PRIVACY AS INVASION: EFFECT OF MODERN LIFE IN PRIVACY & PROTECTION OF PRIVACY IN THE USA

Tehdit Altında Kişisel Gizlilik: Modern Hayatın Mahremiyete Etkisi ve ABD'de Kişisel Gizliliğin Korunması

Yılmaz ŞİMŞEK[*]

Halil BALTACI[**]

Özet

Teknolojinin gelişmesi ile birlikte polisin kullanmış olduğu taktiklerde de gelişmeler ve yenilikler meydana gelmiştir. Tabi bu yeni taktikler beraberlerinde demokratik toplumlarda mahremiyet (kişisel gizlilik) ile ilgili kaygıların oluşmasına da neden olmaya başlamıştır. Öte yandan, teknolojinin beraberinde getirmiş olduğu bu yeni taktiklerin kanun uygulayıcı için suçun oluşumunun önlenmesi ve oluştuktan sonra suçluların çabuk yakalanabilmesi için gerekli olduğu da bir gerçektir. Hatta bazen elektronik izleme (teknik takip/izleme) kanun uygulayıcının suçun tespitinde, önlenmesinde ve suçluların yakalanmasında kullanabileceği tek yöntem olarak görünmektedir. Bu makalede ilk olarak, özellikle devlet kurumları tarafından gerçekleştirilen, gizli izleme ve dinlemeye karşı kişisel gizliliğin sınırları belirlenmiştir. Teknolojinin gelişmesi ile paralel gelişen kanun uygulayıcının kullanmış olduğu yeni taktiklere karşı mahkemelerin vermiş oldukları özel kararlara bakılmış ve kanun uygulayıcının kullanmış olduğu, bilinen teknolojik taktikler uygulanabilirlikleri açısından incelenmiştir. Sonrasında ise, kişisel gizliliğin güvenceleri olarak görülen başta ABD Anayasası dördüncü madde olmak üzere diğer kanunlar ve içtihat kararları tartışılmıştır.

Anahtar Kelimeler: Teknik Takip, İstihbarat, Polis, Gizliliğin Korunması, İnsan Hakları, ABD Anayasası.

[*] Ph.D., Ankara Police Department, ysimsek@yahoo.com

[**] Ph.D., Police Academy Intelligence Studies Research Center, halilbaltaci@hotmail.com

PBD, 14 (1) 2012, ss.33-58.

Abstract

There has been a significant expansion in the use of undercover police tactics and technological means of surveillance in recent years. Such tactics in a democratic society raise significant questions about privacy. On the other hand, there is no doubt that modern methods of surveillance are a powerful tool, sometimes can be the only way, in the detection and prevention of crime and to reach the suspected activity or criminal. This article evaluates the scope of privacy rights, particularly when a search or some kind of surveillance (wiretap/pan registration) has occurred by governmental agencies. It focuses in particular on the courts' response to developments in surveillance technology used by law-enforcement agencies, and assesses the applicability of technological surveillance tools, used by law-enforcements. Then this study discusses the protection of privacy according to the Fourth Amendment of the U.S. Constitution, and some other laws and major developments in the field.

Key Words: Surveillance Technology, Wiretap, Intelligence, Police, Protection of Privacy, Human Rights, Fourth Amendment.

Introduction

As a result of the industrialization and urbanization in the nineteenth century, there have been great developments in technology, which have affected the amount of privacy enjoyed by people. Together with the developments in surveillance and communication systems and information gathering tools, privacy problems have become more common than before. In other words, using of these new methods of surveillance and information gathering tools, especially by the governmental (law enforcement) agencies, can violate both personal and information privacy more than before (Weaver, 2011).

On the one hand, governmental agencies' use of surveillance and information gathering tools of the information age can increase the privacy concerns, but on the other hand those tools can be the only way to get access to criminals, especially to the modern terrorists and their activities. With the public and the suicide bombers, the nature of modern terrorist activities has been far more terrifying than the nature of old-fashioned terrorism activities. Today, the terrorist activities cannot be controlled without heightened security measures, such as monitoring,

tracking, wiretapping, keeping identification records, intercepting internet activities, eavesdropping on conversations, and using surveillance and face recognition devices in public places. Therefore, some extraordinary measures to enhance security, such as the Patriot Act, increased the scope for U.S. governmental agencies to use information gathering tools, were taken worldwide by the governments especially after the 9/11 tragic event.

Even though, for government agencies to effectively detain terrorists and criminals, information gathering tools used to protect the citizens' individual safety may also invade their rights to privacy. There is no doubt that there is a trade-off between the values of liberty and security. In order not to violate an individual's right, there should be a limit for both liberty and security. Citizens need to see a balance between liberty and security to enjoy the protections of the U.S. Constitution. Therefore, the invasion of privacy and the need for information gathering tools can be determined on the legal basis, the reasonable expectation of privacy and the probable cause of criminality.

This article is about the invasion and the protection of information privacy. It is a detailed analysis of an important social problem, planned to discover the causes of the problem as well as to make future recommendations. However, the main focus is on defining the problem rather than finding solutions as it is essential to recognize the source of the problem before offering any solution to it.

First, there is a detailed literature review designed to provide a frame for the research. In order to understand meaning of information privacy and rising problems related to invasion of privacy by the governmental agencies in the U.S, information privacy and the legal history of privacy invasions in the country are checked in detail. Then, legal protections of information privacy are examined. So as to avoid a one-sided approach to interpreting definitions of the invasion of information privacy, numerous court cases and formal and informal sources relating to different views of the concept are reviewed. Collecting data from numerous different sources is advantageous in addressing a comprehensive perspective for this study (Pope, Lovell and Brandl, 2001; Rubin and Barbie, 2009; Neuman, 2010).

