COMMUNICATION ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994:

A CASE STUDY

By: Ali Ozdogan, B.S., M.S.

Thesis Prepared for the Degree of

MASTER OFSCIENCE

UNIVERSITY OF NORTH TEXAS

August 2001

APPROVED:

Bradley S. Chilton, Major Professor and Chair
Robert W. Taylor, Committee Member and Chair of the Department of Criminal Justice
Peggy Tobolowsky, Committee Member
David Hartman, Dean of the School of Community Service
C. Neal Tate, Dean of the Robert B. Toulouse School of Graduate Studies

Ozdogan Ali, Communication Assistance for Law Enforcement Act of 1994: A Case Study. Master of Science (Criminal Justice), August 2001, 179 pp., 1 table, references, 152 titles.

The purpose of this study is: to explore and analyze the Communication Assistance for Law Enforcement Act of 1994 (CALEA), to identify problems related to CALEA, to identify solutions devised by other countries to overcome problems similar to CALEA's, and to propose feasible solutions to CALEA problems.

ACKNOWLEDGMENTS

I would like to acknowledge the Turkish National Police Fellowship I received for this project. Furthermore, I am grateful to the chair of my committee, Dr. Chilton, for his supervision, encouragement, and invaluable discussions. I appreciate helpful discussions and encouragements from Dr. Tobolowsky and Dr. Taylor. I also thanks to Dr. Eric Fritsch, Dr. Gail Caputo, Dr. Tory Caeti, Deanne H. Morgan, and Douglas York. Last but not least, I am grateful to my parents, Osman and Nevriye Ozdogan, for providing motivation, always assuming I would be successful.

TABLE OF CONTENTS

LIST OF TABLE

Table Page

CHAPTER 1

INTRODUCTION, LITERATURE REVIEW AND METHODOLOGY

Telecommunication has been a necessity more than an option in this century. Parallel with the innovations in telecommunications technology, the need for the interception of communications has increased (Diffie & Landau, 1998).

Wiretapping is a traditional and general term used for the interception of communications. This term should not be taken too literally because its use is no longer restricted to the interception of classical wired voice communications. Indeed, wiretapping, as a term, is used for the interception of all forms of communication flowing through both wired and wireless mediums (Diffie, et al., 1998).

Interception, in § 2510 of Title III, is defined as the acquisition of the contents of any oral, wire or electronic communication through the use of any electronic, mechanical, or any other device (Electronic Frontier, 2000).

Wiretapping has developed as an investigative tool within law enforcement in response to advancing communications technology and its effects in society (Freeh, 1999). The use of this tool has been more and more important as telecommunication networks have taken over daily life (Diffie, et al., 1998). Use of wiretapping as an investigative tool requires regulations to minimize or eliminate its possible harmful consequences. Therefore, wiretapping regulations have been created to authorize law

enforcement agencies to use wiretapping as an investigation tool while protecting individuals from its misuse.

In this chapter, first, the historical framework, motivation, scope, and the research question of this thesis are explained. Second, the literature is reviewed. Third, variables, assumptions and limitations of this thesis are explored. Fourth, the methodology of the study is explained. Finally a section is devoted to an overview of the upcoming chapters.

Historical Framework and Motivation of the Present Study

Prior to 1967, there existed a permissive atmosphere that allowed wiretapping to be conducted with minimal regulations (Albanese, 1984). According to Hull (1996), this atmosphere was fostered partially by the 1928 Supreme Court decision in Olmstead v. United States. In Olmstead v. United States (1928), the Court ruled that wiretapping of telephone conversations didn't violate the Fourth Amendment unless it involved an unlawful physical entry to the premises. In Berger v. New York (1967), the U. S. Supreme Court overruled the Olmstead decision by ruling that such conversations fell within the Fourth Amendment's protection, and electronic surveillance of such conversations constituted a search within the meaning of the Fourth Amendment. In the same year, the U. S. Supreme Court, in Katz v. United States (1967) clarified the interpretation of the Fourth Amendment in terms of the right to privacy by stating that the Fourth Amendment "protects the people not the places."

In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act (Title III) to regulate wiretapping while protecting individual privacy rights

(Hull, 1996). Title III authorizes law enforcement agencies to install wiretaps only after a judge makes an ex parte determination that probable cause exists and that other investigative techniques were or would be unavailable (Gruda, 2000). Telecommunications carriers were mandated to assist the law enforcement personnel in the execution of the wiretappings by a 1970 amendment to Title III (Hull, 1996).

The Electronic Communications Privacy Act of 1986 (ECPA) amended protections of Title III against private party eavesdropping and extended Title III's existing legal provisions to new technologies without considering how these technological changes might require different legal responses (Schwartz, 1995). It soon became evident that ECPA's extension of the existing law had not kept pace with the new technologies; therefore, in 1994, the Communication Assistance for Law Enforcement Act (CALEA) was enacted (Ward, 1996). CALEA requires telephone companies to install equipment enabling law enforcement to maintain and facilitate its wiretapping abilities.

It was planned that the first phase of the implementation of CALEA would be completed in October 1998; then, the second phase would begin. However, there has been little implementation done so far, and the Federal Communication Commission (FCC) extended the compliance date from October 25, 1998 to June 30, 2000, and then to March 31, 2001 (Federal Bureau, 2000a; Federal Communications, 1998a; Federal Communications, 2000a). In terms of implementation, the first announcement was made by the Federal Bureau of Investigation (FBI) in September 14, 1999. In the announcement, the FBI announced that the Ameritech Co., as the first company, agreed

to begin to load CALEA compliance software into some communication switches (Federal Bureau, 2000a).

According to the Center for Democracy and Technology (CDT) (1998), CALEA doesn't work. It is evident that there is a significant delay in the implementation. This delay motivates the present study to explore the factors behind the delay and to recommend solutions toward the elimination of these factors.

Problems Related to the CALEA

During the preparation of CALEA, there were long discussions among privacy advocacy groups, telecommunications industry representatives, and law enforcement agencies. According to Congress' reports, CALEA is constitutional and was enacted after numerous compromises between privacy advocates, law enforcement agencies, and congressional and industrial leaders (Dempsey, 1997). On the other hand, the Electronic Frontier Foundation (EFF) argues that the CALEA violates the Fourth Amendment privacy rights, and telecommunications industry representatives argue that it violates the Fifth Amendment property rights (Hull, 1996).

One of the major problems that arises with electronic surveillance in general, and CALEA in particular, is the violation of privacy rights, guaranteed by the Fourth Amendment of the U. S. Constitution (Center for Democracy, 1997a). For example, wiretapping violates the "particularity" requirement of the Fourth Amendment by sweeping all target communications without regard to whether or not they have criminal content (Weil, 1999). In a traditional physical search, law enforcement officers must

leave and obtain a separate order if they wish to return and search again. In contrast, electronic surveillance is an ongoing and continuous process. To be effective, it is conducted without any notice to the parties involved in the communication. According to Weil (1999), this secret nature of electronic surveillance ensures its unconstitutionality.

The second major problem related to CALEA is the governmental taking of private property, guaranteed by the Fifth Amendment (Center for Democracy, 1997a). CALEA mandates that the telecommunications industry retrofits their existing equipment, and design their future systems in such a way as to facilitate governmental wiretapping through such systems. The telecommunications industry claims that such requirements violate their property rights because CALEA provides insufficient reimbursement for the retrofitting, and it provides no reimbursement for future designs (Hull, 1996).

The last major problem related to CALEA is that it hinders the competitive and innovative ability of the U. S. telecommunications industry through its technical requirements (Ward, 1996).

In summary, the opponents of CALEA argue that it violates privacy and property rights guaranteed by the Fourth and Fifth Amendments respectively, and that it hinders the competitive and innovative ability of the U. S. telecommunications industry.

Scope of the Present Study

This study will involve the systematic and detailed description and analysis of the formation, implementation, and evaluation of CALEA from perspectives of the law

enforcement, the telecommunications industry, and privacy advocates. Furthermore, the study involves the exploration of wiretapping laws of Britain, Canada, Germany, France and Turkey in terms of privacy, and property rights. Through these explorations and analyses, the objectives of this study are the following, in order:

- To identify CALEA.
- To make an in-depth analysis of CALEA to determine the problems concerning privacy and property rights.
- To determine possible solutions to the problems related to CALEA by overviewing the wiretapping regulations of a number of countries.
- To generate feasible solutions to CALEA problems.

Research Question

The main question to be addressed by this study is:

- What is the feasible course of action to deal with the problems related to CALEA?

To answer the main question, the following analysis questions have been identified:

- What are the incentives surrounding CALEA?
- Is CALEA socially, economically and legally acceptable?
- Which requirements of CALEA are in conflict with the right to privacy?
- What are the invasion of privacy rights issues with CALEA?
- Which requirements of CALEA are in conflict with the property rights?

