state and private agencies and both national and transnational organizations. This case leads to the enlargement of the boundaries of the Panopticon. Such a confinement and domination in the current society cannot be resolved just through being good citizens or loyal customers, which are predetermined and expected to occur by power holders.

On the contrary, they can be resolved through being sometimes troublesome individuals who question and criticize the environment around them, who are aware of the ideology behind, and the outcomes of, the surveillance applications, and who challenge the practices not merely resulting in the impediment of individuals' emancipation from control and manipulation but also ensuring and promoting the hegemony of power over the society. Questioning the all-seeing and all-knowing eye is the starting point of the salvation from technically-mediated forms of surveillance and control and, thus, from domination.

REFERENCES

Albrecht, K. and McIntyre, L. (2006), *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*, London: A Plume Book

Althusser, L. (2002), *İdeoloji ve Devletin İdeolojik Aygıtları*, İstanbul: İletişim

Attewell, P. (1987), “Big Brother and the Sweatshop: Computer Surveillance in the Automated Office”, *Sociological Theory*, 5, 87-99

Ball, K. and Webster, F. (2003), “The Intensification of Surveillance”, in K. Ball and F. Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, London: Pluto Press, 1-15

Bassett, C. (2007), “Forms of Reconciliation, On Contemporary Surveillance”, *Cultural Studies*, 21 (1), 82-94

Beck, U. (1992), *Risk Society: Towards a New Modernity*, London, Thousand Oaks and New Delhi: Sage

Bell, D. (1976), *The Coming of Post-Industrial Society*, New York: Basic Books

Bentham, J. (1995) in M. Bozovic (ed.), *The Panopticon Writings*, London and New York: Verso

Bignell, J. (2005), *Big Brother: Reality TV in the Twenty-First Century*, New York: Palgrave Macmillan

Castells, M. (2000), *The Information Age: Economy, Society and Culture, Volume I, The Rise of the Network Society*, Oxford: Blackwell

Clarke, R. (1988), “Information Technology and Dataveillance”, *Communications of the ACM*, 31 (5), 498-512

Coleman, R. (2004), *Reclaiming the Streets: Surveillance, Social Control and the City*, the USA and Canada: Willan Publishing

Davies, S. (1998), "Re-Engineering the Right to Privacy", in P. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, Cambridge: The MIT Press, 143-165

Deleuze, G. (1990), *Negotiations 1972-1990*, New York: Columbia University Press

Deleuze, G. (1992), "Postscript on the Societies of Control", *October*, 59, 3-7

Dickson, D. (1974), *The Politics of Alternative Technology*, New York: Universe Books

Doyle, A. (2006), "An Alternative Current in Surveillance and Control: Broadcasting Surveillance Footage of Crimes", in K. D. Haggerty and R. V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, Toronto, Buffalo and London: University of Toronto Press, 199-224

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

Elmer, G. (2003), "A Diagram of Panoptic Surveillance", *New Media and Society*, London, Thousand Oaks and New Delhi, 5 (2), 231-247

Feenberg, A. (1991), *Critical Theory of Technology*, New York and Oxford: Oxford University Press

Feenberg, A. (1995), "Subversive Rationalization: Technology, Power, and Democracy", in A. Feenberg and A. Hannay (eds.), *Technology and the Politics of Knowledge*, Bloomington and Indianapolis: Indiana University Press, 3-22

Foucault, M. (1977), *Discipline and Punish: The Birth of the Prison*, London and New York: Penguin Books

Foucault, M. (1980) in C. Gordon (ed.), *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, Sussex: The Harvester Press

Fox, R. (2001), "Someone to Watch Over Us: Back to the Panopticon?", *Criminal Justice*, 1 (3), 251-176

Fraser, N. (2003), "From Discipline to Flexibilization? Rereading Foucault in the Shadow of Globalization", *Constellations*, 10 (2), 160-71

Gandy, O. H. (1993), *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, San Francisco and Oxford: Westview Press

Goldsmith, C. (2006), “‘You Just Know You’re Being Watched Everywhere’: Young People, Custodial Experiences and Community Safety”, in P. Squires (ed.), *Community Safety: Critical Perspectives on Policy and Practice*, Great Britain: The Policy Press, 13-33

Goss, J. (2002), “‘We Know Who You Are and We Know Where You Are’: The Instrumental Rationality of Geodemographic Systems”, *Economic Geography*, 71 (2), 171-198

Graham, S. (2006), “The Eyes Have It: CCTV as the ‘Fifth Utility’”, in C. Norris and D. Wilson (eds.), *Surveillance, Crime and Social Control*, Hampshire: Ashgate, 147-150

Graham, S. and Wood, D. (2003), “Digitizing Surveillance: Categorization, Space, Inequality”, *Critical Social Policy*, 23 (2), 227-248

Habermas, J. (1971), *Toward a Rational Society: Student Protest, Science, and Politics*, London: Heinemann

Hall, S. et al (1978), *Policing the Crisis: Mugging, the State, and Law and Order*, New York: Palgrave Macmillan

Held, D. (2007), *Introduction to Critical Theory: Horkheimer to Habermas*, London, Melbourne and Auckland: Hutchinson