The concept of privacy is broad and comprehensive such as, territorial privacy, personal privacy, and informational privacy (Rosenberg, 1992; Solove, 2004; Solove, 2008). In this study, however, information privacy

and its invasions are explored, only. In this study law enforcement agencies use of advanced information gathering tools, are also explored. Though, invasion of privacy by governmental agencies is mostly secret and hard to investigate, therefore this side of the intelligence can be considered a limitation for the study. Similarly, the secret nature of the subject limits data acquisition from governmental agencies, as well.

The aim of the study is not to find guilt or innocence, but to search invasion of privacy. This study defines the right to privacy, explores the history and meaning of privacy, and explains related concepts and types of privacy. It also argues the need for using developed information gathering tools in order to keep society safe. Then, it focuses on new technologies' impact on the basic privacy right of citizens and. Finally, it explores the individual information privacy rights and protections against governmental invasions. It discusses the U.S. Constitutional privacy rights, interpretations on reasonable expectation of privacy, as well as federal privacy status, state privacy laws and international protections of privacy in general.

1. The Right of Privacy

The right to privacy is not directly mentioned in the Constitution, but the Supreme Court has indicated in the Fourth Amendment, which stops the police and other government agents from searching people's property without a "probable cause" to believe that they have committed a crime (Weaver, 2011). In one sense, privacy means protection against physical intrusions against the person, such as assaults or physical searches by police. It can be the right to protection from intrusions against one's property, such as home. It can also be the right of protection from surveillance by cameras or eavesdropping devices or, perhaps, investigators. It may mean the right not to have your personal belongings and properties be appropriated.

Privacy is also about information. In the 1988 Supreme Court of Canada Dyment decision, Mr. Justice Lamer quoted a task force report about the importance of information privacy: "privacy is at the heart of liberty in a modern state and is essential for the well-being of the individual" (*R. v. Dyment*, 1988:427-428). This notion of privacy (of information) derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain as he see fit. The U.S Supreme Court Justice Louis Brandeis in a

dissenting judgment characterized privacy as "the most comprehensive of rights, and the right most valued by civilized men" (*Olmstead v. US*, 1928).

According to Merriam-Webster's Dictionary (2004) privacy is "the quality or state of being apart from company or observation, or freedom from unauthorized intrusion." A nice and common description on information privacy was given by Alan Westin and Harles Fried, who state "information privacy is citizens' ability to regular information about themselves, and thus control their relationships with other human beings" (Cate, 1997:19). In another description, information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Cavoukian and Tapscott, 1997:12).

The concept of privacy is inseparable from the concept of freedom. As indicated, "The right to privacy has manifested itself in various institutional structures such as respect for the home, the family, and correspondence to, more recently, quarantines against body search, data collection, DNA sampling, telephone tapping, etc" (Guriskin and Hendrics, 2000:224). These structures try to protect private life from all kinds of governmental or other third party invasions and to secure all zones of individual freedom. Also, the U.S. Supreme Court decision shows the territory of the constitutional protection of family life and intimate relationship: "the constitutionally protected privacy of family, marriage, motherhood, procreation, and child rearing is not just concerned with a particular place, but with a protected intimate relationship. Such protected privacy extends to the doctor's office, the hospital, the hotel room, or as otherwise required to safeguard the right to intimacy involved" (Paris Adult Theatre v. Slaton, 413 U.S. 49, 66 n.13, 1973).

To summarize, privacy is the right of a person to be free from unreasonable searches and seizures, to have control on his/her own information and life zone, and to have protection of herself/himself from all kinds of information gathering tools without his/her permission.

1.1. The Effect of Information Age

The problems of freedom posed by the new technology are complex in nature. We may wonder how to protect privacy in a world where it is

possible to record, everywhere and automatically, vast quantities of personal information that can be compiled, transferred and accessed with the greatest of ease. The effect of information age, with its technological and other advances, serves to eliminate or reduce a person's justified expectation of privacy. If you use a computer and surf the World Wide Web, the Internet's open architecture has made you visible to the world (Jennings, Fena, and Dyson, 2000; Youn, 2009). Sharing your name and other identifying personal information can cause you more serious problems: someone else could use that information to commit fraud or other crimes.

In our day, latest developments in technology has decreased the cost of information storing, gathering, transmitting and manipulating (Rubin and Lenard, 2002; Solove, 2004; Youn, 2009). Technological progress produces social change. Although the social and economic impacts of these advances have been positive, they have raised concerns on the part of individuals about what information is being collected, how it is being used and who has access to it. Countless concerned people foresee that their rights of privacy are threatened by the technological progress. The primary concern is whether the current law provides adequate protection for the individual's right to privacy.

Cyber-surveillance efforts can go too far and threaten the liberties of innocent parties (Taslitz, 2002; Solove, 2004). There can be threats to access-control privacy in our daily life, from CCTV to accessing bank and tax information, medical records, school records (i.e., grades), etc. Individual's Social Security number, medical, education and financial databases empower the government to obtain a detailed portrait of any person: the checks s/he writes, the causes s/he supports, and, etc. Modern devices give the law enforcement agencies even "the power to see through the walls of people's homes (Julie, 2000:129)," listen to every phone call, and watch everyone and all information on the computer. Having exposed most areas of individual life to ongoing government scrutiny and recording, Congress is now poised to expand and universalize federal tracking of citizen life (Twight, 1999:165-200).

1.2. Need for Using Information Gathering Tools

Have you ever asked yourself, in the wake of the September 11 terrorist attack, what additional steps could have been taken on the cyber-security side to prevent that tragedy from occurring?