- What are the invasion of property rights issues with CALEA?
- Are there similar problems in the wiretapping regulations of other countries? If yes, have they found a solution? If yes, what were their solutions?
- What should be done to eliminate the invasion of privacy right problems related to CALEA?
- What should be done to eliminate the governmental taking of property problems related to CALEA?
- What should be done so that CALEA doesn't hinder the competitive ability of the telecommunications industry?

Literature Review

Literature About Electronic Surveillance and Communication Assistance for Law Enforcement Act of 1994

Schuman (1993) classifies the search and seizure issues into two major categories: communitarian and liberal search and seizure. Unlike liberal search and seizure, the communitarian search and seizure gives higher priority to societal needs than individual rights. Both Schuman (1993) and Gurwitt (1993) defend the communitarian search and seizure. From the communitarian perspective, even if wiretapping violates an individual's right to privacy, it can be carried out to meet societal needs to fight crime. Based on the communitarian search and seizure justification, Diffie and Landau (1998), Freeh (1999), and Colbridge (2000) argue that wiretapping has been an invaluable tool in crime fighting.

Weil (1999) argues that all wiretapping regulations involving CALEA invade Fourth Amendment privacy rights because of their secret, unparticularized, and ongoing nature. In her study, Weil (1999) explores the reasons behind the sudden turnaround – why § 604 of the Intelligence Authorization Act for Fiscal Year 1999 was passed without notice. § 604, including an expansion of the FBI's wiretapping authority, was added after it was passed in the House. Weil (1999) labels such a surreptitious inclusion of § 604 into the bill as "Gestapo tactics". According to § 604, mere suspicion of a suspect's actions is sufficient to initiate a wiretapping. By the mere suspicion criteria, it eliminates the probable cause, a Fourth Amendment requirement. She argues that without the probable cause requirement, the wiretapping may lead to excessive privacy violations, and unacceptable expansion of FBI's discretion on wiretapping. According to Weil (1999), the expanding use of criminal law by the national government exemplifies a trend that conflicts with the careful arrangement of power in the Constitution. Such expansion conflicts with the Articles of Confederation, which doesn't provide for any criminal law authority. The Founders inherently mistrusted central authority to act directly upon individual citizens; therefore, wouldn't support the national police force infringing upon the rights of Americans.

According to Wood (1997), although CALEA does not provide adequate privacy protection in cordless telephone conversations, it provides more privacy protections than the Fourth Amendment because the Fourth Amendment does not clearly articulate the privacy protection.

Nylund (2000) agrees that CALEA does not invade the right to privacy guaranteed by the Fourth Amendment. In his study, Nylund (2000) analyzes the Third Report and Order, involving the technical capability standards of CALEA. The Report was prepared by the FCC after the dispute over the implementation of capability and capacity requirements of CALEA (Federal Communications, 1999c). Following the FCC's adoption of the Third Report and Order in August 1999, five industry associations, three telecommunication companies and four civil liberties groups filed petitions for review in the U. S. Court of Appeals for the District of Columbia Circuit. The central issue in the petitioners' briefs was privacy protection. The petitioners claimed that the FBI's requirements concerning the acquisition of cell site location information for mobile subscriber, dialed digit extraction, and packet-mode communication were not covered by the "call-identifying information" concept of CALEA and they could be subject to Fourth Amendment privacy protections. Nylund (2000) rejects the petitioners' arguments concerning the Fourth Amendment, and he argues that excluding of such requirements contravene primary mandate of CALEA, which is to preserve law enforcement's ability to carry out properly authorized electronic surveillance in the face of rapidly changing telecommunications technology. He argues that even though the main concern was privacy protection, each argument turns on whether the FCC overstepped its authority, or acted in an arbitrary and capricious manner when it promulgated technical standards for CALEA implementation in the Third Report and Order; thereby, the FCC violated the Fourth Amendment. Nylund (2000) argues that the Fourth Amendment creates individual rights against certain government searches and seizures but does not grant

telecommunications carriers any rights to avoid FCC regulations; therefore the Third Report and Order is constitutional and it should be upheld.

Schwartz (1995) argues that CALEA represents law enforcement's demand to keep pace with emerging communications technologies; thereby, it expands law enforcement surveillance capabilities. In fact, the major contribution of CALEA to electronic surveillance capabilities of law enforcement is to mandate the telecommunications carriers to assist law enforcement. Under CALEA, interception of communications effectuated through new technological methods must be initiated on the telecommunications carrier's switching premises, and may only be activated by an affirmative intervention of an employee of the carrier. This restriction implies that the intercept is effectuated by government agents while on the carrier's premises, but without the intervention of the employee of the carrier. According to Schwartz (1995), such a method of "turning on the tap" violates CALEA's security provisions.

According to Schwartz (1995), CALEA improves the privacy protection provisions of ECPA and Title III, and it does not violate the Fourth Amendment privacy rights. In fact, CALEA involves four major contributions to protect the invasion of privacy. First, it requires a court order rather than a subpoena (previously mandated by ECPA) for the disclosure of computer records and other information. Second, it restricts the use of pen registers, trap and trace devices. Third, CALEA amends the existing provisions of Title III, so that the interception of communications between a cordless handset and its base requires a warrant. Finally, CALEA prohibits the possession of

telecommunication instruments for the purpose of obtaining unauthorized telecommunication services.

Like Nylund and Schwartz, Hull (1996) agrees that CALEA does not invade the right to privacy guaranteed by the Fourth Amendment. Hull (1996) claims that the objections regarding the privacy invasion nature of CALEA are unfounded. CALEA enhances the privacy provisions of the Title III by requiring a court order prior to the interception of transactional electronic communications (e.g. electronic mail), and it also enhances the privacy provisions of ECPA by extending the provisions to cordless telephones and certain wireless data transmissions. According to Hull (1996), the real issues are not about the invasion of privacy rights, but about the invasion of property rights. The first property right issue is whether the compliance cost of CALEA must be compensated under the Fifth Amendment. The second issue is that telephone carriers argue that since, theoretically, law enforcement can at all times access the carriers' equipment, such access amounts to a permanent occupation requiring compensation. He agrees that CALEA violates the property rights of the telecommunications industry, so he proposes that a federal "communications tax" be imposed on consumers' telephone calls for the resolution of property right debates. This tax has additional attributes. First, without the tax it is likely that carriers would pass any additional system design costs onto customers in the form of higher rates. Second, if law enforcement may decide that there is no need for wiretapping in some areas, it would decrease the expense of the entire program. Finally, if the cost of compliance is too much, small carriers will not face a competitive disadvantage when upgrading their system.

On the other hand, Nylund (2000) agrees with Hull (1996) in that the real issues are the property rights issues rather than the privacy rights issues. According to Nylund (2000), in petitions of the telecommunication companies and civil liberties groups for reviewing the Third Report and Order in the U. S. Court of Appeals for the District of Columbia Circuit the telecommunication companies' privacy arguments largely seem to be a pretext for economic concerns about the costs of meeting technical standards in the Third Report and Order and the expected loss of future profits because of loss of confidence in the international marketplace which demands secure telecommunications equipment and service. In contrast to Hull (1996), Nylund (2000) argues that CALEA does not violate the Constitutional property rights because the FCC's Third Report and Order conveys an intention to strictly construe the language of CALEA so as to minimize its economic impact on the telecommunications industry. Nylund (2000) also argues that the subscriber will also end up paying for CALEA through either higher taxes or increased telecommunications service rates.

Ward (1996) accuses CALEA of representing poor policies and shortsighted legislative principles. He argues that CALEA hinders the competitive and innovative ability of the U. S. telecommunications industry and puts the industry in a disadvantaged position in the global competitive marketplace by allowing governmental needs to be a determinative factor in the research and development of the carriers and having unclear technical and reimbursement requirements. According to Ward (1996), CALEA offers telecommunications carriers the options of either complying with the act and abandoning their business goals, or pursuing their business goals and paying a fine. Ward (1996)

claims that CALEA should be amended to allow telecommunications carriers the freedom they need to compete in the world's global marketplace.

Literature About Privacy and the Privacy Right

According to Banisar & Davies (1999), privacy is difficult to define and circumscribe. It has roots deep in history. The Qoran, the Bible, early Hebrew culture, classical Greece, and ancient China had substantive privacy protections. These protections mostly focused on the right to solitude.