Helten, F. and Fischer, R. (2004), “Reactive Attention: Video Surveillance in Berlin Shopping Malls”, *Surveillance and Society*, 2 (2/3), 323-345, available at [http://www.surveillance-and-society.org/articles2\(2\)/berlin.pdf](http://www.surveillance-and-society.org/articles2(2)/berlin.pdf) (last access in August 2009)

Holtzman, D. H. (2006), *Privacy Lost: How Technology is Endangering Your Privacy*, San Francisco: Jossey-Bass

Horkheimer, M. and Adorno, T. W. (1996), *Dialectic of Enlightenment*, New York: Continuum

Innes, M. (2003), *Understanding Social Control: Deviance, Crime and Social Order*, Berkshire: Open University Press

Jhally, S. (1990), *The Codes of Advertising: Fetishism and the Political Economy of Meaning in the Consumer Society*, New York and London: Routledge

Kammerer, D. (2004), "Video Surveillance in Hollywood Movies", *Surveillance and Society*, 2 (2/3), 464-473, available at [http://www.surveillance-and-society.org/articles2\(2\)/movies.pdf](http://www.surveillance-and-society.org/articles2(2)/movies.pdf) (last access in October 2009)

Koskela, H. (2003), "'Cam Era' - The Contemporary Urban Panopticon", *Surveillance and Society*, 1 (3), 292-313, available at [http://www.surveillance-and-society.org/articles1\(3\)/camera.pdf](http://www.surveillance-and-society.org/articles1(3)/camera.pdf) (last access in September 2009)

Lyon, D. (1994), *The Electronic Eye: The Rise of Surveillance Society*, Cambridge and Oxford: Polity Press

Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Buckingham and Philadelphia: Open University Press

Lyon, D. (2003), "Surveillance as Social Sorting: Computer Codes and Mobile Bodies", in D. Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York: Routledge, 13-30

Lyon, D. (2004a), "Globalizing Surveillance: Comparative and Sociological Perspectives", *International Sociology*, 19 (2), 135-149

Lyon, D. (2004b), "Surveillance Technology and Surveillance Society", in T. J. Misa, P. Brey and A. Feenberg (eds.), *Modernity and Technology*, Cambridge: The MIT Press, 161-183

Lyon, D. (2005), "The Border is Everywhere; ID Cards, Surveillance and the Other", in E. Zureik and M. B. Salter (eds.), *Global Surveillance and Policing: Borders, Security, Identity*, the USA and Canada: Willan Publishing, 66-82

Lyon, D. (2006a), "9/11, Synopticon, and Scopophilia: Watching and Being Watched", in K. D. Haggerty and R. V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, Toronto, Buffalo and London: University of Toronto Press, 35-54

Lyon, D. (2006b), "Bentham's Panopticon: From Moral Architecture to Electronic Surveillance", in C. Norris and D. Wilson (eds.), *Surveillance, Crime and Social Control*, Hampshire and Burlington: Ashgate, 13-34

Lyon, D. (2007), *Surveillance Studies: An Overview*, Cambridge: Polity Press

Mann, S. et al (2003), "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", *Surveillance and Society*, 1 (3), 331-355, available at [http://www.surveillance-and-society.org/articles1\(3\)/sousveillance.pdf](http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf) (last access in October 2009)

Marcuse, H. (2002), *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*, London and New York: Routledge

Marx, G. T. (2002), "What's New About the 'New Surveillance'? Classifying for Change and Continuity", *Surveillance and Society*, 1 (1), 9-29, available at <http://www.surveillance-and-society.org/articles1/whatsnew.pdf> (last access in August 2009)

Marx, G. T. (2005), "The New Surveillance", in T. Newburn (ed.), *Policing: Key Readings*, Cullompton and Portland: Willan Publishing, 761-785

Marx, G.T. (2006), "I'll Be Watching You: Reflections on the New Surveillance", in C. Norris and D. Wilson (eds.), *Surveillance, Crime and Social Control*, Hampshire: Ashgate, 3-11

Marx, K. (1971), *The Grundrisse: Foundations of the Critique of Political Economy*, New York: Harper and Row

Mathiesen, T. (2006), "The Viewer Society: Michel Foucault's 'Panopticon' Revisited", in C. Norris and D. Wilson (eds.), *Surveillance, Crime and Social Control*, Hampshire: Ashgate, 41-60

Mesthene, E. G. (1971), *Technological Change, Its Impact on Man and Society*, Cambridge: Harvard University Press

Murphie, A. and Potts, J. (2003), *Culture and Technology*, New York: Palgrave Macmillan

Norris, C. (2003), "From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control", D. Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York: Routledge, 249-281

Orwell, G. (1987), *Nineteen Eighty-Four*, Harmondsworth: Penguin Books

Poster, M. (1990), *The Mode of Information: Poststructuralism and Social Context*, Cambridge: Polity Press

Shienke, E. W. and Brown, B. (2003), "Streets into Stages: an Interview with Surveillance Camera Players' Bill Brown", *Surveillance and Society*, 1 (3), 356-374, available at [http://www.surveillance-and-society.org/articles1\(3\)/interview.pdf](http://www.surveillance-and-society.org/articles1(3)/interview.pdf) (last access in September 2009)