Although the lawmakers and privacy groups are concerned that the government has increased electronic surveillance, keeping up with advances in technology is becoming increasingly difficult. Some agencies, like the FBI, are arrayed to fight crime, and "electronic surveillance is one of the most important and effective, indeed sometimes the only way to deal with the nation's serious crime problem" (Schneier and Banisar, 1997:XV).

Law enforcement agencies have to protect the privacy of communications. However, their primary mission is to enforce the laws. As indicated, "Federal and state prosecutors often comment that arrests and convictions would not have been possible without the use of electronic surveillance" (Schneier and Banisar, 1997:17). Today, the growing use of surveillance technology by law enforcement agencies has focused on prevention of conventional crimes and terrorism applications.

People generally disapprove of police surveillance. However, it can be seen that there is a significant change in people's thinking. In 1974, 80% of the U.S. citizens disapproved of wiretapping, but in 1991, this percentage dropped to 70% (Schneier and Banisar, 1997:27-29). This means that the people started to believe that police surveillance is for prevention of crime, and for their protection (Van Der Ploeg, 2003). Here, the only problem is confidence (Uthmani, Buchanan, Lawson, Scott, Schafer, Fan and Uthmani, 2011).

A basic function of the police is to keep the peace and maintain public order, which requires sensitivity and common sense. On the one hand, public tranquility and reassurance are important goals that can be addressed by strategies such as visible patrols. On the other hand, reactive policing is felt to have limited impact against serious or professional crime, which must be the target of proactive (preventive) policing. Law enforcement agencies have to be able to respond to the crimes of the modern age. This helps people interact safely in communities, and reduces opportunities for criminal acts to occur (Uthmani et. al., 2011). Clearly, there needs to be balance between the competing interests of crime detection and prevention, and the right of the individual to privacy.

2. Some Applications Against Privacy

2.1. Searches

Illegal searches violate privacy rights. According to the Fourth

Amendment to the U.S. Constitution, searches and seizures must be based on a probable cause, or pursued with a warrant. A search warrant has to "be issued by a neutral and detached magistrate capable of determining probable cause" (*Shadwick v. City of Tampa,* 1972), and certainly "describe the place to be searched" (*Steele v. United States,* 1925).

In 1967, the Court held that administrative inspections to detect building code violations must be undertaken pursuant to warrant if the occupant objects (*Camara v. Municipal Court*, 1967). If a police officer merely suspects that someone is about to commit a felony (probable cause), he may stop and frisk the person in a public place, but may not conduct a full-scale search or arrest without additional information (*Terry v. Ohio, 1968*).

2.1.1. Homes

Police must have a warrant or the consent of the resident before entering a home to arrest the occupant (*Payton v. New York*, 1980). The Fourth Amendment is the law of the land on search. It creates several requirements for a lawful search. First, the warrant must be based upon probable cause. Whether there was a probable cause is often disputed in a criminal case, but the courts have given guidance as to when it is present. Probable cause exists, according to the Supreme Court, when the facts and circumstances would cause a person of reasonable caution to believe that a crime had been or is about to be committed. The officer must provide some reasonable basis for seeking a warrant. If the reason given by the officer is inadequate, the warrant and the resulting search are invalid. For a house, a street address usually satisfies this requirement. If the site is in an apartment complex, however, the police must give the specific apartment number. A warrant to search one unit does not authorize police to make a wholesale search of the building.

Over the years since the Constitution was drafted, the courts have carved out some exceptions to the warrant requirements. One of these is the "search incident to arrest" exception. Police have the power to search the area within an arrestee's immediate reach or control. This may include the inside of a car, but is unlikely to include an entire house and garage. Officers also have the right to pursue a fleeing felon into a private home. They must actually be in "hot pursuit" at the time, but if they are, they can follow the suspect into his home, rather than being forced to let him escape. Certain emergency situations, such as being called upon to stop a

violent conflict, locate a missing person, or stop a gunfire emanating from a dwelling, may also justify a warrantless entry. Courts struggle to define which types of emergency situations qualify for a warrant exception.

There are also circumstances that are not protected by the Fourth Amendment. The amendment only applies where a person has a reasonable expectation of privacy. The bedroom is virtually always such a place. But the protections of the amendment decline in more open settings. If a person was engaging in illegal activity on an open porch or patio, the expectation of privacy is diminished because the individual has exposed his actions to neighbors and passers-by. From this type of scenario comes the concept of "plain view." Police are not barred from acting pursuant to evidence of criminal activity that is plainly visible. If police came to a house because someone had reported a gunshot, and the responding officer saw drugs on the table, he would not need a warrant to seize the drugs. This is because the officer had to make no real invasion of the suspect's privacy to locate evidence of a crime.

In the case of *Wilson v. Layne* (1999), the Wilsons filed a lawsuit, asserting that U.S. Marshals and sheriff's deputies violated their constitutional rights by bringing a reporter and photographer into their home, without their permission, while executing a search warrant for their son. The Wilsons' lawsuit argued that officers should be held personally liable for allowing news media to enter homes on raids and arrests. The court held that a media "ride-along" in a home violates the Fourth Amendment, but because the state of the law was not clearly established at the time the entry in this case took place, respondent officers are entitled to be qualified for the immunity. *Wilson v. Layne* (1999), and its companion case *Hanlon v. Berger* (1999), followed recent cases in limiting police prerogatives to choose how to execute warrants in homes. In particular, after the Layne, police no longer have free reign to bring the media along when they enter a home to execute a warrant.