Definitions of privacy vary widely according to context and environment. Warren and Justice Levis Brandeis was among the first common law scholars to recognize that privacy rights had a central role in the enjoyment of life. They defined privacy as the individual's "right to be left alone" and argued that the invasion of privacy offended the human spirit, an intangible property; therefore, the common law shield should be extended to protect the people from the violation of intangible properties such as dignity, thoughts, emotions, and sentiments. The Preamble to the Australian Privacy Charter states that privacy is a key value underpinning human dignity and freedoms. According to Westin, privacy is the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others. Bloustein defines privacy as an interest of the human personality. According to Gavison, privacy is a combination of three independent and irreducible elements: secrecy, anonymity (the extent to which an individual is the subject of attention), and solitude (the extent to which others have physical access to an individual). In the Calcutt Commission

report, privacy is defined as the right of the individual to be protected in his personal life, home, documents, affairs, or his family (Banisar, et. al., 1999; Craig, 1997). According to Beaney (1966), privacy is the legitimate freedom of an individual to determine the extent to which another individual may a) "obtain or make use of his ideas, names, likeness," and so forth, or b) obtain or reveal "information about him or those for whom he is personally responsible", or c) "intrude physically into his life space". Lusky (1972) defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is to be communicated to others. In Parker's view, privacy is control over when and by whom, the various parts of U. S. can be sensed by others (Banisar, et. al., 1999; Craig, 1997). Banisar, et al. (1999), divides privacy into four categories: information, communication, body and territorial privacy.

As shown from the above definitions, there is much diversity in the meaning of privacy; therefore, it is futile to attempt to develop a perfect definition, but it is preferable to define privacy with a flexible and general definition to accommodate the diverse circumstances relating to privacy (Craig, 1997). Sidney Jourard's definition reflects flexibility and generality. Jourard has linked privacy to the individual's mental health and well-being. He argues that privacy is essential because it allows individuals to escape social pressures for autonomous decision-making, and it creates an environment for everyone to be avoid becoming a victim through pain, depression, anxiety, hopelessness and malaise (Craig, 1997).

Charles Fried has argued that privacy leads to respect, love, friendship, and trust. Close relations can be established by sharing privacy. Surveillance and other privacy intrusions destroy the exclusivity of that sharing, and thereby undermine intimacy, love and friendship (Craig, 1997). According to Marx, privacy invasion through electronic surveillance corrodes the trust between human beings, undermines the basis of social order, and creates paranoia and alienation (Marx, 1988).

Variables, Analysis Criteria, Assumptions, and Limitations of the Study

Variables

In this study, four major variables are identified. These are

- Subjective expectation of individual's privacy that is objectively reasonable.
- Property rights of the telecommunications industry.
- Invasion of the expectation of privacy.
- Invasion of property rights of the telecommunications industry.

Analysis Criteria

- The Fourth Amendment of the Constitution will be used to analyze the subjective expectation of individual privacy that is objectively reasonable.
- The Fifth Amendment of the Constitution will be used to analyze the property rights of the telecommunications industry.
- CALEA's reimbursement provisions explained in §§ 109 and 110, and the compliance costs of the telecommunications industry declared by them will be

used to analyze the invasion of property rights of the telecommunications industry.

Assumptions

- Each individual has the right to privacy.
- The government cannot take private property without sufficient reimbursement.
- Privacy and property rights are Constitutional rights.
- Crime fighting is a societal need and it is carried out by the government.

Limitations of the Present Study

From the perspective of the "public choice theory", CALEA is the outcome of political choices determined by the interests of the stakeholders (BeVier, 1999). To have a rigorous public choice explanation for CALEA, it is essential to know what the intentions of stakeholders were at the beginning of CALEA legislative process and what factors have influenced implementations of these intentions during both legislative and implementation process. Indeed, it is quite difficult to access this information because few of the legislative bargains are in surface in both academic literature and legislative history and published media. In addition, these information sources don't reveal what the hidden agendas had, and what happened in the back rooms or over lunch during the legislative process. From this perspective, I have to admit that the legislative background presented in chapter 3 must be incomplete and insufficient to reveal the nuances and

hidden sides of political and other relevant dynamics. In this speculation, one may question whether it makes sense to find a valid public choice explanation for CALEA; therefore, one questions the validity of the analysis done in this thesis. On the other hand, in this thesis, the analysis is carried out from different perspectives and an extensive review of secondary sources has been conducted to increase validity. It is expected that the analysis made in the present study provide at least an idea about the problematic framework of CALEA and possible solutions to the CALEA problems.

In sum, there is a limitation in data acquisition about CALEA because of the secret nature of wiretapping. In addition to this limitation, there are other limitations:

- Privacy is intangible and has various meanings in accordance with the perceptions of individuals. The highly conceptual nature and the lack of a universally acceptable standard of subjective expectation of individual privacy limit this analysis to some extent. To reduce this limitation, privacy will be used as a proxy variable to analyze the expectation of privacy.
- There is a validity problem in analyzing the invasion of the property rights variable. CALEA mandates that telecommunications manufacturers design their systems in such a way as to comply with the interception requirements of the government. A design must, therefore, be composed of numerous components, which have functions for both normal operations and interception. In such situations, it is difficult to separate the cost of the design for normal operation from the cost of the design for interception facilities.

Therefore, a validity problem is expected in analyzing the invasion of property rights.

- The secret nature of wiretapping may obscure privacy invasions and the biases, which may come up during CALEA's implementation.
- The language problem of the researcher limits direct access to wiretapping regulations of Germany and France. Therefore, second hand information has been used to explore the wiretapping regulations of these countries.
- This study is a social study more than a legal study. Therefore, the legal issues are explored and analyzed by using the social science discipline.

Methodology

This study is a legal and policy analysis using a case study method.

During the analysis, CALEA will be studied without imposing a predefined theory. Instead, a combinatorial approach involving "legal analysis" and "policy analysis" are used. The approach used in the present study is an inductive process and it is interacted with the perspectives presented in the scholarly literature and wiretapping regulations of Canada, Britain, Germany, France, and Turkey to find feasible solutions to the CALEA problems.

Selection of the Research Method

In this study, a case study method is used.

To decide the type of research method, first, the following questions were answered:

- What is the type of (main) research question?
- Is the research going to be focused on contemporary events?
- Is the research going to require control over behavioral events?

The answers to those questions were: "what", "yes", and "no", respectively. According to Yin (1984), the most appropriate research method that fits these answers is the case study method.

The present study has three steps. The first step is the preparation for the case study. In the second step, the data is collected about CALEA and wiretapping issues. In addition, information about the sociopolitical environment surrounding wiretapping in the U. S. is gathered. At the third step, the gathered data is conceptualized and analyzed.

Preparation for the Case Study

Before starting the case study, the relevant basic theoretical, historical and legal knowledge was explored to take advantage of unexpected opportunities, to exercise sufficient care against biases, and to overcome unexpected problems that may come up during the study. For this purpose, relevant chapters of books, for example, Criminal Procedure (Whitebread & Slobogin, 1993), The Changing Supreme Court: Constitutional Rights and Liberties. (Hensley, Smith, & Baugh, 1997), and The Law of Arrest, Search and Seizure (Creamer, 1980) were read and analyzed.

Furthermore, the major stakeholders and their motivations were identified in order to collect data that helps to understand the socio-political environment of CALEA.

Data Collection

Of the six fundamental data sources for case study research identified by Yin (1984), only "documentation" will be used in this study. The data collected is qualitative and it mainly involves the information regarding the legislative history, previous policies, current legislation and the socio-political environment surrounding wiretapping acts.

The data is collected from

- Articles in academic journals and academic web sites such as www.lexis-nexis.com.
- Administrative and legal documents from libraries and web sites of relevant governmental agencies. These documents involve the constitutions, codes, statutes, court decisions, progress reports, consultation papers, proposals, hearings, policies, legislative history of CALEA, and other internal documents concerning the implementation of wiretapping regulations.
- News about the implementation and evaluation of wiretapping and privacy invasion issues in general, and CALEA in particular.
- Books about wiretapping and related subjects.

In determining when the data collection should be stopped, I am constrained by two factors: time available and confidence in the adequacy of the research (Wren & Wren, 1986).

Data Analysis

The data analysis method, used in the present study, has a nested structure involving a policy analysis at the outer frame and a legal analysis at the inner frame. Policy analysis, an interdisciplinary specialty falling under the umbrella of general social sciences, is a process of identifying and evaluating policy alternatives intended to lessen or resolve the social, economic, or physical problems (Einbinder, 2001; Patton, 2001). Legal analysis is an analysis of legal documents to understand the purposes, issues, values, assumptions, variables, and implications inherent therein (Shapo, Walter & Fajans, 1989).

The general framework of the analysis method used in the present study is obtained by combining the eight-step model of the Majchrzak (1984), the pattern-matching model of Yin (1984), and the organized seven-stem approach of Seperich, Woolverton, Beierlein & Hahn (1996). The resulting method is as follows:

1. Identify the legal history of U. S. wiretapping laws and important court decisions before the enactment of CALEA, in order to understand the:
    - Purposes of wiretapping regulations,
    - Definition of the problems addressed,
    - Values and assumptions, inherent in them.

    In identifying the court decisions, the "demonstrative case analysis" and "conclusory case analysis" methods identified by Statsky & Wernet (1984) are used. The main constraints with these methods are the time available, my

tolerance and sophistication and the degree of importance and relevance of the opinion to the subject of the present study.