Simon, B. (2005), "The Return of Panopticism: Supervision, Subjection and the New Surveillance", *Surveillance and Society*, 3 (1), 1-20, available at [http://www.surveillance-and-society.org/articles3\(1\)/return.pdf](http://www.surveillance-and-society.org/articles3(1)/return.pdf) (last access in October 2009)

Staples, W. G. (2000), *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, New York and Oxford: Rowman & Littlefield Publishers

Street, J. (1992), *Politics and Technology*, London: Macmillan

Van den Hoven, J. and Vermaas, P. E. (2007), "Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon", *Journal of Medicine and Philosophy*, 32, 283-297

Van der Ploeg, I. (2006), "Written on the Body: Biometrics and Identity", in C. Norris and D. Wilson (eds.), *Surveillance, Crime and Social Control*, Hampshire: Ashgate, 461-468

Webster, F. (2006), *Theories of the Information Society*, London and New York: Routledge

Whitaker, R. (1999), *The End of Privacy: How Total Surveillance is Becoming a Reality*, New York: New Press

William, C. and Webster, R. (1999), "Closed Circuit Television and Information Age Policy Process", B. N. Hague and B. D. Loader (eds.), *Digital Democracy: Discourse and Decision Making in the Information Age*, London and New York: Routledge, 116-131

Williams, R. (2005) in E. Williams (ed.), *Television: Technology and Cultural Form*, London and New York: Routledge

Wilson, D. (2007), "Australian Biometrics and Global Surveillance", *International Criminal Justice Review*, 17 (3), 207-219

APPENDIX A

FIGURES ABOUT VISUAL SURVEILLANCE AND SURVEILLANCE THROUGH BIOMETRICS



Appendix A.1 A warning sign of CCTV surveillance in London
(Source: www.lodinews.com/articles/2008/01/30/news/4_sign_080130.txt)



Appendix A.2 A car of Google Street View viewing the streets
(Source: www.haberturk.com/galeri.aspxsrc=1&id=85213)



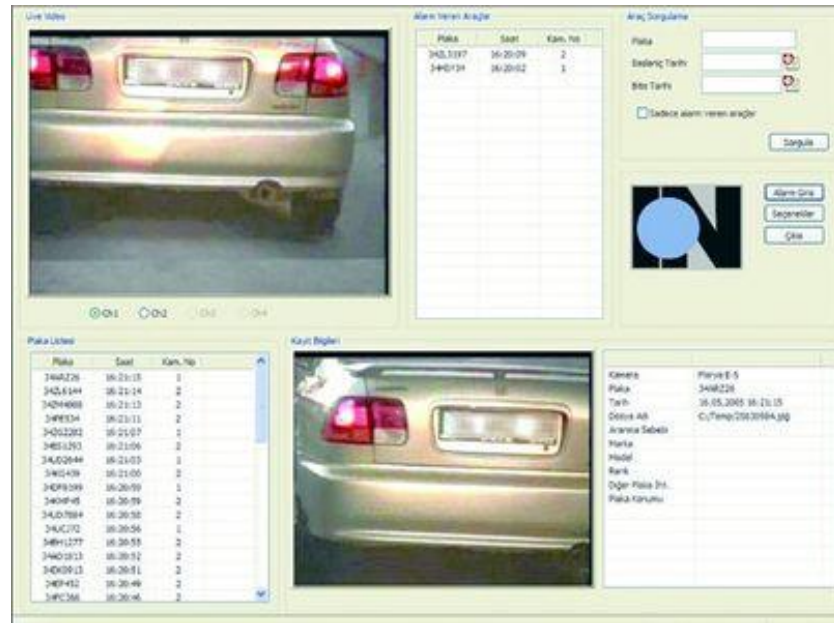
Appendix A.3 A view from San Francisco captured by Google Street View
 (Source: <http://maps.google.com/support/bin/answer.py?answer=68476>)



Appendix A.4 Picture of a man trying to enter a house which is captured by Google Street View cameras
 (Source: <http://www.flickr.com/photos/silvery/2516674106>)



Appendix A.5 The main control room of the İstanbul MOBESE system
(Source: <http://mobese.iem.gov.tr/images/imagesmbs/45.jpg>)



Appendix A.6 MOBESE cameras tracking the cars through license plates
(Source: <http://mobese.iem.gov.tr/images/imagesmbs/plaka2.jpg>)



Appendix A.7 A crime detected by a MOBESE camera in Bağcılar, İstanbul
 (Source: <http://sondakika.milliyet.com.tr/2006/03/23/son/sontur17.asp>)