2.1.2. Vehicles

The probable cause to stop any vehicle must be satisfied by conditions existing prior to the policeman's stop. The "reduced expectancy" concept has broadened police powers to conduct automobile searches without warrants, but according to the Fourth Amendment, they must still have probable cause to search a vehicle. Under the Fourth Amendment, police can search items belonging to a passenger of a motor vehicle when they

have probable cause to believe the driver has been involved in a crime, proof of which might be in the vehicle (*Wyoming v. Houghton*, 1999). It is not lawful for the police to undertake a warrantless search of an automobile and extend the search to the passengers therein (*United States v. Di Re*, 1948).

With respect to automobiles, random stops of automobiles to check drivers' licenses, vehicle registrations, and safety conditions were condemned as too intrusive; the degree to which random stops would advance the legitimate governmental interests involved did not outweigh the individual's legitimate expectations of privacy (*Delaware v. Prouse*, 1979). On the other hand, in *South Dakota v. Opperman* (1976) case, the Court sustained the admission of evidence found when police impounded an automobile from a public street for multiple parking violations.

The Supreme Court followed its recent trend of expanding the prerogatives of law enforcement officers to search cars without prior judicial approval. Automobile exception allows warrantless searches of automobiles even when there is no exigency (*Maryland v. Dyson*, 1999); a car subject to forfeiture may be seized from a parking lot without a warrant (*Florida v. White*, 1998); probable cause to search a vehicle for contraband permits the search of passenger's purse, left on the seat of the car (*Wyoming v. Houghton*, 1999).

It is not a search for law enforcement officials to look into an automobile through a window or open door (*United States v. Owens*, 1999). There are two constitutional bases for the automobile exception to the warrant requirement: (1) mobility, and (2) reduced expectation of privacy; without deciding whether an automobile must be operable at time of a search under the automobile exception, Court holds search lawful where officer did not know vehicle was inoperable and had no duty to ascertain functional capability of vehicle (*United States v. Owens*, 1999).

In *Florida v. Bostick* (1991), a police officer boarded a bus and randomly asked for received a passenger's consent to search his luggage. After the passenger told that he could refuse permission to search, the resulting search revealed contraband. The Supreme Court held that as long as the officer's request was not so coercive that the passenger was not free to refuse. The search was a legal consent search, and the passenger, being on the bus, was not free to leave.

2.1.3. People

In *United States v. Watson* (1976), the Court upholds the warrantless search of a suspect in a public place, based on probable cause. This case presents questions under the Fourth Amendment as to the legality of a warrantless arrest. In *United States v. Sokolow* (1989), the search of a suspect at an airport whom federal agents believed might have been smuggling drugs based on certain behaviors was found valid due to the totality of circumstances.

On October 26, 2001, President Bush signed the USA Patriot Act (USAPA) into law. With this law the U.S. law enforcement has been given sweeping new powers, like expanded surveillance with reduced checks and balances. Previously, agents were required at the time of the search or soon thereafter to notify person whose premises were searched that search occurred, usually by leaving copy of warrant. USAPA makes it easier to obtain surreptitious or "sneak-and-peek" warrants under which notice can be delayed. However, because of the Fourth Amendment a judicial finding of probable cause of criminality is still needed for physical searches.

According to Fourth Amendment, in case of an emergency, police can search without a warrant in order to prevent harm or the destruction of evidence. Also, police can stop and frisk someone if they have a reasonable suspicion that they are breaking the law and/or that the suspect is armed, and they can search someone after they lawfully place them under arrest.

2.2. Investigations by Developed Information Gathering Technology

Interception of communications is a main part of using developed information gathering technology (Taslitz, 2002; Solove, 2004). The role of information gathering within the criminal justice organizations has changed meaningfully over time. As communication systems have become more sophisticated the methods of interception have also become more advanced. Technology plays an important role in facilitating deception during covert operations. The proliferation of surveillance technologies has provided law enforcement agencies with new powers to intrude into people's private lives, homes and workplaces. Electronic surveillance, whether through bugging devices, wiretaps, or ready access to encryption keys, is fundamentally at odds with personal privacy, unless

it has a warrant (Weaver, 2011). As will be explained below, entire wiretapping, pen registering and trap-tracing have to be warranted.

2.2.1. Wiretapping, Pen Registration, and Trap-and-trace Device

In order to collect data, there are several ways some of which are using some devices. A wiretap is "a device that acquires the content of an oral, wire or electronic communication --but not including telephone switchboards or hearing aids" (Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510/4). A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which wire or electronic communication is transmitted" (Anti-Terrorism Act –ATA – of 2001, sec.101). A trap-and-trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information relevant to identifying the source or wire or electronic communication" (ATA of 2001, sec.101).

Intercepting a communication needs an application. For an interception order, for wire or oral communications, there have to be serious felonies specifically identified by statute. These crimes typically involve threats to national security, serious bodily harm or death, organized crime, or conspiratorial conduct (18 U.S.C. §2516/a-p). In such cases, only a specified, high-level Justice Department attorney authorizes an application for an interception order (18 U.S.C. §2516/1). For electronic communication, if there is any federal felony, any federal government attorney authorizes an application for an interception order (18 U.S.C. §2516/3).

If there is probable cause that the suspect "has committed, is committing, or is about to commit a crime, and other investigative procedures have failed or will not succeed" (18 U.S.C. §2518/3), "a federal judge can determine for a wiretap interception order for up to 30 days" (18 U.S.C. §2516/1-5). For a pen registration, "a federal judge or a federal magistrate judge determine that the government has provided the information required to be included in the application, for up to 60 days" (18 U.S.C. §3123/a).

If a wiretap interception and pen registration contains any violation of federal law, there may be a fine up to five years for an illegal wiretap

interception (18 U.S.C. §2511/4-a), and a fine up to one year for illegal pen registration (18 U.S.C. §3121/d).

