DILEMMA BETWEEN SECURITY AND PRIVACY ON THE INTERNET

A Thesis
Presented to the Institute of Science and Engineering
of
Işık University
In Partial Fulfillment of the Requirements for the Degree of
Master of Science
in
The Department of Information Technology

by
Güven Ayduran

July 2005

Approval of the Institute of Science and Engineering

Prof. Dr. Hüsnü Erbay
Director

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

Prof. Dr. Ergül Akçakaya
Head of 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.

Prof. Dr. Ergül Akçakaya
Co. Supervisor

Prof. Dr. Sıddık B. Yarman
Co. Supervisor

Examining Commitee Members

.... ______________________________

.... ______________________________

.... ______________________________

.... ______________________________

.... ______________________________

ABSTRACT

DILEMMA BETWEEN SECURITY AND PRIVACY ON THE INTERNET

Ayduran, Güven

In this thesis, the following issues are discussed. Even in today society, it is hard to talk about security and privacy. And no one can imagine what will be structure of tomorrow society. We study what are the internet security systems and government security projects. Even we discuss that these systems effect to human rights and privacy. We define importance of cryptography and discuss relation with human rights. We examine internet privacy laws. We also study about George Orwell's book '1984' and consider similarity between novel and real life. We give information about intellectual property and its rights on the internet. We show that intellectual property rights are not enough to protect all properties and these rules are valid for some economic environments. We also discuss issue in instead of knowledge society, creates ignorance society. All these discussed and studied issues show big dilemma to us between security and privacy. The dilemma goes to a result that "there is no security" in today's society.

Keywords: Security, privacy, internet security, internet privacy rights, cryptography, Orwell, intellectual property rights, knowledge society, ignorance society, internet and dilemma.

ÖZET

İNTERNET’DE GÜVENLİK VE MAHREMİYET ARASINDAKİ İKİLEM

Ayduran, Güven

Bu tezde takip edilen konular tartışıldı. Günümüz toplumunda güvenlik ve mahremiyet hakkında konuşmak zordur. Ve geleceğin toplumunun yapısının ne olacağını hiç kimse hayal edemez. İnternet güvenlik sistemleri ve devlet güvenlik projelerinın ne oldukları konusunda çalışmalar yapılmış ve bu sistemlerin insan hakları ve mahremiyetine olan etkileri tartışılmıştır. Kriptografinin önemi tarif edilmiş ve bunun insan haklarıyla olan ilişkisi tartışılmıştır. İnternet mahremiyet kuralları incelenmiştir. George Orwell’in kitabı ‘1984’ hakkında calışma yapılmış ve hikayeyle gerçek hayat arasındaki benzerlik incelenmiştir. Fikri mülkiyet ve internet fikri mülkiyet hakları hakkında bilgi verilmiştir. Fikri mülkiyet haklarının, tüm mülkiyetleri korumakta yeterli olmadığı ve yasaların bazı ekonomik çevreler için geçerli olduğu gösterilmiştir. Bilgi toplumunun yerine bilgisizlik toplumu yaratılmaya çalışıldığı tartışılmıştır. Bütün bu tartışılan ve çalışılan konular, güvenlik ve mahremiyet arasındaki büyük ikilemi göstermektedir. Bu ikilem bizi günümüz toplumunda güvenliğin olmadığı sonucuna götürür.

Anahtar Kelimeler: Güvenlik, mahremiyet, internet güvenliği, kriptografi, internet mahremiyet hakları, Orwell, fikri mülkiyet hakları, bilgi toplumu, bilgisizlik toplumu, internet ve ikilem.

ACKNOWLEDGEMENTS

I would like to express my gratitude to all those who gave me the possibility to complete this M.Sc. thesis.

I would like to express my sincerest gratitude to Prof. Dr. Sıddık Yarman for his invaluable advice and supervision in this thesis work. He was always there to listen and give advice. He is responsible for involving in the thesis in the first place. Also I would like to express my sincerest gratitude, I am deeply indebted and respect to Professor Yurdakul Ceyhun.

I would like to thank my second supervisor to Prof. Dr. Ergül Akçakaya for his understanding and positive aspect to my situation.

I would like to extend my gratitude to my friends, Gürol Erdoğan, Onur İhsan Arsun, Tuncay Kamil Güçlü, Mustafa Yıldız, Burçak Boydak and İnci Taşdemir for giving me great motivation and applying some source documents.

I would also like to thank Laura Saez Zafra for her great understanding and supports.

Last, but definitely not least, I would like to thank my parents for giving me life in the first place, for providing me perfect education. I never pay back their love and supports to me.

TABLE OF CONTENTS

CHAPTER 1.INTRODUCTION

1.1. Preliminary Remarks

In today's society, communication is limited among people by computer technology via internet which grew up from a small town to a big city. The internet isn't controlling security and privacy in these days. People are going to need security extremely in on-line area in the same way as they need it in their normal life. A few computers and computer experts and time are enough to destroy systems. We can name this as cyber terror.

Thus, economy, financial systems, physical construction and commercial life of a country or city can be able to damage or destroy by processing is called hacking and cracking. The internet has entered in our normal life now. We can think and talk about internet security together with social life because terror groups are using the Internet to their aim. It is a terminal for them. They can reach everybody in the world using communication links of the internet.

Some developed countries are using different processing for security. Especially, they put cameras everywhere in the effect of the 'Big Brother'. It is still being discussed nowadays, but that processing is very efficient to catch criminals. Another processing is to mark to people via their credit cards, when they were born. Nowadays, people are being marked in airports. In the middle of the twentieth century, some American services and foundations marked people life and cultural habits of other countries. What was their aim? We can give a lot of examples about marking from past to the present. Obviously, it is the privacy problem in the world.

In addition to privacy is infringing for preventing terror and some companies, countries, people assets. Can we mention about privacy where there is no security? No, we can't because private life, people's thinking and human rights aren’t considered for security of some place and people. What about the security of people? This is a dilemma or paradox. Can we talk about security? What can we do about it? And what had people done about it? I am going to explain from past to present with live instances in the following issues.

1.2. Organization of the Thesis

Structure of thesis is planned following chapters. First chapter includes introduction and organization of thesis. It mentions about how today society should be or shouldn’t be. Normally, people need security for their privacy but in today society, security projects don’t observe people privacy where they are applied by national security and information programs of countries. It examines survey about this issue in the first part.

In the second chapter, I answer if we can talk about security. And I mention about security and its problems from ancient time to recent time. I describe or define what internet and information security are and give information about problems as threats, attacks, hackers, and their damage to governments with pointing figures of the damage. Also I mention about security vulnerabilities in the internet and give examples about big threats. After mentioning those problems, I explain approaches to enhance security and important security techniques as cryptography against hacking, wiretapping and attacks. Then I mention about relation between encryption and human rights. In the end of the second chapter, I explain some security projects which have the common situation that they damaged privacy of many people although they are aim of protection to people security.

In the third chapter, I define the term; privacy. Then, I study historical analysis of privacy and internet privacy laws. I also discuss the relation between privacy and governments. I examine effects of “big brother” [47] on the privacy. The fourth chapter explains what intellectual property and its rights are. Also I discuss intellectual property on the internet. Then I show importance of privacy in the intellectual property and Intellectual property rights are not enough for people because of rules are for companies.

The last chapter gives results and opinions.