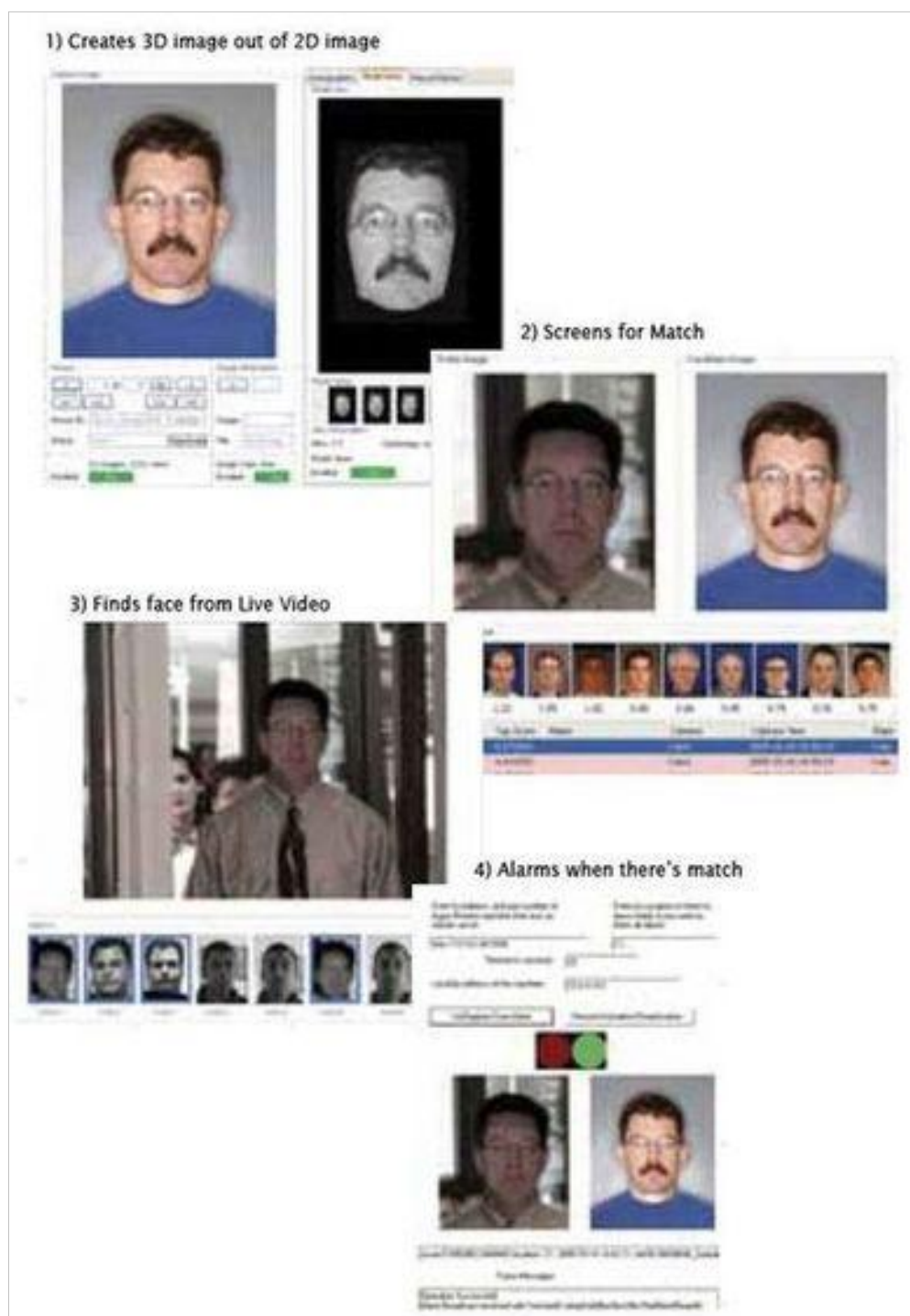
Appendix A.8 A capture of an arson recorded by MOBESE in İstanbul
 (Source: <http://www.milliyet.com.tr/2008/01/01/siyaset/asiy.html>)



Appendix A.9 Two-fingerprint scanners, used in the USA, collecting photographs and fingerprints of travelers
(Source: [http://en.wikipedia.org/wiki/Image:US-VISIT_\(CBP\).jpg](http://en.wikipedia.org/wiki/Image:US-VISIT_(CBP).jpg))



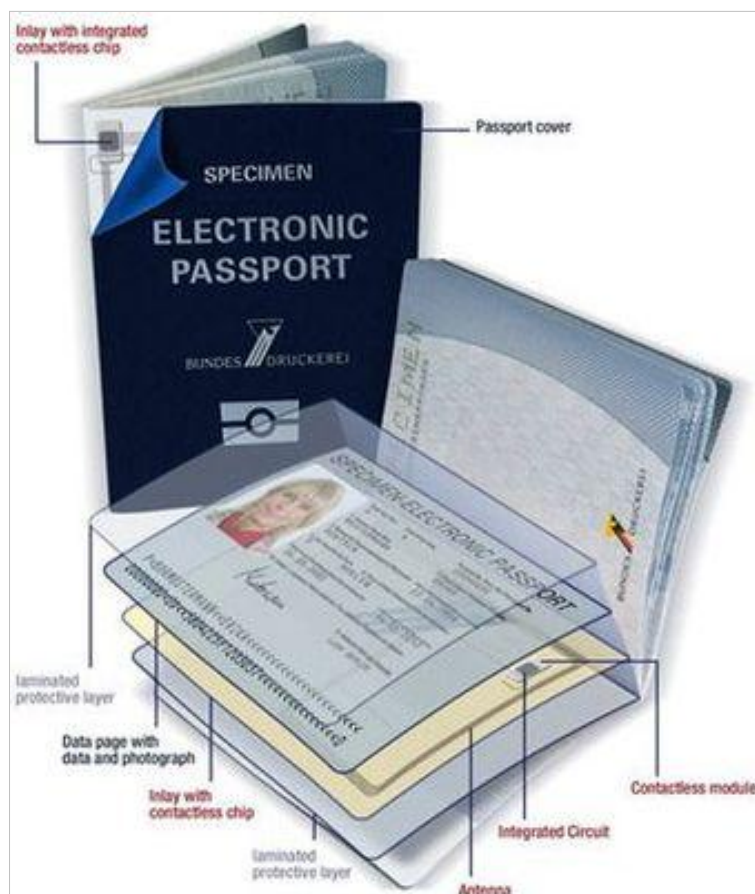
Appendix A.10 Ten-fingerprint scanners recording fingerprints and photographs of visitors at the US ports of entry
(Source: http://www.hurriyetusa.com/haber_detay.asp?id=15165)