18 U.S.C., relating to both wiretapping and pen registration/trap and trace devices, in accordance with a judicial order, authorizes only within the geographic jurisdiction of the issuing court. The ATA of 2001 (Sections 101 and 108), however, enlarged the jurisdictional authority of a court to authorize the installation and using of information gathering tools anywhere in the U.S.

In the *Nardone v. United States* (1937) case, the Court held that Sec. 605 would be violated by federal officers during wiretapping if the officers both captured and revealed the contents of the discussion they eavesdropped, and that testimony in court could generate a form of prohibited divulgence.

In the *Smith v. Maryland* (1979), the Court held that in response to a warrantless police request, an operator's use of a "pen registration" at the office of the phone company did not violate the Fourth Amendment protection of privacy, because it is known that phone companies save such information for long-distance billing, that subscribers of those companies would not expect that the phones that they dial could remain secret.

In another court decision, in the *Commonwealth v. Rekasie* (2001) case, the court held that a there cannot be a reasonable expectation of privacy for an offender in a telephone conversation with a police informant from his home.

2.2.2. New Devices for Information Gathering

As indicated above, there are various ways and methods to gather information. Therefore, "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping" (Marx, 1996. p39). By the progress in technology, there will be always new devices for information gathering and surveillance. This improvement can also create privacy invasions. The secret nature of the governmental agencies does not permit to access all kind of technological devices that they have used and are using. However, giving a few examples can help to understand how those tools can invade privacy.

Forward-Looking Infrared Radar (FLIR) is one of those new tools that has optical automated sensors to notice temperature differences as slight as one-half degree Fahrenheit, at distances up to a quarter mile, and records its measurements (Julie, 2000:135). Warrantless use of it constitutes a search under the Fourth Amendment, and has reached divergent results. Some courts have found that use of FLIR does not violate privacy. In the *United States v. Ishmael* (1995), the court held police's use of FLIR on open field did not violate Fourth Amendment. Similarly, the courts held that thermal imaging did not constitute a "search" under the Fourth Amendment (*United States v. Myers*, 1995; *United States v. Pinson*, 1994; *United States v. Ford*, 1994). However, in the *United States v. Kyllo* (1998) and *United States v. Cusumano* (1995), the court held that warrantless use of FLIR at home violates the privacy, because the thermal imaging device was capable of revealing intimate details.

Concealed Weapon Detectors (Millivision) is another tool that measures the electromagnetic radiation discharged by the objects. It also converts its readings into a visible form, which exposes any item carried on the person, including those made of metal, liquid, ceramics, plastic and powder (Julie, 2000:141-142). It makes the inside of the living place visible. Therefore, according to the Fourth Amendment, the reasons that FLIR violates the reasonable expectation of privacy can be held also for Millivision depending on the circumstances of its use.

There are other technological tools to get personal information of the citizens, such as Face Recognition, Gas Chromatography, Mass Spectrometry and personal record keeping devices. However, courts have not yet ruled on if warrantless use of those tools violates personal information privacy. The Patriot Act of 2001 also allows governmental agencies to access individual records, such as citizen's creditors, doctors and lawyers, connections and allies, cultural and religious interests, education and income levels, and details on lifestyle, health, travels, beliefs, and etc. There will be new tools by technological improvements in the future, so there will be privacy invasions as well. Therefore, in order to protect privacy, the rule of "reasonable expectation of privacy" should be understood and practiced truly.

3. Protection of Privacy

In the Katz Case (1967, 351-352), Justice Stewart said that The Fourth

Amendment did not protect an individual's information even in individual's home or office, consciously exposed to the public by him; however, it protected personal information even in a public area, preserved as private by him. As it is seen, the U.S. Supreme Court strongly supports protection of privacy. The Supreme Court's current Fourth Amendment jurisprudence is protecting the home above all (Weaver, 2011).

Richard Pipes (1999:117) makes a strong statement that "the state is the guarantor of private-property rights and hence the guarantor of individual liberty." Actually, the warrant system in the U.S. is provides safeguards and the basic warranty against state abuse of searches, seizures, wiretapping and using all other kind of electronic information gathering tools (Weaver, 2011). Moreover, personal privacy is also under warranty of the constitution, federal status and state laws in the U.S.

3.1. Constitutional Framework

3.1.1. Fourth Amendment

There is a rich English experience to draw on. "Every man's house is his castle" was decided in 1603. The right to privacy has established itself in various official structures ranging from home to family since the eighteenth century (Guriskin and Hendrics, 2000). In the eighteenth century, when the Bill of Rights was drafted, the show of state agents breaking into a citizen's home and searching her private diaries was considered the model of an illegal search and seizure (Rosen, 2000; Weaver, 2011). Today, the right to privacy agrees to guarantees against body searches, data collection, DNA sampling, telephone tapping, etc.

Olmstead v. United States (1928) and *Katz v. United States* (1967) are two important examples to show the Fourth Amendment's protection against to technological progress.

Olmstead v. United States: Olmstead was imprisoned for the illegal sale of alcohol. The evidence used against him was gained through the use of an illegal bug engaged on his phone. He claimed to the Supreme Court that his Fourth Amendment rights allowed him a "reasonable expectation of privacy." The Court did not agree with him, and stated that nothing touchable was taken. This verdict was later reversed in 1934, when the United States Congress enacted the *Federal Communications Act*. The Act prohibited the interception of any

communication and the declaration of the contents of intercepted communications.