CHAPTER 2.SECURITY

2.1. Security Problem

Human being had given high importance their security for preventing threats, attacks in the future from passed time to during time. When we examine the history, people had tried to provide their security with swords, spears, arrow, arc, rock, and stone e.g. these war terms had improved and evolved when industry was born the entire world. Guns, rifles, cannons e.g. had taken instead of old war terms. Those terms had developed and now it is produced terminating weapons to the world with technology has improved highly for every day. Towards the ending of the twentieth century, information and technology has become the best weapon for protecting. Invested countries to science and information are richer, more developed and secure than others. But we can’t say that countries are secure exactly because it is the most important example had become September 11 attacks and followed by lots of terrorist attacks. Corresponding to September 11, it had been over a period in the world and had opened a new period which can call security period. That day had passed to the history as before September 11 and after September 11.

Nowadays, communication systems, electronic data systems of a government, exchange, bank and firm databases must be ready against the external attacks and threats that may appear suddenly. These systems are easy target for hackers and terrorists. It is not necessary to use tons of explosive and bombs for terminating the communication systems.

Age of hackers is decreasing to 13-14 years old in these days. The use of computers and systems learnt so good that people are habit to be hacker timely for testing their self. They are crazy about entering and damaging a system. It is obsession for them. [5] According to report of one of the Gartner searching experts are Victor S. Whetman and American Society for Industrial Security had occurred damaging only in the U.S.A for a year is 1 billion dollars (1.500 quadrillion T.L.) from entering to information systems. It is approximately five times bigger than national budget of Turkey. Again according to the Gartner sources only ‘Code Red’ and ‘Nimda’ viruses had harmed 3 billion dollars (4,5 quadrillion T.L.) worldwide. This is just a little side of ocean. Cyber terror can wound and damage to a country.

The internet, communication and information systems had become the most important power for terror groups. They have made their plans and organizations using unlimited communication process of the internet. They can be able to collect fun and militant to their self. They also can be able to transmit their propagation via link. We know September 11 event that terrorists had given education about making bomb, using gun and camouflaging on the internet. At the same time, they’ve been able to sell drugs with aim of getting money to their organization through the internet. Security and information bureau of countries have functioned intensively against illegal events.

Yes, we can talk about security. We can also say so many things about it because it is the most important issue in these days in the entire world. The world has got security problems and survey. Reason of we can talk about security is that there is no security. All developed technologies is using for being secure. Especially, internet and information technology are highly effective terms to make systems for security.

2.2. Internet Security

[35] Security is the totality of mechanisms and technologies that protect system assets. [36] It is used in a sense of minimizing the risk of exposure of assets and resources to various vulnerabilities. At the same time, [37] it is combination of methods, procedures, hardware, firmware, and software used by

a system to minimize the vulnerabilities of assets and resources. [31] Security refers to fault tolerance against deliberate interaction intrusions from internal and external sources. The most important definition is about security which is privacy that rights and responsibilities that govern the acquisition, disclosure and use of personal information. In addition, security experts are familiar e-mail security, IP security, web security, intruders, alerts and general security pointers for protecting against threats, risks and attacks.

There are three main aspects of information security: confidentiality, integrity, and availability. These protect against the unauthorized disclosure, modification or destruction of information. Confidentiality refers to the property that information is made available or disclosed only to authorized parties. Integrity refers to the property that information is changed only in a specified and authorized manner. [62] According to internet society, the number of internet users has doubled each year. This rapid of growth increased more during the first half of 1994. The internet linked over 3 million host computers worldwide; 2 million of these internet hosts are in the United States. Including users who connect to the internet via public and private messaging services some 20 to 30 million people can exchange over internet.

[62] The use of information networks for business is expanding enormously. The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2 million per day in 1993. An average $800 billion is transferred among partners in international currency markets every day; approximately $1 trillion is transferred daily among U.S. banks; and an average $2 trillion worth of securities are traded daily in New York markets. Nearly all of these financial transactions pass over information networks. Government use of networks characteristics prominently in plans to make government more efficient, effective and responsive. Because of this reason is necessary to protect definitely their information networks and assets.

2.2.1 Security Vulnerabilities

Generally, we can mention about vulnerabilities where security problems are on internet area. These vulnerabilities are

a) Increasing openness of IT systems and wireless communications,
b) Advanced software technologies are cookies, mobile objects or active agents and electronic commerce,
c) Technological gap is between what a computer system can and should enforce,
d) Sociotechnical gap is between social policies and achievable computer system policies,
e) Social gap is between desired social policies and actual human behavior.

One of the biggest problems is hackers. We can describe kinds of hacking that classical threat to security is mostly;

- Eavesdropping, message tampering or replaying,
- Masquerading,
- Exploiting trapdoors or security flaws,
- Password attacks,
- Trojan horse programs.

Other threats are viruses which

- can attach itself to legitimate software, can replicate itself and can perform a malicious act depending on the state of some internal triggers
- worm,
- A particular style of virus which can spread from machine to machine in a distributed system exploiting security gaps as it goes.

2.2.1.1 Some Stories about Threats and Attacks

We can talk some stories about threats and attacks to the internet. For instance, Kevin Mitnick is one of the most popular hacker in the world. U.S government investigated to him a long time and arrested to him. His exploits were hacking into California vehicle database, stealing 20.000 credit card numbers, controlling of telephone switching hubs, hacking into NORAD (North American Aerospace Defense Command). Other instances of information security and privacy problems:

[62] In November 1988, a virus caused thousands of computers on the internet to shut down. The virus's primary impact was lost processing time on infected computers and lost staff time in putting the computers back on line. These event dollar losses are estimated to be between $100,000 and $10 million. Between April 1990 and May 1991, hackers attacked computer systems at 34 Department of Defense sites by weaving their way through university, government, and commercial systems on the internet. The hackers exploited a security hole in the Trivial File Transfer Protocol which allowed users on the internet to access a file containing encrypted passwords without logging onto the system. MIT password file appear as MOTD, Caltech students take over the 1984 rose bowl scoreboard, new labor web site hacked, temporary BT worker obtains phone numbers of Queen, PM, agents..., and Pentagon was hacked.

2.2.2 Approaches to Enhance Security

1) **Security Against Hacking**
    - Encryption: it is conversion of data into a form which is called chiphertext that can’t be easily understood by unauthorized people. It is necessary to understand encrypted data by authorized user. Decryption is the process of the converting encrypted data back into its original form so it can be understood. The more complex the encryption algorithm becomes to eavesdrop difficulty on the communications without access to the key. The encryption and decryption is especially important in wireless communications because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, the encryption / decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online or the discussion of a company secret between different departments in the organization. The stronger the cipher that is harder for unauthorized people to break it.
    - Authentication
    - Access control

2) **Security Against Pest Programs (Threats, Viruses)**
    - Virus checkers
    - Removing trapdoors and security flaws
3) **Underlying Cryptographic Techniques**
    - Secret key encryption (e.g. the data encryption standard)
    - Public-key encryption (e.g. the RSA algorithm)
    - Hybrid schemes (e.g. pretty good privacy(PGP))

2.3 Cryptography

For a long time, mainly before the common use of computers by the public, cryptography has been used only by governments for use in protecting military and diplomatic messages, and by banks to protect and authenticate financial transactions.

2.3.1 Importance of Cryptography

Computer and communications technologies are altering radically the ways in which we communicate and exchange information. Along with the speed, efficiency and cost-saving benefits of digital revolution become new challenges to the security and privacy communications. In response to these challenges, the security mechanisms of traditional paper-based communications media are being replaced by cryptographic security techniques. Communication and information stored and transmitted by computers can be protected against interception to a very high degree through the use of cryptography. Until these days, there was little non-governmental demand for cryptography capabilities. Modern encryption technology was traditionally deployed the most widely to protect the confidentiality of military and diplomatic communications. With the advent of the computer revolution and recent innovations in the science of encryption, a new market for cryptographic products has developed. Electronic communications are now widely used in civilian sector and have become an integral component of global economy. Computers store and exchange an ever-increasing amount of highly personal information which including medical and financial data.