Appendix A.11 The working process of FaceIT ARGUS program
 (Source: <http://www.i-secure.sg/Products/FaceITArgus.aspx>)



Appendix A.12 An example of an RFID tag
 (Source: <http://www.themajorlearn.info/SoftwareRFID.html>)



Appendix A.13 Hidden placement of the RFID tag inside a passport
 (Source: <http://webmsi.free.fr/HEC-MSI-0705W-GR9/nouvellepage2.htm>)


APPENDIX B


FIGURES ABOUT LOYALTY CARDS IN TURKEY

[illegible]

Appendix B.1 The membership form of Praktiker card

Üyelik Formu






**Yüzlerce üründe
indirimlerden
faydalanın.**

**Alışveriş
keyfiniz için
listenin
bir numarası!**
Daha birçok avantaj bu kartta...

**Migros Club Kartınızı
Para Üye İşyerlerinde
kullanın, avantajlardan
faydalanın.**



Migros Club kartınız ile,

- Yüzlerce üründe anında indirimlerden faydalanın.
- Sevdiğiniz ürünlerde size özel indirimler kazanın.
- Çekilişlere katılın.
- Özel Migros Club aktivite ve davetlerine katılın.
- Para Üyesi İşyerlerinde ekstra indirimler ve diğer avantajlardan yararlanın.
- Alışveriş yaptıkça parapuan kazanın.
- Kazandıkça bedava alışveriş yapın.
- Puanlarınızı kioskardan alışverişinize çevirin.


M

MIGROS

Lütfen dikkatlice okuyunuz

- Büyük harf ve koyu renk tükenmez kalem kullanınız. • Seçmeli yanıtlarınızı (X) işareti koyarak doldurunuz.
- Kutuları taşımadan işaretleyniz. • Başvuru formunuzu doldurduktan sonra üyelik ve rıza beyanını okuyup imzalamayı unutmayınız. • Kelimeler arasında bir boşluk bırakınız.

Migros Club kartınızın numarası

 → Lütfen Migros Club kart numaranızı yazmayı unutmayınız!

Kişisel bilgiler

Adınız _____

Soyadınız _____

Doğum tarihiniz _____ / _____ / _____ (gün/ay/yıl) Bilgilerinizin güvenliği için gereklidir.

Cinsiyetiniz ☐ bay ☐ bayan

Migros Club 8F20070120 Aşağı sayfaya geçin →

İletişim bilgileri

Adres tercihiniz ☐ ev ☐ iş

İşyeri adı _____

Mahalle _____

Cadde _____

Sokak _____

Bina adı _____

Posta kodu _____ apt. no _____ blok no _____ daire no _____

Semt/ilçe _____

İl _____

Cep telefonu (0) _____

Ev telefonu (0) _____

İş telefonu (0) _____ dahili _____

Faks (0) _____

e-posta adresi _____

Lütfen küçük harf kullanın! Örnek: migrosclub@migros.com.tr

Yeşil bölümdeki kutuları doldurmanız zorunlu değildir. Doldurduğunuz takdirde avantajlarınız size özel olacaktır.

Medeni durum bilgileri

Medeni durumunuz ☐ bekar ☐ evli ☐ evlilik tarihiniz _____ / _____ / _____

Varsa 0 - 15 yaş arası çocuklarınızın doğum tarihleri ve cinsiyetleri

1	_____ / _____ / _____	_____	kız	erkek
2	_____ / _____ / _____	_____	kız	erkek
3	_____ / _____ / _____	_____	kız	erkek

Eğitim ve meslek bilgileri

Öğrenim durumunuz ☐ ilköğretim ☐ ortaokul ☐ lise ☐ üniversite ☐ yüksek lisans

Mesleğiniz _____

T.C. Kimlik No _____

Appendix B.2 The membership form of Migros club card

Değerli Müşterimiz,

Aşağıda, Paro Programı'na ilişkin genel bilgi içeren "Paro Programı Üyelik ve Rıza Beyanı" yer almaktadır. Aşağıdaki metni imzaladığınızda, genel şartları belirtilen Paro Programı'na üyeliğinizi gerçekleştirmiş ve Paro Programı'nın size özel avantajlarından haberdar edilebilmeniz için kişisel bilgilerinizin Paro Program ortakları arasında paylaşılmasına ve işlenmesine izin vermiş olacaksınız. Paro Programı hakkında ayrıntılı bilgiyi www.paro.com.tr veya 444 7276'dan edinebilirsiniz.