Katz v. United States: Katz was arrested for illegal gambling after using a public phone to transmit "gambling information." The FBI had engaged an electronic intercepting device onto the public phone booth that Katz consistently used. They argued that this constituted a legal action since they never actually entered the phone booth. The Court, however, ruled in favor of Katz, stating the Fourth Amendment allowed for the protection of a person and not just a person's property against illegal searches. It held that whatever a citizen seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

3.1.1.1. Protection of the Fourth Amendment

The Fourth Amendment protects individuals against unreasonable searches and seizures by the government (Solove, 2004; Weaver, 2011). The Fourth Amendment provides: "The right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated." As a starting point it must be recognized that electronic surveillance and information gathering did not fit the accustomed definition of a search. This position altered when the Supreme Court held that without a warrant, electronic listening and recording of phone conversations created an unreasonable search and seizure that violated the reasonable expectation rule of the Fourth Amendment (*Katz v. United States*, 1967).

The Fourth Amendment makes information collectors responsible to the courts. It restrains the police by telling them that they must have probable cause or a warrant to search and seize. It does not limit the type of the information, as evidence, gathered by the government; however, it limits the means by which that evidence may be gathered (Singleton, 1999). Accordingly, "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A warrant is not required if the arrest occurs in a public place (*United States v. Watson*, 1976). The warrant must be given by a neutral and detached judge capable of determining probable cause (*Shadwick v. City of Tampa*, 1972). Additionally, the warrant must clarify with accuracy the

place to be searched (*Steele v. United States*, 1925), and the things to be seized (*Go-Bart Importing Co v. United States*, 1931).

3.1.1.2. Some Exceptions

There are some exceptions in the case of warrant requirement. Emergency searches (*United States v. Santana*, 1976), automobile searches (*United States v. Ross*, 1982), and "plain view" searches (*Arizona v. Hicks*, 1987) do not necessitate a warrant, but must be dependent upon probable cause.

The following searches require neither a warrant nor probable cause: searches incident-to-arrest (*Chimel v. California*, 1969), "stop and frisk" searches (*Terry v. Ohio*, 1968), inventory searches (*South Dakota v. Opperman*, 1976), and consent searches (*Schneckloth v. Bustamonte*, 1973). In *Hester v. United States* (1924), the Court held that the Fourth Amendment did not protect "open fields", so the police did not require providing warrants or probable cause in such areas.

The main object of the Fourth Amendment is the protection of privacy rather than property because the Fourth Amendment protects people against unreasonable searches and seizures, not places or businesses (Singleton, 1999). In *New York v. Burger* (1987), for example, the Court held that an automotive junk dealer, who is required by statute to save a record for police review of all automobiles and parts in his supervision, has a diminished expectation of privacy in his job. Thus, he had no constitutional protection against a warrantless search of his junkyard. In *California v. Greenwood* (1988), the court held that people have no right to privacy in the garbage.

3.1.2. First Amendment

The First Amendment, which protects speech, affects informational privacy (Solove, 2004). Although it places limitations on the right to informational privacy, it also provides additional information about privacy protection. Because anyone posting messages on the Internet or online services can be considered a "publisher," this Act may prove to have special significance.

3.2. An Important Principle: Reasonable Expectation of Privacy

As quoted, "there is no explicit constitutional guarantee of a right to privacy in the United States" (Cate, 1997:98). When the Constitution was framed, people were not capable for the future changes in technology. However, they made a nice Constitutional frame to protect privacy against the changes in technology: "Reasonable Expectation of Privacy."

Without a reasonable expectation of privacy, however, there would be no privacy right to protect (Weaver, 2011). For example, files stored on disks or tapes at home are protected by a specific law, but the rule becomes less clear when applied to files stored on an Internet access provider's server, so technology creates lots of new privacy invasions. Therefore, the constitution needs to keep up with the changes.

When a new kind of "invasion of privacy" occurs, "reasonable expectation of privacy" helps establish a new case law pertaining to privacy. For these kinds of cases, judges decide according to general laws and the reasonable expectations. Reasonable expectation makes the Fourth Amendment always reliable, valid and timeless, and in that it applies to technological advancements.

When and under what circumstances is it justifiable to infringe personal privacy in the interests of preventing and detecting crime? The interpretations/comments of the Court provide a framework for answering this question. They can also be a frame for reasonable expectation of privacy. According to the Fourth Amendment:

1. There must be a legal basis that is sufficiently accessible and precise so that a person is clear about when interference is permitted.

2. It must be shown to be clear and proportionate.

3. There must be proper methods of accountability over both the authorization and the use of such means.

4. There must be a legal remedy available to those whose privacy has been wrongly invaded.

3.3. Federal Statutes

3.3.1. Electronic Communication Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA, 18 U.S.C. §2510) exactly mentions the interception of communications. It allows

communication between two parties to be recorded and released, but not for the content of the communication to be publicized. For all intents and purposes, the ECPA extended previous prohibitions on the illegal and unauthorized interception of communications to include other practices of electronic communications.

In order to react to new information and communication technologies such as SMS and private internet chat, the ECPA extended prohibition on the unauthorized interception of communications to encompass "other acquisition" to the description of interception of communications. By the expanding the definition of interception, the ECPA makes electronic surveillance a federal crime for an individual, who illegally and intentionally intercept, capture, access, release or use another individual's electronic communication.

The ECPA explains "interception" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Moreover, it explains "electronic communication" as "any transfer or signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate commerce, . . ." (18 U.S.C. § 2510/12). According to the ECPA, the individual, who illegally intercept electronic communications, has both criminal and civil liability for his offense. The criminal punishment for his offence includes up to five years' incarceration and up to $5000 monetary penalty. Furthermore, an accuser who verifies a violation of the ECPA may recover the greater of either: (1) actual damages suffered and any profit made by the violator; (2) for statutory damages (the greater of $100 a day for each day of violation or $10,000); attorneys' fees and trial costs of the plaintiff are recovered as well.