Government regulation of cryptographic security techniques endangers personal privacy. Encryption provides and ensures the confidentiality of personal records, such as medical information, personal financial data and electronic mail.

In a networked environment, such information is increasingly at risk of theft or misuse.

2.3.2 Encryption and Human Rights

[15] In many countries in the world, human rights organizations, journalists and political dissidents are the most common targets of surveillance by government intelligence, law enforcement agencies and other non-governmental groups. The U.S. Department of State, in its 1996 Country Reports on Human Rights Practices, reported widespread illegal or uncontrolled use of wiretaps by both government and private groups in over 90 countries.

In some countries, such as Honduras and Paraguay, the state-owned telecommunications companies were active participants in helping the security services monitor human rights advocates. These problems are not limited to developing countries. French counter-intelligence agents had wiretapped the telephones of prominent journalists and opposition party leaders. The French Commission Nationale de Contrôle des Interceptions de Securité had estimated that there are some 100,000 illegal taps conducted each year in France. There have been numerous cases in the United Kingdom which revealed that the British intelligence services monitor social activists, labor unions and civil liberties organizations. A recent UK bill was enacted that allows for the surveillance of lawyers and priests. In Germany, a bill was currently pending that would allow for the first time since the Nazi era, the ability to bug journalists' offices. The European Parliament issued a report in January 1998 revealing that the U.S. National Security Agency was conducting massive monitoring of European communications. Many human rights groups currently use their encryption to protect their files and communications from seizure and interception by the governments who monitor for abuses.

Thus, most countries in the world today don’t have controls on the use of cryptography. In the vast majority of countries, the cryptography may be freely used, manufactured and sold without restriction. This is true for both leading industrial countries and for countries in emerging markets. The OECD Cryptography Policy Guidelines and the Ministerial Declaration of the European Union, both released in 1997, argue for the liberation of controls on cryptography and the development of market-based, user driven cryptography products and services. These new multi-national agreements have implications for controls that currently restrict the use of cryptography. There are a small number of countries where strong domestic controls on the use of cryptography are in place. These include Belarus, China, Israel, Pakistan, Russia, and Singapore. There are an even smaller number of countries that are currently considering the adoption of new controls. These include India, South Korea and the United States.

2.4 Some Security Projects

2.4.1 Carnivore

[32] Carnivore essentially is a technology that allows the government to wiretap email communications. The internet security system was only included U.S.A. Details of program are still quite vague, and a federal court has ordered that it is examined by a group of independent experts most likely at a university. It unleashed an internet surveillance program called Carnivore which can be set up on any Internet Service Provider (ISP) and be used to search every message that passes through the system for a given bit of information. It controls any entered e-mail addresses. The FBI, who would be primary users of Carnivore, at least initially, insist that Carnivore would be aide them greatly in the interception of relevant email communications related to criminal investigations and nothing

more. They say Carnivore would limit the messages viewable by law enforcement to those allowed only via court order which would include messages only by the person or group under investigation.

2.4.2 Echelon

[50] Echelon is a project of the United States' National Security Agency (NSA). It is a worldwide network for intercepting communications that made headlines in February 1998 when a report from an arm of the European Parliament revealed that telephone, fax, and e-mail traffic in several parts of the world were routinely intercept.

[22] The NSA has many partners. It is the most important function that U.S.A and the U.K had become consortium to each other for "ECHELON" which works for listening process and observation or watching to the entire world. It works using agent satellites in the space and satellite foundations worldwide. Relation between U.S.A and U.K. had started with signing negotiation which name is UKUSA agreement. Then, they had started listening to the world with joining of Canada, Australia and New Zealand timely. After that, Germany, Denmark, Japan, South Korea, Norway, Turkey, China and Netherlands had wanted to enter to that network and anyway they were wanted by founder countries. These countries had joined to UKUSA as "Third Countries".

In addition to observed to the world via Satellites in the space has been listening in people using private listening terms among intercontinental communication cables under deep of the ocean with the echelon system. The internet is the most advantage for the echelon. While it detects circulation, it filters entered key words to the system and records suspicious interviews and writings automatically. Twenty one thousand expert workers in working NSA (National Security Agency) have been analyzing gotten information and then they have been report to superiors that undesirables. It can be able to control all communication terms which is phone interviews, SMS, e-mails, faxes, telex, radio waves and wireless traffic. Those great security systems had failed unsuccessfully in 11 September. Writings and interviews of Terrorists hadn't been aware on the internet and hadn't been warned superior. Thus, NSA invested money seriously to develop Quantum computers for momentum decoding process.

2.4.3 Video Surveillance

[29] Video surveillance is already popular in Europe. It refers to government, commercial, and private surveillance of individuals in public and private places. There has been a particular increase generally in the amount of video surveillance after September 11. Many people are afraid of the increasing use of video surveillance and not just because they fear it will lead to self censorship but because people genuinely don't like being watched like test tube experiments. The greater use of surveillance is to protect government and people's security so people have complacently accepted its use for the most part. Is video surveillance appropriate however for law enforcement, and does it actually provide greater security? These are some of the most complex questions posed by privacy rights activists regarding the use of said surveillance technologies. In Europe video surveillance has not been shown to stop crime significantly more than traditional methods of surveillance.

2.4.4 National ID Cards

[27] Nothing brings to mind privacy concerns to more Americans than National ID cards. Essentially, national ID cards are personal identification cards used to uniquely identify an individual a passport is theoretically such a device although people are not required to have passports at this time. The idea behind the use of national ID cards is to enhance security, unmask potential terrorists and guard against illegal immigration. Such cards are in widespread use in Europe, Malaysia, Hong Kong, Singapore, and Thailand however and there is little evidence that the introduction of such cards created much of a stir in those places. Moreover such cards have greatly increased the efficiency of bureaucracies that utilize them. National ID cards have been proposed in many forms since the 1970's including such schemes as using Social Security Numbers, and biometrics as ID cards, always with widespread opposition.

2.4.5 Microsoft Passport

[28] Passport is Microsoft's online ID and authentication system that stores user information in a central database, and is intended to give Microsoft and Passport affiliates the ability to send unsolicited commercial email (spam) to Internet users and to profile their activities. Microsoft Kids Passport is a particular version of MS Passport that allows parents to consent to the collection of personal information about kids for similar purposes. .NET is Microsoft's platform for delivering centralized web services and is dependent on Passport authentication and identification information. So far Microsoft has managed to steer clear of many of the privacy arguments directed at government, despite the fact that Microsoft technologies are just as intrusive in many ways as many government technologies such as Carnivore and targeted at a greater percentage of the population to boot. Regardless, Microsoft has failed to stir the same

amount of controversy with their Passport system as the government has with Carnivore.

2.4.6 ENUM

[26] ENUM is a technology for storing contact information about oneself, accessible by others, via one number. You could store a fax, voice, and phone number for instance with ENUM in one number and your private information contained in the number would be available to anyone who wished to see it. URI's are likely to be the main system for utilizing ENUM's. URI's are the addressing scheme being promoted to replace the limited system of URL's which are currently used to identify locations based on networks. URI’s would instead identify locations based on some higher order thing than networks.