2. Identify the technological and legal motivations of CALEA.
3. Identify the stakeholders and socio-political dynamics surrounding them.
4. Read and evaluate CALEA carefully and thoroughly
5. Legal analysis of CALEA: To analyze CALEA, first it is dismantled into parts that can be relevant to the purpose of the present study. Second, the secondary sources involving articles, hearings, specific reports, and so forth are reviewed and incorporated in interpretation of each part of the statute. Finally each part of the act is analyzed separately to understand the
    - Purposes,
    - Definition of the problems addressed,
    - Values and assumptions inherent in CALEA,
    - Constraints.
6. Identify the practical implementations of CALEA and analyze the important court cases relevant to the implementation.
7. Identify the central issues subject to the debate among the stakeholders and then separate those central issues from the more trivial issues to accurately determine the causes of the debate.
8. Define the problems related to CALEA.

9. Explore the wiretapping regulations of Britain, Canada, Germany, France and Turkey in terms of privacy and property right issues to find out possible options to solve the CALEA problems defined in the previous step.
10. Identify and develop solutions to the CALEA problems.

Validity and Reliability of the Present Study

To maximize validity, data was collected from multiple sources. For example, the interpretation of CALEA was obtained from documents from the FBI, the Center for Democracy and Technology (CDT), and various law reviews. Then all of the sources were reviewed and analyzed together, and the findings are based on the convergence of information obtained through the reviewed sources.

As well as validity, data collection from multiple sources has the advantage of addressing a broader range of perspectives and attitudes about the issues involved.

Since there is only one researcher, a considerable reliability problem is not expected.

Overview of the Forthcoming Chapters

This thesis involves six chapters including the first chapter. In Chapter 2, the U. S. wiretapping regulations from 1928 Olmstead v. United States to 1986 ECPA are explored. Furthermore, in Chapter 2, the U. S. wiretapping criminal procedure are explored.

Chapter 3 is devoted to CALEA, the last comprehensive U. S. wiretapping legislation. In this chapter, in addition to CALEA itself and subsequent court decisions, background, interpretations, implementation plan of CALEA, and criticisms of stakeholders about the CALEA process are explored.

In Chapter 4, legal positions of Canada, Britain, Germany, France and Turkey with respect to wiretapping are explored. In this chapter, wiretapping issues predominantly related to privacy and property rights issues are overviewed, and they are analyzed with Title III and CALEA.

In Chapter 5, after identifying the stakeholders of CALEA, the problems related to CALEA are determined. Furthermore, some recommendations are made toward the resolution of the problems identified.

The last chapter is a conclusion.

CHAPTER 2

OVERVIEW OF HISTORICAL WIRETAPPING REGULATIONS IN THE UNITED STATES

Electronic surveillance is a broad term that encompasses a number of surveillance techniques, including wiretapping, bugging, the use of beepers, video surveillance, thermal surveillance and so forth. Wiretapping is the interception of the communications involving both call content and call identifying information (Whitebread, et. al., 1993).

Although the use of wiretapping can be traced as far back as the 1920s, the first effort toward regulating its use occurred through Olmstead v. United States (1928), and the first comprehensive federal legislation was passed in 1968. Since then, rapid and continuous innovations in the telecommunications arena have created the need for a rapid, continuous and proactive wiretapping regulation-making process to enable the law enforcement community to keep pace with the emerging telecommunication technologies used by criminals.

This chapter involves two parts. In the first part, U. S. electronic surveillance regulations in general, wiretapping regulations in particular from the 1928 U. S. Supreme Court decision in Olmstead v. United States to pre-CALEA legislation are explored. CALEA, the most recent comprehensive wiretapping legislation, and Court decisions following CALEA are not explored in this chapter. In the second part, the fundamental principles of U. S. wiretapping criminal procedure are overviewed.

Electronic Surveillance and the Constitution

The Fourth Amendment of the U. S. Constitution protects a person, his home, and his papers against unreasonable search and seizure by the government. According to Albanese (1984), the framers of the Fourth Amendment originally intended to protect personal privacy, an issue raised during the physical search and seizure process. As a result, electronic surveillance has historically been subjected to the requirements of the Fourth Amendment.

Although electronic surveillance has not been considered a physical search, it is generally considered more intrusive than a physical search and seizure in terms of privacy. According to CDT (1997a) and Weil (1999), premises underlying this argument are as follows:

- Unlike conventional search and seizure, electronic surveillance always carries the risk of becoming a general search. It sweeps all target communications, allowing for a general unparticularized search, thereby violating the "particularity" requirement of the Fourth Amendment.
- In traditional search and seizure, the subject is informed of the existence and purpose of the search so that the person whose privacy is invaded can observe the search and seek remedy if any violation takes place. However, in order to be effective, electronic surveillance is conducted without notice to involved parties. The inherently secret nature of electronic surveillance, thus threatens privacy rights.

- Electronic surveillance is an ongoing process. The traditional search warrant authorizes law enforcement officers to conduct only one search. If the officers cannot find what they are looking for and if they want to return to search again, they must obtain a new search warrant. Electronic surveillance, in contrast, is carried out over a prolonged period, including one that is several months in length.

Regulation Prior to 1967

The U. S. Supreme Court made its first ruling concerning electronic surveillance in Olmstead v. United States (1928). Federal agents in Washington had obtained evidence through wiretapping in order to convict Olmstead, who had violated the National Prohibition Act. In a five to four decision, the justices held that wiretapping conversations passing over telephone lines did not violate the Fourth Amendment because wiretapping was not a physical entry of the defendant's premises. In addition, because there was no seizure of those tangible things protected by the Fourth Amendment, no search and seizure occurred. As a part of the Olmstead decision, the Court also argued that Congress should regulate the secrecy of telephone messages and the use of wiretap evidence in court (Hull, 1996; Whitebread, et. al., 1993; Wintersheimer, 1988). Through 1967, the Olmstead decision served as the foundation for subsequent Supreme Court decisions regarding electronic surveillance (Albanese, 1984).

In 1934, Congress passed § 605 of the Federal Communications Act of 1934 (FCA), which made federally obtained wiretap evidence inadmissible at trials, thereby

confirming the decision of the Supreme Court in Olmstead (Center for Democracy, 1997a). In addition to prohibiting nonconsensual interception of communications, § 605 also prohibited divulgence or publication of the existence, contents, purport, effect or meaning of such intercepted communications to any person." Furthermore, the Act contained provisions that restricted the admissibility of wiretap evidence in court, provided for the individual rights of calling and called parties, and outlined intrastate and interstate distinctions that affected the law (Center for Democracy, 1997a).

In 1937, the Supreme Court interpreted § 605 as prohibiting the use of wiretap evidence at trial. However § 605 was not effective because several states passed laws based on the Olmstead decision to permit the use of wiretap evidence at trials (Hull, 1996). The interpretation of § 605 was expanded further in 1939, when the Supreme Court in Weiss v. United States, ruled that § 605 also applied to intrastate wiretaps (Whitebread, et. al., 1993).

In 1942, in Goldman v. United States, the Supreme Court held that the evidence obtained by federal agents while monitoring the conversation of Mr. Goldman through the wall by using a detectaphone was admissible in court because interception of private conservations through a detectaphone placed against an office wall did not violate the Fourth Amendment, despite the trespass of adjoining property (Morley, 1993; Whitebread, et. al., 1993). In contrast, in 1961, in Silverman v. United States, the Supreme Court held that interception of private conversations through a microphone concealed in a heating duck at Silverman's house violated the Fourth Amendment because there was a physical intrusion (Morley, 1993; Whitebread, et. al., 1993).

Thus, prior to 1967, the Fourth Amendment was interpreted in such a way that it was applied only when government agents physically searched or seized "houses, papers, or effects" (Wood, 1997).

The FCA, in conjunction with the Supreme Court Decisions, regulated wiretapping until the 1960s. Despite this, there was still no regulation of bugging (i.e. eavesdropping by using mini microphones). Furthermore, the decisions of the federal and state courts muddled the provisions of the FCA until the 1960s. As a result, electronic surveillance activities were carried out on a basis designated by the policies of state administrators and the U. S. Attorney General, rather than the law, until 1967 (Albanese, 1984).

The 1967 Presidential Commission on Law Enforcement and Administration of Justice

The 1967 Presidential Commission did a study and found that the lack of comprehensive Federal prohibition and prosecutive action substantially reduced respect for law. According to the Commission, both private parties and law enforcement were invading the privacy of many citizens without control from the courts and without reasonable legislative standards. The Commission concluded that legislation should be enacted to properly authorize law enforcement to conduct electronic surveillance (Hull, 1996).

Berger and Katz Cases in 1967

Two 1967 decisions of the Supreme Court constituted a landmark in the legal framework of electronic surveillance. Through the Berger and Katz decisions (1967), the Court overruled the Olmstead decision and clarified the interpretation of the Fourth Amendment in terms of invasion of privacy (Albanese, 1984; Hull, 1996; Weil 1999; Whitebread, et. al., 1993).