3.3.2. Privacy Act

The Privacy Act of 1974 (5 U.S.C. § 552a) is the main legislation leading the government agencies' acquisition and use of government records holding individual information. The act forbids release of a record without any written permission of the subject of the record with the exception of certain circumstances. These circumstances consist of release for a "routine use" (5 U.S.C. § 552a (b)-3), for law enforcement purposes, and for protecting the health or safety of public or an individual

(5 U.S.C. § 552a-b). This Act also requires that the public must be known about the existence of databases holding individual information (5 U.S.C. § 552a (e)-4).

3.3.3. Supplementary Federal Legislations

There are also some other legislations supporting individual information privacy in the U.S. Those legislations include the Telecommunications Act of 1996 (47 U.S.C. § 153, 1996): protects customer information held by telecommunications carriers; the Internal Revenue Code (26 U.S.C. § 6103, 1994): protects the privacy of taxpayer records; the Family Education and Right to Privacy Act of 1984: disallows the government to disclose information to third parties; the Computer Security Act of 1987 and the Privacy Protection Act of 1988: mandates the government to provide a secure computer storage system to protect individual information of the citizens.

3.4. State Law

State laws also mostly protect an individual's privacy rights in the U.S. A number of states have rulings protecting against the electronic surveillance and interception of communications, like New Jersey's Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1, and Pennsylvania's Wiretapping and Electronic Surveillance Act, 18 Pa. Cons. Stat. Ann. § 5702. California, New York, Virginia, Utah, and Oklahoma, have also privacy laws.

There are four distinct torts protecting the right to privacy: "intrusion, appropriation of name or likeness, unreasonable publicity and false light" (Restatement (Second) of Torts § 652A- 652I). Privacy as guaranteed by the U.S. Constitution differs from privacy protected by tort law. Constitutional privacy protects against invasions by governmental agencies, while state tort laws primarily protects against intrusions by private parties.

3.5. International Rights

Information privacy is also sheltered by international rights, the U.S. has accepted. The International Covenant on Civil and Political Rights, Article 17 puts limits on the state power to manage covert electronic

surveillance on people: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." This protection is also supported by the article 12 of the Universal Declaration of Human Rights.

4. Recommendation

No doubt that there is a strong need for governmental agencies', especially law enforcement agencies' use of electronic information gathering tools to protect people from the criminals and terrorists. Therefore, electronic information gathering mechanism will remain to be used and may have an impact on individual privacy. It will be used for the sake of the greatest good, with a strict control and oversight.

The law and legislations should not be drag behind the developments and changes happening around and not be inadequate towards the crime and criminals. They should make themselves be valid, reliable and everlasting to keep up with the changes and advancements in technology. In addition, the authority of government agencies to use information gathering tools should not be open-ended.

The legal right to privacy is strongly linked to the ethical principle of confidentiality (Guriskin and Hendrics, 2000; Solove, 2004). The courts have to be alerted in terms of balancing the rights of the people. Also, they should make it certain that the main Constitutional protections would stay vital in the future applications regardless of new data collecting technologies.

It is highly possible that if people believe that governmental agencies do not use the information gathering means and tools without probable cause of criminality, there may be a decline in their privacy concerns. They should protect and respect human dignity and support human rights of all individuals.

Conclusion

Privacy means individual freedom and the citizens' ability to protect information about themselves. In addition, it is an inevitable right of people to keep it protected. By the progress in technology, its importance

is increasing every single day because the new information gathering tools make the probability of its invasion easier than ever before.

Whereas nobody was aware of wiretapping, any other surveillance tools or information gathering techniques in the previous century; they became very common today for most of the people. Using those tools and techniques are very important for government agencies to make the country safer and the people more secure, however, they might be threat to privacy, as well. Here, the concern does not merely conflict between right and wrong, but, between right and right, the conflicts that are much harder to resolve. So, technological progress needs new legal decisions for all the crimes and invasions related to it.

Information gathering technologies present a serious challenge to every administrative and legislative system, as well. They try to adapt themselves to the new developments and continually balancing the individual's civil liberties and the needs of society. The U.S. has established a broad and compound Constitutional and statutory system to protect privacy. Its system restricts the ability of government agencies to gather and disclose information about its citizens, but the vitality of these laws is the most important part. Written laws are stable and cannot go ahead with technological progress; however, the reasonable expectation of privacy principle makes the Fourth Amendment vital at all times.

According to Fourth Amendment, the Court has found constitutional violations when the police have searched for or seized records without a warrant, or met one of the exceptions to the warrant's requirement. American citizens have the protection of the Fourth Amendment when there is no reasonable expectation of privacy. Consequently, reasonable expectation always has to be a guide for the police officers, and they have to know and act according to warrants and the "reasonable expectation of privacy" rule.

References

Cate, H. Fred, (1997), *Privacy in the Information Age*, Washington D.C: Brookings Institution Press.

Cavoukian, Ann and Tapscott, Don, (1997), *Who Knows*, New York: McGraw-Hill.

Guriskin, Sofia and Hendrics, Aart, (2000), "The Right to Privacy", Theodore S. Orlin, Rosas, Allan & Scheinin, Martin, (Ed.), *The Jurisprudence of Human Rights Law*, New York: Syracuse Un. Press, pp.223-252.

Jennings, Charles and Fena, Lori & Dyson, Esther, (2000), *The Hundredth Window: Protecting Your Privacy and Security in the Age of the Internet*, New York: Free Press.