2.4.7 Operation TIPS

[34] Operation TIPS (Terrorism Information and Prevention System) was one of the first designs of the US Justice Department in the wake of September 11. The idea behind Operation TIPS was that American citizens would be used by law enforcement to spy on their fellow Americans, in an apparent effort to prevent local terrorism. Operation TIPS was defeated in Congress however and never became law.

2.4.8 CAPPS II

[1] CAPPS II is an acronym for 'Computer Assisted Passenger Pre-screening System II'. CAPPS II is still pending congressional review, but if

passed would allow a secret data-mining system to be implemented and used by government to conduct background checks on all airline passengers. The system will be tested around the country at several airports in March 2003. Under CAPPS II, according to the government, citizens will be labeled as either 'red', 'green', or 'yellow' security risks. Red codes would be reserved for those people who are on terrorist watch lists, and it is not clear who would be labeled as 'yellow' but those passengers would be subjected to additional screening. Would this create a permanent blacklist or underclass of Americans who cannot travel freely? The American Civil Liberty Union thinks so. CAPPS II would not only label Americans but the law would make it impossible for Americans to determine their label, or to seek redress if improperly labeled. CAPPS would collect financial data, housing information, communications records, health records, and legal records as well.

CHAPTER 3.PRIVACY

3.1 What is Privacy?

Privacy is a concept like freedom. What privacy means to you may be quite different than what it means to me or to any other person. However, like freedom, privacy is highly valued by most people because they want to live their private life. General idea is the right to be let alone. Computer scientists often equate privacy with confidentiality which places privacy within information security. Lawyers and ethicists define it more as the “right to be let alone” which places it within discussions of freedom. Some advocates say that their personal information belongs to them which turn privacy into intellectual property. Practical definitions and theories of privacy are disappointedly needed as businesses increasingly turn to information technology to enforce norms, principles, business rules and consumer transactions. And the tragic events of September 11 have raised still higher public awareness about privacy, security, and the value and risks of information technology.

3.2 Historical Analysis

Since computer technology joined with our life, important of privacy issue had increased every past day and is increasing highly as a problem in daily life at the world nowadays. Actually, people had lived with privacy violation at life history but although they had known that they lived worse moments, maybe they didn’t know what privacy means. We can make analysis some events from history which kind of privacy infringement it has got.

Firstly, we can go to ancient history for understanding what had happened. In the primitive colonies, they’d sacrificed young girls to their believed gods. This wildness is still continuing rarely in some primitive colonies. The most important analysis is here privacy right of young girls. The first privacy right says that to live upon seclusion. Those girls hadn't had any rights and private things for living. Secondly, at the agricultural society, in the Europe, had slavery and racism. Slaves had just worked for their bosses. They'd been able to talk and go somewhere when their bosses permitted to them. They hadn't done anything without allowing and hadn't had living right in equal and common life. This is horrible privacy violation.

Thirdly, when countries passed to industry society in the world, competition among countries were increasing highly. They were in the competition to be the richest and strongest country. This ambition had pushed to them to secure against others. For instance, in the U.S.A a group of women worked in the Federal Agency had read letters of people randomly. Aim of reading letters looked at any bad idea, plan and operation against U.S.A. When they found any suspicious things, they must convey their superior for investigating. This is to attack to private life of people and an example of government intrusion. Another instance is to mark people when they were born in U.S.A. Although these actions are for people security, at the same time it gives damage to people privacy.

Finally, we are living in the information society. Internet entered to our life with technology develops increasingly. It provides to learn more information, to see easily to the new world what it happens, to communicate people around the world and to share our information with everybody but it is bringing privacy problems enormously and some people can use for their terror attacks and actions too. Security actions of countries are improving nowadays together developed technology. After 11 September, U.S.A marked everybody again. Marking is continuing means to put in front of us huge privacy problem. People had matched privacy problems in the history but it will continue too.

3.3 Internet Privacy Law

[59] Privacy is the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties when that disclosure would cause either embarrassment emotional distress to a person of reasonable sensitivities. Information is interpreted broadly to include facts, photographs, videotapes and disparaging opinions. The right of privacy is restricted to individuals who are in a place that a person would reasonably expect to be private (e.g., home, hotel, room, telephone booth).

The concept of a ‘right to privacy’ was invented more or less in a law review article published in 1980 in U.S.A. The law developed along the following two lines:

- Common law rights protecting individuals from invasion by others
- Federal constitutional rights protecting individuals from government intrusions

3.3.1 Common Law

Common law rights stipulate four instances where individuals have privacy rights, and those are the following:

- Unreasonable intrusion upon the seclusion of another. For example, physical invasion of a person’s home (e.g., unwanted entry, looking into windows with binoculars or camera, tapping telephone), searching wallet or purse, repeated and persistent telephone calls, obtaining financial data (e.g., bank balance) without person’s consent, e.g.

- Appropriation of a person’s name or likeness; successful assertions of this right commonly involve defendant’s use of a person’s name or likeness on a product label or in advertising a product or service. A similar concept is the “right of publicity” in Restatement (Third) Unfair Competition. The distinction is that privacy protects against “injury to personal feelings” while the right of publicity protects against unauthorized commercial exploitation of a person’s name or face. As a particular matter, celebrities generally sue under the right of publicity while ordinary citizens sue under privacy.
- Publicity given to private life or publication of private facts, for instance, income tax data, sexual relations, personal letters, family quarrels, medical treatment, and photographs of person in his/her home.
- Publication that places a person in a false light which is similar to defamation. A successful defamation action requires that the information be false. In a privacy action the information is generally true but the information created a false impression about the plaintiff.

Only the second of these four rights is widely accepted in the U.S.A. In addition to these four pure privacy torts, a victim might recover under other torts such as intentional infliction of emotional distress, assault or trespass. Unreasonable intrusion upon seclusion only applies to secret or surreptitious invasions of privacy. An open and notorious invasion of privacy would be public, not private and the victim could then choose not to reveal private or confidential information. For example, recording of telephone conversations is not wrong if both participants are notified before speaking that the conversation is or may be recorded. There certainly are offensive events in public but these are properly classified as assaults, not invasions of privacy. [59] Other privacy rights are contained in criminal statutes. For instance,

- Surreptitious interception of conversations in a house or hotel room is eavesdropping.
- One has a right of privacy for contents of envelopes sent via first-class U.S. Mail.
- One has a right of privacy for contents of telephone conversations.
- One has a right of privacy for contents of radio messages.
- A federal statute denies federal funds to educational institutions that don't maintain confidentiality of student records which enforces privacy rights of students in a backhanded way.
- Records of sales or rentals of video tapes are confidential.
- Content of e-mail in public systems are confidential.
- Bank records are confidential.
- Library records are confidential in some states.

Furthermore, it is still unclear whether email is private or public information. The law generally legislates in favor of email privacy, but it is often legislated as though it were public information. Moreover, individuals and companies are generally free from prosecution for sending unwarranted emails (spam) which are in some ways a clear invasion of privacy. Has email ever really been private? That question is still largely unanswered, although recent legislation is pointing more and more towards the establishment of email as a public medium for better or worse.

3.3.2 Federal Constitutional Right to Privacy

A more heavily contested area of privacy rights is in the federal arena. Here, many laws have been passed to regulate the right to privacy, either in favor of governmental intrusion or in favor of individual privacy rights.