Paro Programı Üyelik ve Rıza Beyanı

Tanı Pazarlama ve İletişim Hizmetleri A.Ş. (Tanı)'ye ait olan Paro Programı; Üyelerine (Üye), genel ve özel kampanya, promosyon, tanıtım, puan kazanma/harcama, hediye çeki verilmesi, kulüplere üye olunabilmesi ve indirim gibi avantajlar sağlamak amacıyla oluşturulan müşteri memnuniyeti odaklı pazarlama programıdır. Paro Programı'nın program ortakları; Paro Programı'na katılan üye işyerleri, Koç Topluluğu Şirketleri, diğer firmalar ile tüm bunların bayi, acente, franchise'ları ve ileride katılabilecek diğer şirketlerdir (Program Ortakları). Tanı ve/veya Program Ortakları Paro Programı haricinde müşteri memnuniyeti odaklı ve aşağıdaki amaçlar doğrultusunda başka pazarlama uygulamaları ve programları da yürürlüğe sokabilir. Üye, Paro Programı da dahil olmak üzere tüm uygulama ve programlardan yararlanmak için aşağıdaki koşulları kabul eder.

1. Üye, Paro Programı ve/veya yürürlüğe sokulacak diğer uygulamalar ve programlar çerçevesinde; Tanı ve/veya Program Ortakları tarafından, kendisine, genel ve özel kampanyalar, avantajlar, ürün, hizmet tanıtımları, reklam, pazar araştırması anketleri ve diğer müşteri memnuniyeti uygulamaları sunulmasına, kulüplere üye kaydedilmesine izin verir. Üye, Program Ortaklarına ve/veya Tanı'ya geçmişte vermiş olduğu, bu formla ilettiği ve sair yöntemlerle ileride vereceği alışveriş ve kişisel bilgilerinin yukarıda sayılan benzeri amaçlarla kullanılmak üzere toplanmasına, Tanı ve diğer Program Ortakları arasında paylaşılmasına ve bu firmalarca işlenmesine; Üye aksini belirtmediği sürece bu firmaların, kendisiyle SMS, internet, mektup, telefon vb kanallardan temasa geçmelerine izin verir. Üye aksini belirtmedikçe, Paro Programı veya üyelik sonlandığında da, verilerinin toplanmasına, Tanı, Paro Programı Program Ortakları ve devreye alınabilecek diğer programların ortakları ve Koç Topluluğu Şirketleri arasında, bu madde kapsamında sayılan benzeri amaçlar doğrultusunda, paylaşılmasını, işlenmesini ve kendisine erişilmesini kabul eder.

Üye, veri paylaşım tercihlerini değiştirmek isterse bu talebini Paro Programı iletişim kanallarından bildirebilir. Üye'nin bilgileri Tanı ve Program Ortaklarının hizmet sağlayıcılarıyla (gönderi, çağrı merkezi, veri tabanı vb hizmetleri firmaları ile) bu firmalar tarafından verilen hizmetler dahilinde kullanılması kaydıyla paylaşılabilir. Üye'nin verileri işlenip, bilgiler, Üye kimliği açıklanmaksızın, gruplar halinde 3. kişiler ile paylaşılabilir.

2. Üye, Paro Programı da dahil olmak üzere programlardan faydalanması için kendisine verilen kart ve numarasını, kullanıcı adı ve/veya şifreyi başkasına vermemeyi, kullanılmamayı, bunların saklanmasıyla ilgili sorumluluğunu; kartın, Üye veya başkası tarafından kötüye kullanıldığı, programların suistimal edildiği tespit edilirse, üyeliğe ilişkin her türlü hak ve kazanımların geri alınacağını, diğer tedbirlerin uygulanabileceğini kabul ve taahhüt eder. Üye, bu konuda doğabilecek ihtilaflardan Program Ortakları ve Tanı'nın sorumlu olmadığını, üyelik kartını veya kart numarasını başkasına vermemeyi, verdiği takdirde tüm sorumluluğun kendisinde olduğunu ve üzerindeki tüm haklarını kaybedeceğini kabul eder. Üye, üyelik kartının kaybolması, çalınması halinde, bu durumu çağrı merkezine bildirecektir. Bildirim yapılmıyca kadar doğabilecek her türlü zarardan Üye sorumludur. İleride, programlarda kart harici araçlar kullanılırsa, bu maddedeki koşullar kart harici araçlar için de geçerli olacaktır.

3. Her Program Ortağı'nda Paro Programı koşulları, faydaları farklı olabilir ve değişebilir. Tanı kişisel verilerin kullanım amacına yönelik hususlar hariç, önceden bildirirmeden, Paro Programı şartlarını değiştirebilir, programı durdurabilir, üyeliği iptal edebilir, üyeliğe ilişkin aldatılabılır. Geçerli koşullar Paro Programı'nın iletişim kanallarından öğrenilebilir. Kendileri tarafından Üye'ye satılmamış olan malların ayıbından, sistemin üzerinde çalıştığı elektronik altyapıdaki anızalar nedeniyle geç veya yanlış alınan duyuru, promosyon, puanlar vb'den, çeşitli nedenlerle promosyon, puan gibi imkânların Üye'ye sağlanamamasından dolayı oluşabilecek ihtilaflardan Program Ortakları ve Tanı hiçbir şekilde sorumlu tutulmayacaktır. Bu maddedeki koşullar devreye alınacak diğer programlar için de geçerli olacaktır.