In Berger v. New York (1967), the agents had obtained evidence through court-ordered wiretapping to convict Berger who had bribed the chairman of the New York State Liquor Authority. Berger claimed that his privacy had been invaded, and the Court agreed. For the first time, the Supreme Court held that "conversation" fell within the Fourth Amendment's protection, and electronic surveillance of such conversations constituted a "search" within the meaning of the Fourth Amendment. Therefore, the Justices held that the court order had to comply with the requirements of a traditional search (Albanese, 1984; Hull, 1996; Whitebread, et. al., 1993). The Court determined that the New York statute that permitted wiretapping was deficient in six areas: (1) it failed to require probable cause that a particular offense had been or was being committed, (2) it failed to have a particularized requirement, (3) it permitted interception of communications irrelevant to the probable cause mentioned in the court order, (4) it failed to have a termination date for the eavesdropping, (5) it didn't let the defendant know that (s)he was subject to eavesdropping, and (6) it failed to require feedback to the judicial branch, which made judicial supervision difficult (Whitebread, et. al., 1993).

In Katz v. United States (1967), the FBI had placed a listening and recording device outside the telephone booth used by Katz, who had violated the federal statute prohibiting telephonic transmission of wagering information over state lines. Katz claimed that his privacy rights had been violated, and the court agreed. The Supreme Court considered two issues in the Katz case. The first issue was if the public telephone booth was an area protected by the Fourth Amendment (so that evidence obtained by attaching an electronic listening recording device to the top of such a booth would be obtained in violation of the right to privacy of the user of the booth). The Supreme Court ruled that the telephone booth is an area protected by the Fourth Amendment. The second issue was if physical penetration of an area protected by the Fourth Amendment was necessary before a search and seizure was said to be violative of the Fourth Amendment. For this issue, the Supreme Court ruled that the physical penetration of an area is not necessary in order for a violation of the Fourth Amendment to occur because the Fourth Amendment protects "the people not the places." Justice Harlan's concurrence in Katz has since been a constitutional standard for Fourth Amendment protections. He outlined a two-prong requirement for the constitutional protection of conversations. First, "a person must have exhibited an actual subjective expectation of privacy" and, second, that "the expectation be one that society recognizes as reasonable" (Katz v. United States, 1967). The Court thus adopted a test of privacy expectations that required a subjective expectation of privacy that society must consider reasonable. Finally, the Court found the FBI's surveillance constitutionally wrong because it had not been conducted pursuant warrant (Hull, 1996; Weil 1999; Wood, 1997).

In summary, in Berger, the Court held that court orders for electronic surveillance must comply with the requirements of a traditional search considered within the meaning of the Fourth Amendment. In Katz, the Court held that electronic surveillance is a "search" within the meaning of the Fourth Amendment; thereby a person's "reasonable expectation of privacy" was protected by the Fourth Amendment (Weil, 1999; Wood, 1997).

Title III of the Omnibus Crime and Safety Streets Act of 1968

In response to the constitutional standards outlined in the Berger and Katz decision, as well as the recommendations of the 1967 Presidential Commission, Congress quickly enacted Title III of the Omnibus Crime and Safety Streets Act of 1968. Title III, the first comprehensive electronic surveillance legislation in the U. S., has become the foundation of U. S. electronic surveillance legislations.

Congress defined the two purposes of Title III as: "(1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized" (Hull, 1996; Weil 1999).

Title III had the following components (Weil, 1999):

- Wiretapping would be permitted only for specified crimes.
- Wiretapping is authorized only as a last resort.
- Wiretapping could be executed pursuant to a warrant based on probable cause.
- Wiretapping without a warrant would be outlawed.

- Wiretapping would be carried out in such a way as to minimize the interception of innocent (i.e. irrelevant to the offense) conversations. This minimization is essential to satisfy the Fourth Amendment's "particularity" requirement.
- Notice would be provided after the investigation had been concluded.
- Evidence obtained without probable cause is not admissible in court.

Important Court Decisions from 1968 to 1986

The original Title III contains no guidance concerning the responsibilities of telecommunications carriers in assisting law enforcement with electronic surveillance. In 1970, the U. S. Court of Appeals for the Ninth Circuit decided that telecommunications carriers had no obligation to assist lawful wiretaps. This decision pushed Congress to revise Title III. Two months after the decision, Congress added a provision which mandated telecommunications carriers to technically assist law enforcement with electronic surveillance. The provision also required that the applicant (law enforcement) reimburse the carrier for the "reasonable expenses" involved in providing such assistance (Hull, 1996; S. Rep. No. 103, 1994).

In United States v. New York Telephone Co., the U. S. Supreme Court ruled that the telephone company had an obligation to provide the FBI with technical assistance in conducting electronic surveillance of two telephone lines used in a gambling business. Although the Supreme Court based this decision on the All Writs Act, rather than Title III, the Court stated that, even if Title III had applied, the 1970 Amendment would lead to

the same result. This decision ensured that wiretapping was a judicially accepted law enforcement tool (Hull, 1996).

In 1973, in United States v. Hall, the U. S. Court of Appeals for the Ninth Circuit held that conservation between a mobile and landline telephone was a wire communication, and that conservation between two mobile phones was categorized as an oral communication. This oral/wire classification is important because there is a more reasonable expectation of privacy in wire communications than that in oral communications. The Court concluded that the privacy protection of Title III was only applied to the communications between a mobile and a landline phone, and communication between two mobile phones was protected by Title III only if a reasonable expectation of privacy existed (Wintersheimer, 1988; Wood, 1997). On the other hand, in State v. Delaurier (1985), the Supreme Court of Rhode Island declined to follow the Hall decision. The Court held that there was no reasonable expectation of privacy in conversations through cordless phones. The court reasoned that the owner's manuals stated that privacy was not ensured, as required by the FCC (Wood, 1997). In Edwards v. Bardwell (1986), the U. S. District Court for the Middle District of Louisiana held that in the case of the existence of radio waves at either side of a communication, the conversation was counted as an oral communication under Title III. The court also held that there was no reasonable expectation of privacy in a communication broadcasted by radio in all directions to be heard by countless people (Wood, 1997).

In United States v. Kahn (1974), the U. S. Supreme Court held that wiretapped evidence could be used against a defendant for whom the warrant had not been issued.

Mr. Irving Kahn was convicted through wiretap evidence. Some of the wiretapped telephone conversations that had been used in the conviction were extracted from conversations between Irving and his wife, Minnie. Minnie claimed that the wiretap evidence involving her could not be used to accuse her because the warrant had been issued only for Irving. The Court held that the evidence could be used against Minnie, even though the warrant had not been issued to intercept her conversations, because, according to the language of Title III, a person must be identified only if that individual was known to be committing an offense that subject to interception (Wintersheimer, 1988).

In United States. v. Miller (1976), the Supreme Court ruled that the Fourth Amendment did not protect the privacy concerns of the business records of individuals (Center for Democracy, 1997a).

In United States v. Donovan (1977), the U. S. Supreme Court held that evidence obtained against a person whose name had inadvertently been omitted on the warrant is admissible in court. The Court reasoned that there was no evidence that government agents intentionally failed to identify the defendants for the purpose of keeping relevant information from the issuing judge (Albanese, 1984). Another issue in the Donovan case was the failure of the government to give post-intercept notice to the defendant after completion of the interception. The Court held that the government's inadvertent failure to give post-intercept notice did not provide sufficient grounds to suppress the intercepted evidence because the defendants were not prejudiced by the failure (Goldstein, 1999).

In Scott v. United States (1978), the U. S. Supreme Court held that compliance with the minimization requirement of Title III was based on an objective assessment of the actions of the officer that listened to the taped conversations. Frank Scott, who was in the drug business, was convicted through wiretap evidence. During thirty days of wiretapping, only forty percent of the conversations were about narcotics. Mr. Scott claimed that the law enforcement officers had not made a good-faith effort to minimize the interception of unrelated conversations as required by Title III. The Court disagreed with Scott's argument (Albanese, 1984).

In Smith v. Maryland (1979), the U. S. Supreme Court held that the installation and use of a pen register was not considered to be within the frame of the Fourth Amendment; therefore, no warrant was required. The court stated that because all telephone users realized that dialed numbers can be detected by the telephone company, a person has no legitimate expectation of privacy while he/she was dialing a number. Since telephone service providers know the dialed numbers, users realize that there is a risk of revealing of these numbers to third parties (Albanese 1984).

In United States v. Knotts (1983), the U. S. Supreme Court ruled that the use of electronic beepers[1] without a warrant was not considered to be within the frame of the Fourth Amendment because it did not invade the legitimate expectation of privacy. Albanese (1984) argued that, by this decision, the Court legitimized continuous surveillance without a warrant.

[1] Electronic beepers are the small transmitters surreptitiously concealed in a target object by law enforcement personnel to track the target by using the signal transmitted by the beeper.