Julie, Richard S., (2000, Winter), *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, American Criminal Law Review, Vol.37, No.127.

Marx, T. Gary, (1996), "Ethics for the New Surveillance", Rebecca A Grant & Colin J. Bennett (Ed), *Vision of Privacy: Policy Choices for the Digital Age*, Toronto: University of Toronto Press.

Merriam-Webster Dictionary, (2004), Springfield, MA: Merriam-Webster, Incorporated.

Neuman, Lawrence, (2010), *Social Research Methods: Qualitative and Quantitative Approaches*, Boston: Allyn and Bacon.

Pipes, Richard, (1999), *Property and Freedom*, New York: Alfred A. Knopf.

Pope, Carl, Lovell, Rickie, and Brandl Steven G., (2001), *Readings in Criminal Justice Research*, Belmont, CA: Wadsworth/Thomson Learning.

Rosen, Jeffrey, (2000), *The unwanted gaze: The destruction of privacy in America*, New York: Random House.

Rosenberg, Richard, (1992), *The Social Impact of Computing*, Boston. MA: Academic Press.

Rubin, Allen and Barbie, Earl, (2009), *Essential Research Methods for Social Work*, Belmont, CA: Brooks/Cole.

Rubin, H. Paul & Lenard, M. Thomas, (2002), *Privacy and the Commercial Use of Personal Information*, Boston: Kluwer Academic Publishers.

Schneier, Bruce and Banisar, David, (1997), *The Electronic Privacy Papers*. New York: John Wiley and Sons Inc.

Singleton, Solveig, (1999, December), *Privacy and Human Rights: Comparing the United States to Europe*, Washington, D.C.: Cato Institute.

Solove, Daniel J., (2004), *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press.

Solove, Daniel J., (2008), Understanding Privacy, Boston: Harvard University Press.

Taslitz, Andrew, (2002), "The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions", *Law and Contemporary Problems*, Vol. 65, No. 2, pp.125-187

Twight, Charlotte, (1999, Fall), "Watching You Systematic Federal Surveillance of Ordinary Americans", *Independent Review: A Journal of Political Economy*, Vol. 4, No. 2, pp.165-200.

The U.S.C. Amendment 1st, 4th, 5th, & 14th.

The Anti-Terrorism Act of 2001.

The Electronic Communications Privacy Act of 1986.

The International Covenant on Civil and Political Rights, (1966). UN General Assembly.

The Privacy Act of 1974.

Uthmani, Omair; Buchanan, William; Lawson, Alistair; Scott, Russell; Schafer, Burkhard; Fan, Lu and Uthmani, Sohaib, (2011), "Crime Risk Evaluation within Information Sharing Between the Police and Community Partners", *Information & Communications Technology Law*, Vol.20, No. 2, pp.57-81.

Van Der Ploeg, Irma, (2003), "Biometrics and Privacy A note on the politics of theorizing technology", *Information, Communication & Society*, Vol. 6, No. 1, pp.85-104.

Weaver, Russell, (2011), "The Fourth Amendment, Privacy and Advancing Technology", *Mississippi Law Journal*, Vol. 80, No. 3, pp.1131-1227.

Youn, Seounmi, (2009), "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents", *Journal of Consumer Affairs*, Vol. 43, No. 3, pp.389-418.

Cases

Arizona v. Hicks, 480 U.S. 321, 326 (1987)

Chimel v. California, 395 U.S. 752, 762-73 (1969)

California v. Greenwood, 486 U.S. 35, 108 (1988)

Camara v. Municipal Court, 387 U.S. 523 (1967)

Commonwealth v. Rekasie, 778 A.2d 624 (2001)

Delaware v. Prouse, 440 U.S. 648 (1979)

Florida v. White, 119 S. Ct. 1555 (1998).

Florida v. Bostick, (89-1717), 501 US 429 (1991)

Go-Bart Importing Co v. United States, 282 U.S. 344, 357 (1931)

Hanlon v. Berger, 119 S. Ct. 1706 (1999)

Hester v. United States 265 U.S. 57 (1924)

Katz v. United States, 389 U.S. 347, 351-53 (1967)

Maryland v. Dyson, 119 S. Ct. 2013 (1999)

Nardone v. United States 302 U.S. 379 (1937)

New York v. Burger 482 U.S. 691 (1987)

Olmstead v. United States 277 U.S. 438 (1928)

Paris Adult Theatre v. Slaton, 413 U.S. 49, 66 n.13 (1973)

Payton v. New York, 445 U.S. 573, 576 (1980)

R. v. Dyment, the Supreme Court of Canada, 2 S.C.R.417, (1988)

Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973)

Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972)

Smith v. Maryland, 442 U.S. 735 (1979).

Steele v. United States, 267 U.S. 498, 501 (1925)

South Dakota v. Opperman, 428 U.S. 364, 372-75 (1976)

Terry v. Ohio, 392 U.S. 1, 30-31 (1968)

United States v. Cusumano (67 F.3d 1497, 1506 (1995)

United States v. Ford, 34 F.3d 992, 997 (1994)

United States v. Ishmael, 48 F.3d 850, 857 (1995)

United States v. Kyllo, 140 F.3d 1249, 1254 (1998)

United States v. Myers, 46 F.3d 668, 669-70 (1995)

United States v. Pinson, 24 F.3d 1056, 1058 (1994)

United States v. Ross, 456 U.S. 798, 825 (1982)

United States v. Santana, 427 U.S. 38, 42-43 (1976)

United States v. Watson, 423 U.S. 411, 414, 416-17 (1976)

Wilson v. Layne, (98-83) 141 F.3d 111 (1999)

Wyoming v. Houghton, (98-184) 956 P.2d 363 (1999)