4. Tanı veya Üye, 1 hafta önceden bildirimde bulunmak kaydıyla, her zaman ve bir sebep göstermeye gerek olmaksızın üyeliği sona erdirebilirler. Bu durumda 1 hafta içinde üyelik sona erer. Üye, kazandığı haklarından, geçerli koşullar dahilinde, üyelik sona erme tarihine kadar yararlanabilecektir. Üyelik sona erdiğinde kartta biriken puanlar ve Üye'ye kazandırılan haklar Tanı tarafından silinecek ve geri alınacaktır.

Üye, Tanı'ya ve diğer program ortaklarına bu form ile açıklanan ve sair şekilde açıklanacak ve açıklanmış bilgilerinin doğruluğunu, bunlarda değişiklik olması halinde bunları güncelleyeceğini, uyumsuzluk halinde Tanı ve Program Ortaklarının defter ve her türlü kayıtlarının kesin delil sayılacağını, aksi Tanı ve Paro Program ortağı şirket tarafından düzenlenmediği ve duyurulmadığı sürece, Paro Programı'na 18 yaşın üzerinde Türkiye'de yaşayan gerçek kişilerin üye olabileceğini kabul eder.

Yukarıdaki program koşullarını kabul ve beyan ediyorum.

Ad - Soyadı ve İmza:

Lütfen Paro Üyelik Formu'nu
doldurmayı unutmayın.

Tarih: / /

Appendix B.3 The form of “The Declaration of Membership and Consent” of Paro club cards



Migros, Tansaş, Şok, 5M Migros ve Macrocenter marketlerinde cazip fırsatlar

Money Card hakkında bilgi almak için bilgilerinizi doldurun, sizi arayalım.

www.money.com.tr







İLETİŞİM BİLGİLERİ

TCK no:

Soyadınız:

Adınız:

Doğum tarihi:

Migros Club kart no:

İşyeri santral no: 0

Varsa dahili no:

İşyeri direkt no: 0

Ev telefon no: 0

Cep telefon no: 0 5

Tarafınıza verdiğim bilgilerimin aynı zamanda program ortağı Migros Türk T.A.Ş.'ye (Migros) de verilmiş sayılacağını, Bankanız ve Migros'un verdiği hizmetlerin tanıtımı amacı ile benimle temasa geçebilmesi, söz konusu bilgileri işlemesi konusunda yetkili kıldığımı, Banka ve/veya Migros tarafından yürütülen/yürütülecek olan sadakat programları doğrultusunda bu bilgileri kendi program ortakları ile paylaşmasına muvafakat ettiğimi beyan ve kabul ederim.

İmza

BU KISIM MAĞAZA/ŞUBE TARAFINDAN DOLDURULACAKTIR

Satış kanalı:



F 1 - F L B







Appendix B.4 The membership form of Money Card

CarrefourSA Plus Barkodunu Yapıştırınız

Lütfen koyu renk tükenmez kalem kullanınız ve büyük harf ile doldurunuz.

Kişisel Bilgiler

Adınız*

Soyadınız*

Doğum Tarihiniz* Cinsiyetiniz K ☐ E ☐

Ev Adresiniz*
Cadde*
Sokak*
Apt. No* Daire No*
Semt*
İlçe*
İl*
Posta Kodu

Lütfen en az 1 telefon no bildiriniz. (Kampanyadan yararlanmak için cep telefon numaranızı bildiriniz.)

Ev Telefonu

İş Telefonu

Cep Telefonu*

E-Posta*

Haneniz

Hanenizde, siz dahil kaç kişi yaşıyor? (Lütfen x işareti koyunuz)*
☐ 1 ☐ 2 ☐ 3 ☐ 4 ve üzeri

18 yaş altı kaç çocuğunuz var? (Lütfen x işareti koyunuz)*
☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ve üzeri

Kampanyalardan haberdar olmak istiyor musunuz?*
Evet ☐ Hayır ☐

Size hangi iletişim yoluyla ulaşmamızı istiyorsunuz? (Lütfen x işareti koyunuz)
Cep telefonu ☐ E-Posta ☐ Posta ☐

Mesleğiniz;

Ev hanımı ☐ Öğretmen ☐
Memur / İşçi ☐ Orta-üst kademe yönetici ☐
Öğrenci ☐ Kendi hesabına çalışan / Esnaf ☐
Emekli ☐ Uzmanlık Gerektiren meslekler (Doktor, Avukat, Eczacı vs.) ☐

CarrefourSA dışında en sık alışveriş yaptığınız market (Lütfen tek cevap işaretleyin)
Migros ☐ Tansaş ☐ Bim ☐ Semt pazarı ☐
DiaSA ☐ Şok ☐ Kiler ☐ Farketmiyor / Değişiyor ☐
Kipa ☐ Yerel Marketler ☐ Bakkal ☐ Başka yer yok ☐

Evinizde internet erişiminiz mevcut mu ?
Evet ☐ Hayır ☐

İlgi alanlarınız (Lütfen X işareti koyunuz.)*

Ev, bahçe <input type="checkbox"/>	Hırdavat, dekorasyon <input type="checkbox"/>	Moda, tekstil <input type="checkbox"/>
Bakım, kozmetik <input type="checkbox"/>	Kültür, müzik, edebiyat <input type="checkbox"/>	Evcil hayvanlar <input type="checkbox"/>
Dünya mutfak <input type="checkbox"/>	Yöresel mutfak <input type="checkbox"/>	Sağlık ve diet ürünleri <input type="checkbox"/>
Spor <input type="checkbox"/>	Multimedya/ internet <input type="checkbox"/>	Seyahat, tatil <input type="checkbox"/>