Foreign Intelligence Surveillance Act of 1978 (FISA)

Electronic surveillance for national security cases was authorized through the FISA. The act was enacted for foreign intelligence and counter-intelligence purposes (Center for Democracy, 1997a). The FISA doesn't provide for the protection of privacy to the same extent as Title III (Center for Democracy, 1997a). For example, it doesn't require giving a notice of surveillance to the target unless the obtained information is used for prosecution (Weil, 1999). Similarly, according to the FISA, probable cause is not necessary to support the warrant if the target is not a U. S. citizen or a resident alien. In summary, the Fourth Amendment protections required under Title III are not expanded to protect foreign nationals (Weil, 1999).

Electronic Communication Privacy Act of 1986 (ECPA)

The ECPA was enacted in 1986, as a result of judicial muddling, rapidly changing telecommunications technologies, and pressure from the telecommunications industry (Hull, 1996; Weil, 1999; Wood, 1997). The original Title III did not involve a legal authority to intercept wireless, digital, modem, and optical communications; therefore, it became obsolete in some respects in the 1980s. The ECPA was passed by Congress and approved by the President in 1986. It was intended to form a legal foundation for electronic surveillance on the new communication platforms (i.e. digital, wireless, modem, optical, and other forms of communications), while protecting privacy concerns. According to Dempsey (1997), the ECPA had three goals: to promote privacy protection,

to facilitate the job of law enforcement, to support the development and use of new technologies.

The ECPA included four major contributions designed to expand the means of electronic surveillance originally defined in Title III.

- The ECPA expanded the types of communication that may be subjected to surveillance by including the term "electronic" in the definition of "wire or oral communication." This authorized probable cause-based court ordered interception of modem, radio and video communications (Schwartz, 1995; Weil, 1999)
- The ECPA expanded the definition of "intercept" by adding the phrase "other acquisition" to the definition of electronic surveillance in Title III[2] (Schwartz, 1995).
- The ECPA created a legal foundation for the interception of cellular communications by adding the phrase "between two cellular telephones or between a cellular telephone and a landline telephone" to the definition of "wire communication" in Title III (Schwartz, 1995; Weil, 1999).
- The ECPA created a legal foundation for the interception of communications flowing through fiber-optic lines by adding the phrase "photo-electronic or photo-optical system" to the definition of "wire communication" (Electronic Frontier, 2000).

[2] The new form of the definition has been "aural or other acquisition of any wire, electronic or oral communication..."

- Finally, the ECPA confirmed the legitimacy of the use of pen registers, and trap and trace devices[3] (Wintersheimer, 1988.)

As well as provisions to expand the surveillance capabilities of law enforcement agencies, the ECPA expands the protection shield of the Fourth Amendment to include electronic storage and processing of information (Electronic Frontier, 2000; Whitebread, et. al., 1993; Wintersheimer, 1988). In doing so, the ECPA provides a number of privacy protections.

- The original Title III had referred to wire communications operated by common carriers; therefore, it was not clear that Title III provided protection to private wire and electronic communications. The ECPA made it clear that Title III protects private wire and electronic communications (Wood, 1997).
- The ECPA created a legal foundation for the disclosure of evidence obtained from wiretapping of any wire, oral, or electronic communication. According to § 2517, a law enforcement officer is allowed to disclose the content or derivatives of the content of an interception to another law enforcement officer "to the extent such disclosure is appropriate", or as a requirement of the proper performance of their duties, or while giving testimony under oath

[3] A pen register is used to detect the numbers dialed by the intercept (target) subject. Trap and trace devices are used to determine the connection path of the incoming call made to the intercept subject (Nylund, 2000). The use of a pen register provides the capabilities beyond law enforcement purposes because it can detect all dialed digits, including those, which may be outside of law enforcement concerns (i.e. credit card numbers). Therefore, the use of a pen register is considered more invasive than the requirements of the act (Albanese, 1984).

or affirmation in any proceeding held under governmental authority (Electronic Frontier, 2000; Gruda, 2000; Weil, 1999).

- According to §§ 2703, and 2705, law enforcement agencies can access e-mail messages stored in the facilities of service providers. For messages held less than 180 days, a warrant is required. For messages held more than 180 days, notification to the subscriber is required. However, that notification can be delayed up to ninety days under some circumstances (Electronic Frontier, 2000).

Although the ECPA enhanced the privacy protections of Title III, it excluded cordless phones from protection against interception (Wood, 1997). In 1990, in Schubert v. Metrophone case, the Third Circuit held that the ECPA did not impose a general duty on cell phone service providers to protect transmissions from interception. In 1992, in United States v. Smith, the Fifth Circuit considered individual privacy expectations when using a cordless phone, and concluded that advancement in cordless phone technology, which made interception more difficult, could create an objectively reasonable expectation of privacy. Wood (1997) agrees that the Smith court is correct in asserting that developments in technology may affect privacy expectations. According to Wood (1997), because of their agreement with the Smith Court's assertion, Congress passed CALEA in 1994.

Criminal Procedure for Electronic Surveillance

Criminal procedures for conducting legal electronic surveillance are defined in Title III (Electronic Frontier, 2000). According to § 2516(2) of Title III, the criminal procedure defined in state law must conform to Title III. In fact, according to Whitebread, et al. (1993), the legislators of Title III intended that states enact wiretapping statutes in such a way as to provide more privacy protection than Title III.

The major issues of criminal procedure with respect to electronic surveillance are: probable cause and type of offense which may subject to surveillance, the exhaustion principle, warrant issues, the minimization principle, maintaining the integrity of intercepted evidence, notice to the intercepted subject, disclosure of intercepted information, the exclusionary principle, and citizen assistance. In this part of the study, these issues are explored in separate sections for the sake of articulacy.

Probable Cause and the Offenses Subject to Electronic Surveillance

The legislators of Title III intended to form a legal foundation for effectively combating organized crimes (Gottlieb, et al., 1997). In its original form, Title III allowed electronic surveillance for twenty-six different offenses, which predominantly involved organized crimes and national security threats. However, the number of offenses subject to wiretapping has been increased since 1968, so that as of January 2000 it includes almost one hundred, each listed in § 2516(1) (Electronic Frontier, 2000).

According to § 2518(3), a court may issue an order for the interception of communications if there is probable cause to believe that (Center for Democracy, 1997a; Electronic Frontier, 2000; Gruda, 2000):

- A suspect is committing one of the crimes enumerated in § 2516 (1) of Title III. The law also authorizes government use of electronic surveillance for conspiracy to commit those offenses.
- Communications related to the offense will be obtained through interception.
- The facilities from which the communications will be intercepted are connected with the commission of the crime.

Exhaustion Principle

The exhaustion requirement aims to maintain the privacy of the subject through minimizing the number of cases subject to electronic surveillance. § 2518(3) requires adherence to the exhaustion principle by restricting the government's ability to use electronic surveillance if at least one of the following conditions is satisfied (Electronic Frontier, 2000):

- Other investigative techniques have been tried and failed.
- Other investigative techniques are reasonably unlikely to succeed.
- Other investigative techniques are too dangerous to be tried.

In Title III, it is stated that conclusions and allegations without reasonable support do not satisfy the exhaustion requirement. What reasonable support is needed to satisfy the exhaustion statement depends on the circumstances. Some circumstances make the

use of electronic surveillance necessary because of the goals of the investigation. For example, in narcotics operations, if the goal is to reveal the street-level dealers, the use of an undercover agent is a sufficient investigative technique. If, however, the goal is to identify the sources and associates of the street dealer, more sophisticated techniques are needed. In some circumstances, electronic surveillance may be the only useful investigative tool. For instance, if a person with no criminal history engages in an individual criminal activity such as counterfeiting, electronic surveillance may be the only resort. There may be other circumstances that make electronic surveillance necessary because of the need for further investigation. In such circumstances, the court can authorize electronic surveillance, even if other investigative techniques have not failed. Therefore the exhaustion requirement is also interpreted to mean that electronic surveillance cannot be used if other less intrusive investigative techniques are sufficient (Colbridge, 2000).

Another point that needs to be clarified is what alternative techniques to electronic surveillance exist. This point is important because, according to the Supreme Court decision in United States v. Giordano (1974), the applicant is required to specify the futility or dangerousness of using alternative techniques on the warrant application form. During Title III's legislative debates, Congress identified four alternative investigative techniques: visual and aural surveillance, interrogation and interview, search (with warrant), and infiltration (by undercover or informant). On the application form, the applicant must specify why interrogation, search, and infiltration have not been chosen for the ongoing investigation (Colbridge 2000).

Warrant and Related Issues

Electronic surveillance always possesses a risk to the liberty and privacy of target individuals; therefore, Title III authorizes law enforcement agencies to install wiretaps only after a judge makes an ex parte determination that probable cause exists and that other investigative techniques were or would be unavailable (Colbridge, 2000; Hull, 1996).