The typical arguments in favor of privacy intrusion by government, includes government and individual security, enforcement of laws, and efficiency. Efficiency may strike you as strange argument for privacy intrusion. Always remember though that computerized databases as used by the federal government especially are some of the most hotly contested technologies in the battle over privacy rights today. These databases have one purpose and that is the efficient collection, storage, retrieval and sorting of data that is largely what databases are for. The government argues for the right to use these databases on the grounds that they make their jobs easier and better by virtue of making their jobs more efficient. It's a compelling argument.

Since the right to privacy is a relatively new concept, it is not so odd that there is no Amendment in the U.S. Constitution that protects it. Despite this apparent disadvantage, privacy activists routinely point to the fourth Amendment of the U.S. Constitution as their champion of individual rights to privacy. However this Amendment does not clearly specify a right to privacy. [51] It does imply it as you can see yourself from the following excerpt from fourth Amendment:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated , and no Warrant shall issue , but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched , and the persons or things to be seized."

Unfortunately for privacy activists, this excerpt is arguably ambiguous. Therefore it is open to interpretation by many groups including the federal government. In fact, the excerpt has been interpreted by the federal government including courts in many varied ways both for and against individual privacy rights.

3.4 Privacy in the Shadow of Big Brother

It is the most important novel about privacy is belongs to George Orwell who wrote 1984. [47] 1984 sets the standards for paranoia about right of privacy erosion. It is the truly frightening tale of Winston Smith, a ‘drone’ who works at the so-called ‘Ministry of Truth’, essentially the ‘Ministry of Lies’ in doublespeak. Winston’s job is to rewrite history to fit the needs of the ‘inner party’ which the people who essentially control Oceania. Oceania is a country that includes England, South Africa and North America; England is where the story mostly takes place.

The world is a divided place in Orwell’s 1984 and is comprised of three empires, each of which is constantly doing battle with the other two. No details are given on the nature of this combat save that it involves gaining and losing land and bombing. The population of Oceania is divided into three separate groups: 71% ‘proles’, 18% outer party ‘drones’ like Winston, and 1% ‘inner party’ members who effectively run everything. The ‘proles’ are completely ignorant of their situation. The ‘outer party’ makes up the ‘drones’ or what we might call the ‘middle class’ in contemporary terms. The ‘inner party’ works behind a figurehead they call “Big Brother’. Everyone in Oceania assumes ‘Big Brother’ is their leader, when in fact he is just a figurehead for the ‘inner party’.

Orwell’s 1984 is not just the story of Winston however; it is also the story of a totalitarian future where conformity and self-censorship are the methods of ‘inner party’ control. Propaganda such as the’ 2 minute hate’ is practiced regularly by the ‘drones’, under the daily guidance of ‘Big Brother’. Kids are socialized to rat out their parents to the ‘Thought Police’ if their parents say anything against ‘Big Brother’ or if anything suspicious is said or perceived at all by the kids. Sex is essentially outlawed, except for purposes of procreation. Telescreens in every room monitor and make sure people are conforming to daily regimen proscribed by ‘Big Brother’ at all times except when they are sleeping , which is, according to Winston, the only time when they are allowed their own thoughts.

When speaking of modern-day loss of privacy people often refer to ‘Orwellian’ or ‘Big Brother’ schemes. What these people are referring to is the resemblance to the story 1984. George Orwell wrote in his powerful futurist novel 1984. One of the most important points in this novel is that wherever you went, Big Brother was watching you. But 1984 was 21 years ago. Has it all come true, or is it just a bad dream? Walk along any major downtown street, look up and you will probably see cameras bolted to building overhangs looking back at you. Or perhaps you won’t see them. But they are there that at street crossings, inside cash machines, behind mirrors, peering from inside walls, above freeways, in federal parks and in the workplace. Your image could be on its way to millions of viewers on the internet and you wouldn’t even know it. For instance, [54] at a Mariacopa County jail in Arizona, four cameras send out live pictures to an Internet Website, Crime.com. They show the facility’s search area, the holding cells for men and women and the pre-intake area. These images are used without consent and even without the subjects’ knowledge. But the Website assures viewers that the jail’s famously innovative sheriff, Joe Arpaio, “is convinced that the use of the World Wide Web will deter crime.” What rights do prisoners have to prevent such constant snooping and broadcast of their images? For that matter, what rights has anyone under completely normal circumstances?

[54] In New York City in the U.S.A alone, thousands of outdoor cameras are in use. Police credit the machines for curbing crime in the city. With today’s technology, even darkness cannot prevent surveillance by the growing number of video cameras. But the fuzzy lines between social benefits and decreasing privacy from use of such equipment are necessitating scrutiny of their own. According to the Electronic Privacy Information Center, this type of technology

is being referred to as the “fifth utility” and surveillance cameras are profoundly changing the nature of the urban environment and are now an important of the core management of cities. Visual surveillance is becoming a fixed component in the design of modern urban centers, new housing areas, public buildings and even the road systems. The world’s biggest user of such technology is the United Kingdom but United States is catching up.

[42] Another important issue is surveillance of employees. Workers spend their shifts under the scrutiny of hidden video cameras, typing at computers with special software that allows supervisors to monitor everything from the number of errors made to how often breaks are taken. In the United States, when millions of Americans go to work each day, they leave their privacy rights at home because video surveillance is in restrooms, locker rooms and everywhere.

On the other hand, population in big cities with immigration and another reason which is education, job and better life circumstance, is highly increasing as parallel to unemployment and crime ratio. Thus, cities are giving red alarm for security of people around the world. Kidnapping, murder, robbery, assassination, burglary, taking or buying drugs and terrorism are continuing as the most important problems in these days. How can we prevent these crimes? How can police find criminals immediately? It seems the best way to use video cameras for being secure and arresting criminals easily. This method was successful on September 11 although echelon system failed. Terrorists were arrested through videotaped records.

Another example from our country, killer of Üzeyir Garih was fixed using mobile phone conversations records on near assassination time. Developed technology is effective term for police to investigate crimes. Nowadays, governorship of Turkey started to locate video cameras to important points in

Istanbul because of kidnapping is increasing. Here, it should be important goal that just arrests criminals. We should also ask ourselves this question; does this system protect our privacy? Or do we want to be secure from kidnapping? At result, it is becoming paradox or dilemma between security and privacy because when video surveillance and wire-tapping are used, privacy infringement can be but sometimes to use necessarily it for providing people secure.

CHAPTER 4.INTELLECTUAL PROPERTY RIGHTS

4.1 What is Intellectual Property?

Intellectual property is not an ancient principle. It is an explicitly modern notion, having made its debut quite recently. [45] The first patent law was enacted in 1623 and the precursor of modern copyright Statute of Anne came into being in 1710. These early laws were limited in scope and restricted to only a few types of information. The broader interpretation of these principles used today in the western world is quite modern, certain elements having been added only within the last few years. Intellectual property allows people to own their creativity and innovation in the same way that they can own physical property. The owner of intellectual property can control for its use and this encourages further innovation and creativity to the benefit of us all. In some cases intellectual property gives rise to protection for ideas but in other areas, there will have to be more elaboration of an idea before protection can arise. It won't often be possible to protect intellectual property and gain intellectual property rights unless they have been applied for, but some intellectual protection such as copyright arises automatically without any registration as soon as there is a record in some form of what has been created.

[45] There are several main types of intellectual property or ownership of information, including copyright, patents, trademarks, trade secrets, design rights and plant breeders' rights. Copyright covers the expression of ideas such as in writing, music and pictures. It gives the creators of a wide range of material such as literature, art, music, sound recordings, films, and broadcasts, economic rights enabling them to control use of their material in a number ways such as by making copies, issuing copies to be public, performing in public, broadcasting and use on-line. It also gives moral rights to be identified as the creator of certain kinds of material and to object to distortion or mutilation of it.