GENEL ŞARTLAR
CarrefourSA Plus hamili, CarrefourSA Plus'ın mülkiyetinin CarrefourSA'ya ait olduğunu, CarrefourSA'nın gerekli gördüğünde CarrefourSA Plus'ı iptal edebileceğini ve/veya iadesini talep edebileceğini, işbu başvuru formunda yer alan bilgilerin eksiksiz ve doğru olduğunu, belirlenmiş sürelerin yazısına sınırlı olduğunu, işbu formu verdiğini ve/veya şahısları ilgilendirilerek CarrefourSA tarafından edinilmiş tüm kişisel bilgilerin CarrefourSA tarafından 3. şahıs kişi ve/veya kurumlar ile paylaşılmasına muvafakat ettiğini, kabul beyan taahhüt eder.

Başvuru tarihi* İmza*

G G A A Y Y Y Y

* CarrefourSA Plus kampanya bilgilendirmelerinden ve katılım hakkından yararlanmak için lütfen işaretli alanları doldurun.

Appendix B.5 The membership form of CarrefourSA card

beğendik clubcard KAYIT FORMU

CLUB CARD NO 1 9 8 6 0 0

KİMLİK BİLGİLERİNİZ

ADINIZ _____

SOYADINIZ _____

CİNSİYET ☐ KADIN ☐ ERKEK

DOĞUM TARİHİ (gg/aa/yyyy) ____/____/____ DOĞUM YERİ _____

BABA ADI _____

MEDENİ DURUM ☐ EVLİ ☐ BEKAR

ANNENİZİN KIZLIK SOYADI _____

ÖĞRENİM DURUMUNUZ ☐ İLKOKUL ☐ LİSE ☐ LİSANS ÜSTÜ

☐ ORTAOKUL ☐ ÜNİVERSİTE

ADRES VE TELEFON BİLGİLERİNİZ

MAHALLE _____ CADDE _____

SOKAK _____ APT. NO _____

İLÇE _____ DAİRE NO _____

İL _____ POSTA KODU _____

ÖLKE _____

E-POSTA ADRESİNİZ _____

TELEFON NUMARALARINIZ

EV _____ Alan Kodu : _____

CEP _____ Alan Kodu : _____

AYLIK ORTALAMA NET GELİRİNİZ

☐ 0 - 500 YTL ☐ 501 - 1.000 YTL ☐ 1.001 - 1.500 YTL ☐ 1.501 - 2.000 YTL ☐ 2.001 - ve üzeri YTL

İmza _____

Appendix B.6 The membership form of Beğendik club card

Öğütler "hep güvenle güler yüzle..."

artı kart

Artı Kart Başvuru Formu

Artı Kart No: _____

Kişisel ve İletişim Bilgileriniz

Adınız _____ Soyadınız _____ Doğum Tarihiniz _____

E-İst. _____ Cep İst. _____ Telefon _____

Adres _____

Semt/Bölge _____ İl _____

E-mail _____

Kampanyalarımız için Gerekli Bilgileri

Cinsiyetiniz ☐ Erkek ☐ Kadın

Medeni Durumunuz ☐ Evli ☐ Bekar ☐ Evli Tarihiniz _____ Çocuk Sayınız _____

Eğitim Durumunuz ☐ İlkokul ☐ Ortaokul ☐ Lise ☐ Yüksek Okul ☐ Lisans ☐ Yüksek Lisans ☐

Mesleğiniz ☐ Emekli ☐ Emniyet Görevlisi ☐ Sağlık Personeli ☐ Diğer Kamu Personeli ☐ Serbest Meslek ☐

☐ Emekli ☐ Öğrenci ☐ Ev Hanımı ☐ Diğer _____

Anket Formu

Aylık Geliriniz ☐ 300-600 YTL ☐ 600-1000 YTL ☐ 1000-1500 YTL ☐ 1500 Üzeri YTL

Ankara Yarı ☐ Var ☐ Yok ☐ Marka / Modeli _____

Harcama Kartı Kartınız ☐ Bonus ☐ World ☐ Maximum ☐ Avaraz ☐ Card Finans ☐ Diğer _____

Hobileriniz ☐ Sinema ☐ Yürüyüş ☐ Kitap Okumak ☐ Müzik Dinlemek ☐ Diğer _____

En Çok Dinlediğiniz Radyo ☐ Akı FM ☐ Radyo Ok ☐ Megastar ☐ Radyo D ☐ Radyo Ses ☐ Radyo Ekin ☐

☐ Kral FM ☐ Radyo ODTÜ ☐

En Çok Okuduğunuz Gazete ☐ Hürriyet ☐ Milliyet ☐ Sabah ☐ Star ☐ Akşam ☐ Zaman ☐ Diğer _____

Tarih: ____/____/200____

Bu formdaki bilgilerin doğru olduğunu kabul ederim.

İmza: _____

Appendix B.7 The membership form of Öğütler card