Warrant Application

According to § 2518(1), a warrant for electronic surveillance is granted by a judge of competent jurisdiction following a written or affirmation application by an authorized law enforcement official. According to § 2518(1), the following information must be specifically listed on the warrant application form (Electronic Frontier, 2000; Goldstein, 1999; Gruda, 2000):

- The identity/identities of the intercept subject/subjects.
- A full statement of the alleged offense.
- The place or telecommunications facility where the interception is to occur.
- A particular description of the communications to be intercepted.
- The period of time during which interception is to be maintained.
- An exhaustion statement involving a complete statement about why other investigative procedures will not be used instead.

Judicial Procedures Related to Warrant

According to § 2516(1), the warrant must be approved by the U. S. Attorney General or a specially designated Assistant or Deputy Assistant Attorney General before forwarding to a local U. S. Attorney for application to a federal district court or other court of jurisdiction. The application to the court must involve the applicant and the person authorizing it (Communication Assistance, 1994; Electronic Frontier, 2000; Gruda, 2000). Federal district court judges can authorize electronic surveillance within the jurisdiction of the court. However, if the intercept subject uses a mobile telephone, the judge may authorize electronic surveillance throughout the U. S. (Colbridge, 2000).

The judge authorizes two warrants. One authorizes the law enforcement agency to conduct the interception, and the other directs the telecommunication service provider to set up the intercept (Electronic Frontier, 2000).

According to § 2518(4), the warrant involves the identity/identities of the intercept subject/subjects, offense relevant to interception of communications, the location of the place or telecommunication facility where the interception is to occur, description of communication to be intercepted, and the period of time during which interception is to be maintained (Electronic Frontier, 2000; Gruda, 2000).

Wiretapping Duration

Under normal circumstances, a warrant is valid for 30 days. If needed, the court may extend that period by 30 days for each application for extension. This period begins on the first day of interception or ten days after issuance of the warrant, whichever comes

first (Electronic Frontier, 2000). The warrant for pen registers, trap and trace devices, is issued for up to sixty days and can be extended for additional sixty day periods (Gruda, 2000).

§ 2518(5) of Title III requires termination of the surveillance upon attainment of the authorized period of interception. If government officials wish the surveillance to continue after the initial interception period, § 2518(1) requires that they prepare an affidavit detailing that probable cause exists to believe that additional communications will be relevant to the offense subject to electronic surveillance (Electronic Frontier, 2000).

Minimization Principle

Like the exhaustion principle, the minimization principle aims to minimize privacy invasion to the intercepted subject. According to § 2518 (5), electronic surveillance must be conducted in such a way as to minimize the interception of communications outside the scope of the warrant. Communications outside of the scope of the warrant involve the unrelated and non-criminal communications of the subject and the communications of others whose names are not specified in the court order. On the other hand, it is technologically difficult to comply with the minimization requirement. The U. S. Supreme Court decision in Scott v. United States (1978) clarified the minimization requirement so that the minimization requirement of Title III was based on an objective assessment of the actions of the officer listened to the taped conversations (Electronic Frontier, 2000, Gruda, 2000).

Maintaining Integrity of Intercepted Evidence

Maintaining the integrity of intercepted evidence is one of the post-authorization duties of electronic surveillance. It both protects confidentiality and prevents tampering. According to § 2518(8), the integrity of the intercepted evidence is achieved in a number of ways (Electronic Frontier, 2000):

- The intercepted information must be recorded in such a way that addition, deletion or any other form of alteration of the records is not be possible.
- Recordings obtained through electronic surveillance as well as the application for the order, must be sealed and presented to a court of jurisdiction immediately after the expiration of the court order and any relevant extensions.
- If there is a mistake while conducting electronic surveillance as authorized in a court order, or if the surveillance is found to be conducted illegally, or the intercepted information was not properly sealed, or if the government unsatisfactorily explains the delay or absence of a seal, the information obtained through the electronic surveillance can not be used as evidence or for other purposes.

Notice to Intercepted Subject

§ 2518(8) requires that after completing the interception, an "inventory" notice must be issued to those persons named on the court order and, if the judge requires, to

other persons whose conversations have been intercepted. The inventory must include the notice of application and court order, surveillance period and whether any interception occurred (Electronic Frontier, 2000; Gruda, 2000).

Disclosure of Intercepted Information

According to Title III any intercepted information can lawfully be used in three situations. According to §§ 2517(1), 2517(2) and 2517 (3), a law enforcement officer is allowed to disclose the content or derivatives of the content to another law enforcement officer "to the extent such disclosure is appropriate", or as a requirement of proper performance of their duties, or while giving testimony under oath or affirmation in any proceeding held under the governmental authority (Electronic Frontier, 2000; Gruda, 2000; Weil, 1999). § 2518(9) requires that before the disclosure of intercepted evidence at a trial, hearing or any other proceeding, the government must provide each party with a copy of the application and court order at least ten days before the proceeding (Electronic Frontier, 2000).

Exclusionary Principle

According to Wood (1997) Title III provides two types of remedies when the communications are improperly intercepted: the exclusionary principle requiring suppression of intercepted evidence, and a civil cause of action.

§ 2518(10) requires suppression of intercepted evidence when "the communication was unlawfully intercepted;" the interception warrant is "insufficient on

its face;" and "the interception was not made in conformity with" the order. (Electronic Frontier, 2000). Whitebread, et al. (1993) identifies additional intercepted communications requiring exclusion: the communications that are not disclosed to the judge "as soon as practicable" or that are irrelevant to the offense mentioned on the warrant; the communications that are not properly sealed immediately after completing the interception when there is no appropriate excuse; and the inventory notice is not delivered to the parties at least 10 days before the proceeding.

On the other hand, there are two major exceptions to the exclusionary principle known as the central role, and the good faith exceptions (Whitebread, et al., 1993). In United States. v. Giordano (1974), the U. S. Supreme Court held that the intercepted evidence was not suppressed, even though the initial warrant had been authorized by the Attorney General's Executive Assistant, not the specially designated Assistant Attorney General. The reasoning was that the statutory provision which had been violated did not play a central role in the statutory scheme. Similarly, in United States v. Donovan (1977), the Court held that failure to provide an inventory notice does not create sufficient grounds to suppress evidence, unless the failure has caused untreatable prejudice, and if the statutory provision which was violated did not play a central role in the statutory scheme.

Another exception for the suppression of intercepted evidence is the good faith doctrine. In United States v. Ojeda Rios (1990), the Supreme Court held that the intercepted evidence was excluded because the intercepted communications had not been sealed immediately after completing the interception, but instead were sealed after 118

days without a reasonable excuse. The majority decided to remand the case for a determination that the delays were the result of good faith. This result of Ojeda Rios permits a good faith exception to the exclusionary principle (Whitebread, et al., 1993).

Assistance of Citizens

Title III permits citizens to assist law enforcement officials in electronic surveillance. However, according to § 2511(2), before rendering assistance, an individual or entity must receive either a court order directing the assistance or a written certification indicating that no court order is required for the assistance (Electronic Frontier, 2000).

Electronic Surveillance without Warrant

Under certain circumstances, interception of communications without a warrant does not violate the Fourth Amendment or Title III. These circumstances are usually created by the lack of a legitimate expectation of privacy on the part of the conversation's parties. Whitebread, et al. (1997) identifies five cases for which Title III doesn't require a warrant for the interception of communications:

- Interception of communications where one of the parties has consented to such interception,
- Interception of communications that are accessible to the general public, including radio communications,

- Interceptions, by common carriers and government agencies, as a part of their normal course of business,
- Interceptions for the purpose of national security. In United States v. United States District Court (1972), the Court held that the national security exception did not eliminate the need for a warrant for federal investigations of cases not linked to foreign powers,
- Interceptions in certain emergency situations involving danger to life, and some emergency situations related to national security and organized crimes.

CHAPTER 3

CASE STUDY OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994

In this chapter, CALEA is studied thoroughly. After describing the motivations leading to new legislation in the early 1990s, the non-legislative and legislative efforts toward the CALEA, and the FBI's interpretation and implementation plan of CALEA are explored.

Background of Communication Assistance of Law Enforcement Act of 1994

At the end of the 1980s and beginning of the 1990s, three major factors motivated the enactment of new electronic surveillance legislation. These factors are technical difficulties, legislative difficulties, and privacy concerns came up with new technologies.

Technological Factors Making Electronic Surveillance Difficult in the Late 1980s and Early 1990s

During preparation of CALEA, the Electronic Communications Service Provider (ECSP) Committee stated that new and emerging telecommunications technologies posed problems for law enforcement, and the Committee recommended a legal action. The report of the ECSP cites three sources for this recommendation, the evidence came from

three sources: the General Accounting Office (GAO), the FBI, and telecommunications industry itself (S. Rep. No. 103, 1994).

In 1992, analysts from the Information Management and Technology Division of the GAO interviewed technical representatives from local telephone companies, switch manufacturers, and cellular providers, as well as the FBI. The GAO found that the FBI had not adequately defined its electronic surveillance requirements, and the GAO concluded that law enforcement agencies did have technical problems with tapping a variety of services or technologies.