However, copyright doesn’t protect ideas or such things as names or titles. The purpose of copyright is to permit creators to gain economic rewards for their efforts and the development of new material which benefits us all. Copyright material is usually the result of creative skill and / or significant labor and / or investment and without protection; it would often be very easy for others to exploit material without paying the creator. Patents cover inventions such as new substances or articles and industrial processes. A patent gives an inventor the right for a limited period to stop others from making, using or selling an invention without permission of the inventor. It is an agreement between an inventor and the state in which the inventor is allowed a short term monopoly in return for allowing the invention to be made public. Patents are about functional and technical aspects of products and processes. Most patents are for incremental improvements in known technology. The technology does not have to be complex. Specific conditions must be fulfilled to get a patent. Major ones are that the invention must be new, involve an inventive step and be industrially applicable.

Trademarks are symbols associated with a good, service or company. A trademark is any sign which can distinguish the goods and services of one trader from those of another. A sign includes words, logos, colors, slogans, three-dimensional shapes and sometimes sounds and gestures. Trade secrets cover confidential business information. Design rights cover different ways of presenting the outward appearance of things. Plant breeders’ rights grant ownership of novel, distinct and stable plant varieties that are “invented”.

4.2 What are the Intellectual Property Rights?

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time. They are normally divided into two main areas which are copyright and rights related to copyright and industrial property. In the copyright and rights related copyright, the rights of authors of literary and artistic works such as books and other writings, musical compositions, paintings, sculpture, computer programs and films, are protected by copyright for a minimum period of 50 years after death of the author. Also protected through copyright and related rights are the rights of performers which are actors, singers and musicians, producers of phonograms such as sound recordings, and broadcasting organizations.

The main social purpose of protection of copyright and related rights is to encourage and reward creative work. In the industrial property, industrial property can usefully be divided into two main areas. One area can be specified as the protection of distinctive signs, in particular trademarks which distinguish the goods or services of one undertaking from those of other undertakings, and geographical indications which identify a good as originating in a place where a given characteristic of the good is essentially attributable to its geographical origin. The protection of such distinctive signs aims to stimulate and ensure fair competition and to protect consumers by enabling them to make informed choices between various goods and services.

Other types of industrial property are protected primarily to stimulate innovation, design and the creation of technology. In this category fall inventions which is protected by patents, industrial designs and trade secrets. The social aim is to provide protection for the results of investment in the development of new technology, thus giving the incentive and means to finance research and development activities.

4.3 Intellectual Property on the Internet

According to the United States Information Agency, intellectual property is information that derives its intrinsic value from creative ideas. It is also information with a commercial value. Intellectual property rights are bestowed on owners of ideas, inventions and creative expression that have the status of property. Like tangible property, intellectual property rights give owners the right to exclude others from access to or use of their property.

[14] The concept of intellectual property has been around for a few hundred years. Although the concept has been around for a long time, protection of intellectual property has never been as much of an issue as it is today. Intellectual property was fairly easy to protect. Books, illustrations and reports could all be held in your hands. Even computer software, though trickier to protect, usually resides on disks that can be protected. But the internet makes it a cinch for any personal computer owner to copy and distribute. It publishes virtually anything on the World Wide Web. This powerful technology threatens to make copyright and other intellectual property protection obsolete.

For instance, on one of my friend's web sites he had an original graphic design which is done by one of his friends. The design was interesting and eye-catching, two necessary elements for his site. He had kept the design on the site for over six months before taking it down and rebuilding. Almost a year after the graphic went up on his site; person who designed it had seen it on another site. After he showed my friend, he had expressed his disappointment. He had put his time and hard work into this and someone else had just copied the image off my friend's site and used it for themselves. The design was his friend's work and intellectual property.

The copying of text, sound and graphics has become easy to do but it is extremely hard to detect. With the increased use of the internet and software tools that ease the copying of information, text, sound and graphics can be used without the permission of the author or creator. In recent years, the internet has become both a major front in the battle between proponents of open access to new technologies versus proponents of the protection of proprietary rights and a key source of patent-related information.

Developments in internet technology have been accompanied by an increasingly strategic view of patents by firms seeking to maximize the overall value of their intellectual property. Identifying the creators of works raises problems as new works on the internet may be created and / or adapted by a multiplicity of contributors incapable of differentiation. Similarly, the traditional categories of works which are the subject of copyright protection have been collapsed through the process of digitization such that all digitized works exist in the same type of format capable of being transmitted electronically.

[33] In the past, everyone was at liberty to read a book without breaching copyright but on the internet the mere act of gaining access to a site and perusing its content may infringe copyright even if the work is not downloaded or printed out. Under the existing Copyright act 1968, copyright owners' exclusive rights in relation to the electronic transmission of literary, dramatic or musical works to the public are limited to the right to broadcast the work and the right to cause the work to be transmitted to subscribers to a diffusion service. These rights are limited and don't provide adequate protection for the transmission of copyright works on the internet. There is some evidence that intellectual property infringements generally are being reported more often than in the past. Between 1992 and 1995, for example, the number of copyright and patent offences reported to the Australian Federal police increased 152 per cent. In the United States, over the same period, reports of intellectual property loss incidents

increased 320 per cent to an average of 31 incidents per month in 1995. Losses of more than US $5 billion were reported for 1995.

The copying and illegal sale of hard-copy CDs, videotapes, and DVDs costs the music industry over $4 billion a year worldwide and the movie industry more than $3.5 billion. The internet piracy is primarily a problem for the entertainment and software industries. In fact, it is estimated that when all peer-to-peer services are taken into account more than 2.6 billion files are copied each month. If internet piracy continues unfettered, it will likely increase piracy in both traditional counterfeiting and illegitimate sales over the internet.

The problem of internet piracy did not gain national attention until Napster gained an enormous following in 1999. The original Napster created by college student Shawn Fanning in may 1999. It was an online music service that enabled users to trade digital music files. Napster used a technology known as peer-to-peer networking. P2P networking essentially enables users to link their computers to other computers all across the network. Each user linked to the Napster network was able to share his or her music files with all other users on the network and each user was in turn able to download a copy of any music file on almost any other computer in the network. Napster claimed to have over 20 million users in July 2000, all of them making copies of each others' music. By that time, Napster had become the subject of a massive discussion over online file sharing. Many fans of Napster didn't view downloading music as piracy. They argued that Napster was a tool for music sharing, not stealing. The creators of Napster claimed that they were not responsible for what users did wit their software.

The music industry and especially Recording Industry Association of America disagreed. Several record labels suit against Napster in December 1999 and after months of hearings, Napster was eventually shut down in July 2001.

Other file-sharing services emerged to take Napster's place. Some never gained a wide following of users, while others such as Scour, Grokster, Morpheus and Audiogalaksy were targeted by copyright infringement lawsuits.

In late 2003 one of the most popular file-sharing services was Kazaa. Now other most popular file-sharing services are Imesh and Emule plus. Although legal online music stores such as iTunes and a relaunched version of Napster have begun selling songs for $0.99, users prefer and are still using file-sharing services. However, despite the efforts to fight it and the alternatives that are being offered, online file sharing remains rampant. An estimated 2.6 billion music files are downloaded through peer-to-peer networks each month and more than four hundred thousand movies are downloaded each day. These figures will probably rise as computers become more powerful and broadband internet access becomes more widespread.

The growth of online file sharing demonstrates how new technologies pose a fundamental problem for copyright law. Computers and the internet have made the transmission of information easier than ever before, but the entire copyright system depends on the ability of copyright holders to control the transmission of information specifically to control who has the ability to access and copy their work. The most vehement defenders of online file sharing believe that since the internet has revolutionized the way people access information which is including intellectual property such as music or movies, the law should change as well. John Perry Barlow who is a co-founder of the Electronic Frontier Foundation, had argued that "copyright's not about creation, which will happen anyway it's about distribution."

Applying this view to online music sharing, some defenders of the practice argue that copyright law is not designed to protect musicians for whom it costs relatively little to create songs but instead to reward record companies who make large investments in choosing to produce thousands of CDs. Record companies, according to this logic, benefit society by helping to distribute creators' work, and the law should enable them to make a profit in doing so. But, the argument goes, since the internet has made transmitting information almost free and thus made CDs largely unnecessary as a means of distributing music, record companies are no longer necessary and neither are the laws that make copying songs illegal.

Generally, economic efficiency and common sense argue that ideas should be protected and available for sale just like any other commodity. But intellectual property has come to mean not only the right to own and sell ideas, but also the right to regulate their use. This creates a socially inefficient monopoly and what is commonly called intellectual property might be better called intellectual monopoly. When you buy a potato you can eat it, throw away it, plant it or make it into sculpture. Current law allows producers of a CDs and books to take this freedom away from you. When you buy a potato, you can use the "idea" of a potato embodied in it to make better potatoes or to invent French fries. Current law allows producers of computer software or medical drugs to take this freedom away from you. It is against this distorted extension of intellectual property rights. If there aren't intellectual property rights, we can say that there is no privacy too. Intellectual property rights and privacy depend on each other. These issues should be thought and discussed together in how we can protect creative ideas.

CHAPTER 5.CONCLUSION

In this work, I studied issues of security and privacy on the internet and daily life because the internet includes thinking, opinion, projects, entertainment, politics, education and unlimited information. Obviously, it is part of our life anymore. In today's society, experts and national security agencies make security programs or projects using the internet, information and communication technologies. I explained threats and attacks problem to governments, companies and private groups, and also I gave their damage how much money is lost approximately according to statistical researches. Damage is increasing really high while the internet users are enormously increasing because it is not enough controls, rules and enforcements to protect people rights. I discussed benefit of cryptography to protect data and uncontrolled use of wiretaps by both government and private groups in over 90 countries.

After September 11, importance of security was dramatically increased by developed countries which they care so much their national security. They started to make international security projects immediately without considering privacy and human rights. It was a big mistake because they forgot the fact that if people don't have privacy, they won't be secure. Privacy infringements are seriously continuing with defined security projects which are Carnivore, Echelon, Video Surveillance which is the most important one, Microsoft Passport, National ID Cards, ENUM, TIPS and CAPPS II in this thesis. I believe, these projects and other similar systems and programs should enhance with considering human rights and privacy comprehensively. It should determine limits where are human rights between privacy and security. After that, project can be able to build again. In this way, security can provide but although privacy is considered, dilemma goes to continue. The best solution will be to examine root of problem which is education and exploited to people by countries. People don't want to be much power because they want to be let alone. Security problem starts in this point what people want for living. Do people decide themselves how they live or do governments decide it? Bad politic decisions create spite, money and hatred where people are uneducated. In this way, terrorism and uprising start.

In today, we can say that there are no secure computers. Antivirus and security programs don't pass over being commercial necessity. If you want to be secure certainly from threats and attacks, you should put your computers under the ground but you completely may not be secure again. It isn't enough to turn off the internet. Normally, only information of in your mind can be secure but they can learn through torture by some injection techniques. Some security companies, groups and governments invest to technology for being secure but technology is developing for bad aimed people who are professional computer users, too. Each system can break by them in today's technology.

There never has been privacy any time in the world. Privacy infringement is rising highly with the internet because damage can be from person to person via the internet anymore. Privacy is drowning on the internet. Instead of human agents and old techniques, machines and information technologies get their missions. It is still read letters by some secret people. Won't wire-tapping make? Actually, it can be under inspection or control efficiently because some criminal events need to conversation data but nobody should use except government, and also it should use when police or government need emergency. Taking information for using bad aimed should be prevented.

September 11 showed to us that 2 days were very enough for catching criminals. Credit cards, tickets and videos can give and show many clues to us for investigation. These terms are ways of surveillance. Thousand of outdoor cameras are watching to us in somewhere. This is privacy problem but one question almost is coming on my mind that should I allow that Big Brothers watch me for my security? Anyway they are watching normally. When we think about our security, we don’t consider our privacy thus we are dropping in a paradox. According to me, we should know positive and negative sides about privacy but we shouldn’t waste our money to bring the issue to paranoia situation.

In Turkey, we should focus on the relation of privacy and security seriously. We do not have necessary rights and rules yet. Potential of computer users are raising everyday. If government does not make enforcement widely, government, private groups and companies will loose much many because of threats and attacks. Information awareness should be increased but meaning is not to know how use word and excel. That awareness means to teach how people should use and protect their computer. People should know security vulnerabilities. Another issue is big privacy infringement on the internet in Turkey. Everybody has got mobile phone with camera. They take on and use pictures without permission from picture’s owner on the internet. All of similar events should forbid with rules. Outdoor cameras can put some important points as considering privacy for catching criminals. Substructure workings should be made rapidly with details.

Finally, in this work, we studied, discussed, contested and showed true and wrong ideas, projects e.g. about security, privacy, intellectual property and knowledge society. These issues show to us that dilemma will always be in our life between security and privacy. One important result is that we are not and won’t be secure. We always try to be secure. Human will find new technologies for protecting but bad aimed people will find new technologies for attacking too.

REFERENCES

[1] ACLU, CAPPS II Data-Mining System Will Invade Privacy and Create Government Blacklist of Americans, ACLU Warns, 2003. [Online]. http://www.aclu.org/Privacy/Privacy.cfm?ID=11956&c=130

[2] ACLU, Goverment Activity, 'BIG BROTHER IN THE WIRES: Wiretapping in the Digital Age', Online Newsletter, April 2000.

[3] Ahi M.Gökhan, 'Yarının Hukuku' e.Yaşam, Hürriyet, November 2003, No:13 p.2.

[4] Akkurt, Dursun "Bilgi İşlem Sistemleri için Güvenlik Politikası" and "email Güvenliği", January 2002.

[5] Aksu Halil, 'Teknometre' e.Yaşam, Hürriyet, November 2003, No: 13, p.5.

[6] Baker, C. Edwin, Human Liberty and Freedom of Speech, New York: Oxford University Press, 1989.

[7] Bequai, A., Technocrimes, Lexington Books, Lexington, 1987.

[8] Bereiter, Carl., 'Education and mind in the knowledge age. ', Mahwah, NJ: Lawrence Erlbaum Associates, 2002.

[9] Bob Brewin, "DOD To Brief White House on Hacker Attacks," Federal Computer Week, July 25, 1994, pp.1, 4.

[10] Boldrin M. and D.K.Levine, "Perfectly Competitive Innovation", mimeo, University of Minnesota and UCLA, 2001.

[11] Boldrin, M. and D. K.Levine, "The Case Against Intellectual Property", University of Minnesota and UCLA, January 14, 2002.

[12] Boyle, James, “Conservatives and Intellectual Property”, The National Federalist Society Annual Meeting in Washington DC Published in Engage, Volume: 1, April 2000, p. 83.

[13] Butts, Carter. "Against Intellectual Property.", March 16 1997. [Online] http://www.duke.edu/~eagle/anarchy/intelprop.html

[14] Butts, Carter. "Some myths about intellectual property.", March 16 1997. [Online] http://www.duke.edu/~eagle/anarchy/docs/ipmyths.html

[15] By international human rights organizations is contained in the briefing paper "Encryption in the Service of Human Rights," produced by Human Rights Watch http://www.aaas.org/SPP/DSPP/CSTC/briefings/crypto/dinah.htm

[16] Ceyhun, Yurdakul and Boydak, Burçak, “Yeni Ekonomi, Getirdiği Sorunlar ve Mahremiyet”, Işık University, 2004.

[17] Ceyhun, Yurdakul, ‘Information Communications Course Notes’, IT590, Işık University, 2002.

[18] Chang, Herskowitz, Lee, and Page. "Intellectual Property in the Information Age.", March 26 1997. [Online] http://www.seas.upenn.edu/~cpage/cis590/

[19] Cheng, H. K., “Hacking, computer viruses, and software piracy: The implications of modern computer fraud for corporations”, Corporate Misconduct: The Legal, Societal and Management Issues, Eds M.P. Spencer, M. P. & R. Sims, Quorum Books, Westport, pp.125-47.

[20] Chester, R., “Piracy worst in western world”, Brisbane Courier Mail, April 16, 1996, p.5.

[21] C. Hettinger, Edwin, "Justifying intellectual property", Philosophy and Public Affairs, Vol. 18, No. 1, Winter 1989, pp. 31-52, quotes at pp. 39 and 42.

[22] Çelik Melih, ‘Biri Sizi Gözetliyor’, Byte, April 2004, No: 2004/04 p.62-63-64.

[23] Dempsey, Noel, “Building the Knowledge Society”, Organisation for Economic Cooperation and Development. The OECD Observer, March 2004.

[24] Dayıoğlu, Burak, “Bilim Savaşlarına Hazır Mısınız?”, February 22, 2002.

[25] Elizabeth Sikorovsky, "Rome Lab Hacker Arrested After Lengthy Invasion," Federal Computer Week, July 18, 1994, p.22.

[26] EPIC, ENUM, 2003. [Online]. http://www.epic.org/privacy/enum/

[27] EPIC, National ID Cards, 2003 [Online] http://www.epic.org/privacy/id_cards/

[28] EPIC Sign Out of Microsoft Passport, 2003. [Online]. http://www.epic.org/privacy/consumer/microsoft/

[29] EPIC, Video Surveillance, 2003.[Online]. http://www.epic.org/privacy/surveillance/

[30] European Computer Manufacturers Association. Framework for Distributed Office Applications, ECMA TC32-TG5, Dec. 1986.

[31] F. Lynn McNulty, Associate Director for Computer Security, National Institute of Standards and Technology, "Security on the Internet," testimony presented before the Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994, p.8.

[32] FBI, Carnivore Diagnostic Tool. [Online]. http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm

[33] G. Smith, Russell, ‘Internet Piracy’, Trends & Issues, Australian Institute of Criminology, January 1997, No: 65.

[34] Hentoff, Nat., the Death of Operation TIPS, 2003. [Online]. http://www.villagevoice.com/issues/0251/hentoff.php

[35] International Standards Organization. Addendum to ISO 7498 on Security Architecture, ISO/TC 97/SC 21/WG 16.1.

[36] International Standards Organization. Use of Encipherment Techniques in Communication Architectures. ISO/TC 97/SC 20/WG 3, N66, September 1986.

[37] International Standards Organization. Information Processing Systems-OSI RM. Part 2: Security Architecture. ISO/TC 97 DIS 7498-2, June 1987.

[38] Information Society Commission, "Building the Knowledge Society", Report to Government, December 2002.

[39] Karadere, Tufan, Bilgi Güvenliği, August 26, 2002.

[40] Kinsella, N. Stephan, 'Against Intellectual Property', Journal of Libertian Studies, Spring 2001, Volume :15, No: 2.

[41] Koç Çetin Kaya, 'Network Security and Cryptography Course Notes' Işık University, 2002.

[42] Lewis Charles, 'American Workers Beware: BIG BROTHER IS WATCHING' , USA Today (Magazine), May, 1999.

[43] M. Entman, Robert, Democracy without Citizens: Media and the Decay of American Politics, New York: Oxford University Press, 1989.

[44] Mandeville, Thomas, Understanding Novelty: Information, Technological Change, and the Patent System, Norwood, NJ: Ablex, 1996.

[45] Martin, Brian, "Information Liberation", Chapter III, 1998. [Online]. http://dannyreviews.com/h/Information_Liberation.html

[46] Neocleous Mark, 'Privacy, secrecy, idiocy.', Social Research, Spring, 2002.

[47] Orwell, George. '1984', Can Yayinlari.

[48] Öymen Edip Emil, 'Bilgi Toplumu' e.Yaşam, Hürriyet, November 2003,

No:13 p.5.

[49] Peter H. Lewis, "Hackers on Internet Posing Security Risks, Experts Say," The New York Times, July 21, 1994, pp. 1, B10.

[50] Privacilla, the Electronic Communications Privacy Act, 2002. [Online]. http://www.privacilla.org/government/ecpa.html

[51] Privacilla, the Privacy Protection Act of 1980, 2003. [Online]. http://www.privacilla.org/government/privacyprotectionact.html

[52] Prewitt Kenneth, L.Cohen Jean, M. Mcgovern Theresa, Scarf Maggie, L. Allen Anita, Berman Jerry, Bruening Paula, ‘Is Privacy Now Possible? A Discussion.’, Social Research, Spring, 2001.

[53] Potts Colin, ‘What is Privacy’, Georgia Tech, October 10, 2001.

[54] Ray, Diana, ‘Big Brother Is Watching You – electronic surveillance’, Insight on the News, July 23, 2001.

[55] Report of the Commission on Intellectual Property Rights, ‘Intellectual Property Rights and Development Policy’, London, September 2002. [Online]. http://www.iprcommission.org

[56] Scardamalia, Marlene “Collective cognitive responsibility for the advancement of knowledge.” , In Liberal education in a knowledge society, ed., Barry Smith. Chicago: Open Court, 2002.

[57] Scardamalia, Marlene; Bereiter, Carl; and Lamon, Mary, “The CSILE Project: Trying to bring the classroom into World 3.” In Classroom Lessons: Integrating Cognitive Theory and Classroom Practice, ed., Kate McGilley. Cambridge, MA: Massachusetts Institute of Technology Press, 1994.

[58] Schauer Frederick, J. Garrow David, J.Richards David, ‘Privacy and the Law: The Legal Construction of Privacy.’, Social Research, Spring, 2001.

[59] Standler, Ronald B., Privacy Law in the USA, 1997. [Online]. http://www.rbs2.com/privacy.htm

[60] Survey Methodology, “Worldwide Internet Piracy Study”, A Motion Picture Association of America survey in consultation with Online Test Exchange (OTX), July 2004.

[61] Ueli Maurer, Cryptography, Fundamentals and Applications, Advanced technology seminars, 1998.

[62] U.S. Congress, Office of Technology Assessment, Electronic Enterprises: Looking to the Future, OTA-TCT-600
Washington, DC: U.S. Government Printing Office, May 1994

[63] US Department of Justice, the Privacy Act of 1974, 2001. [Online]. http://www.usdoj.gov/foia/privstat.htm

[64] Vaver, David, "Intellectual property today: of myths and paradoxes," Canadian Bar Review, Vol. 69, No. 1, March 1990, pp. 98-128.