In April 1994, after surveying for two years, the FBI reported 183 instances where State or local agencies had encountered problems when they attempting to intercept communications. The FBI presented details of these instances to the House and Senate Judiciary Subcommittees (S. Rep. No. 103, 1994). These 183 instances were the following:

- Insufficient port capacity: 54
- Inability to capture dialed digits contemporaneous audio: 33
- Cellular-provider could not intercept long-distance calls to or from a targeted phone: 4
- Speed dialing / voice dialing / call waiting: 20
- Call forwarding: 10
- Direct inward dial trunk group (provider unable to isolate targets communications to the exclusion of all other customers): 4

- Voice mail (provider unable to provide access to the subjects audio when forward to voice mail or retrieve messages): 12
- Digital Centrex (provider unable to isolate targets communications to the exclusion of all other customers): 4
- Others (such as call back, inability of provider to isolate targets communications to the exclusion of all other customers, and so forth): 42

Representatives of the telecommunications industry, the third source of evidence, acknowledged that there would soon serious problems for law enforcement interception posed by new technologies and the competitive nature of the telecommunications market. The industry maintained that companies had a long tradition of working with law enforcement under current laws to resolve technical issues. However, with the proliferation of services and service providers, such a company-by-company had become increasingly insufficient.

According to Office of Technology Assessment (OTA) (1995), the contributing factors that made electronic surveillance difficult after 1980s were the following:

- End of monopolies in the telecommunications industry: The emerging technologies and financial strategies ended the telephone monopoly of AT&T on standards and procedures of the national telephone system in 1984. No longer have the standards and architectures been determined by one hand. Telecommunication protocols or standards became incompatible with another. Since then, many new telecommunication standards and many carrier

companies have been launched. Every company has their own technology deployment plans.

- Technological innovations: Electronic surveillance was simple when telecommunication systems were simple, but the technology has raced ahead in recent decades. Computer, facsimile, modem, wireless, and satellite based personal communication technologies were introduced to everyday life. Digital technologies, providing new features including video, data, voice or a mixture of them, replaced the analog technology. Data communication has been more important than voice communication in some areas.
- Increasing complexity in telecommunications technologies: The structures of telecommunication networks have become complicated with emerging technologies. For instance, Iridium, which is one of the satellite-based mobile telecommunication systems, even do switching procedures on the satellites without using ground-based switching stations. Similarly, encryption has contributed to the complexity of conducting electronic surveillance.
- Increasing decentralized control of telecommunication systems: New technologies have placed some choices and controls in the hands of its users. For example, a user can activate call forwarding, call waiting, and conference call features by himself/herself.

Legal Factors Making the Electronic Surveillance Difficult in the New Age

The 1970 Amendment of Title III mandates the cooperation of telecommunication companies with the government entities for electronic surveillance purposes. The Supreme Court interpreted this amendment as requiring the Federal courts to compel, upon request of the government, "any assistance necessary to accomplish an electronic interception," in United States v. New York Telephone. However, it remained questions regarding the degree and level of cooperation required between law enforcement and telecommunication companies. For example, there was a question about whether the industry has the obligation of making required modifications and additions in the design level of their products to provide interception capability and capacity that were required by the law enforcement community (Colbridge, 2000; H. Rep. No. 103, 1994).

ECPA extended Title III's existing legal provisions to new technologies. However, ECPA has not dynamic regulations to meet the law enforcement needs that come up with the emerging technologies; therefore, it soon became evident that new legislation was necessary to keep pace with the emerging technologies (Hull, 1996). For example, ECPA include nothing about how law enforcement entities should access new communication technologies for wiretapping purposes.

In sum, both ECPA and Title III became obsolete in some respects in late 1980s, in terms of providing legal background for the electronic surveillance.

Need to a New Communication Privacy Shield

In the early 1990s, privacy groups worried that Title III and ECPA were not sufficient to cover the privacy issues that were being created by new technologies (Koppell, 1992, May 22). For example, ECPA doesn't provide protection for wireless and cordless communications (Wood, 1997). Similarly ECPA doesn't prohibit the possession of telecommunication instruments for the purpose of obtaining unauthorized telecommunication services (Electronic Frontier, 2000). Thus, it soon became evident that neither Title III, nor ECPA had not kept pace with the new challenges in terms of protection of right to privacy (Hull, 1996).

Efforts to Overcome the Difficulties in Electronic Surveillance

In 1990, Senator Patrick Leahy, chairman of the Senate Judiciary Subcommittee on Technology and Law, assembled a Privacy and Technology Task Force with experts from business, consumer advocacy, law, and civil liberties, to examine developments in communications technology and the extent to which the law in general, and ECPA in particular, protected, or failed adequately to protect, personal and cooperate privacy. After examining the wide array of communication media, including cellular phones, personal communications networks, the newer generation of cordless phones, wireless modems, wireless local area networks (LANs), and electronic mail and messaging, the task force issued a final report on May 28, 1991 recommending, inter alia, that the legal protections of ECPA be extended to cover new wireless data communications, such as

those occurring over cellular laptop computers and wireless local area networks (LANs), and cordless phones. In addition, the task force found that ECPA was serving well its purpose of protecting the privacy of the contents of electronic mail, but questioned whether current restrictions on government access to transactional records generated in the course of electronic communications were adequate (H. Rep. No. 103, 1994; Office of Technology, 1995; S. Rep. No. 103, 1994).

Consistent with the task force's conclusions and in view of the increasing impediments to authorized law enforcement electronic surveillance, the Committee concluded that continued change in the telecommunications industry deserves legislative attention to preserve the balance sought in 1968 and 1986. However, it became clear to the Committee early in its study of the "digital telephony" issue that a third concern now explicitly had to be added to the balance, namely, the goal of ensuring that the telecommunications industry was not hindered in the rapid development and deployment of the new services and technologies that continue to benefit and revolutionize society. Therefore, the Committee's proposal sought to balance three key policies: (1) "to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts"; (2) "to protect privacy in the face of increasingly powerful and personally revealing technologies"; and (3) "to avoid impeding the development of new communications services and technologies" (H. Rep. No. 103, 1994; S. Rep. No. 103, 1994).

Despite the report to Congress recommending legislative attention, no immediate action was taken. Then, the FBI, on behalf of the U. S. law enforcement community,

started a secret campaign called “Operation Root Canal”. In this campaign, the FBI targeted telecommunications industry and standard organizations to understand electronic surveillance needs of law enforcement through a collaboration process (Koppell, 1992, May 22). On the other hand, according to Hull (1996), the process was not collaborative, but it mostly involved the demands of the FBI from telecommunications industry. In fact, the FBI specifically requested access to the carrier’s central switches for wiretapping because the FBI realized that, in long run, the most comprehensive solution for wiretapping would be possible by accessing central switches. Despite this barely acceptable request of the FBI, telecommunications industry feared to take an offensive action because of the FBI’s relationship with the Department of Justice, which has considerable power over telecommunications industry. This fear led the industry not to articulate their opinions clearly about the FBI’s attempts for the cooperation. As well as this fear, the cost of the FBI’s demands was another factor, influencing the attitudes of the telecommunications industry in the collaboration process. For the telecommunications industry, it wasn’t the 1960s, or 1970s when there was a monopoly by AT&T, as opposed to competitive market. Competitive realities led the carriers to argue that unless universal compliance was assured, competitors would not accept any agreement proposed by the FBI (Hull, 1996).

Because of the broad demands of the FBI and cost of these demands, the non-legislative efforts of the FBI didn’t produce a result. Then, the FBI turned to a legislative solution, which would address the compliance, security, and cost recovery issues. In July 1992, the FBI, on behalf of the U. S. law enforcement community, published a document

entitled “Law Enforcement Requirements for the Surveillance of Electronic Communication”. The document involved the procedures for the government-industry collaboration (Office of Technology, 1995). Based on this document, in fall 1992, the FBI drafted a proposal for a digital wiretapping bill. In spite of support by the Bush Administration, the proposal was confronted with harsh criticisms, and it was withdrawn (Hull, 1996). In this proposal, one of the provisions, subjected to harsh criticism, was the one that forbade the introduction of new technologies, not wiretap accessible. That provision had no exception such as mail, PBX or online services (Nelson, 1994). The industry representatives supposed that such provision would impede technological development because about 88 % of the telecommunication technology came from the non-domestic market. On the civil liberties side, the proposal was criticized because it had no sufficient provisions protecting constitutional rights (Hull, 1996).

In March 1993, the Electronic Communications Service Provider (ECSP) Committee was formed under the authority of Alliance for Telecommunication Solutions to determine the needs of law enforcement and to develop the solutions for these needs. ECSP committee has been co-chaired by representatives of the Attorney General and telecommunications industry. The Committee had nearly 200 individual participants in its six action teams. Each action team has been co-chaired by a representative of law enforcement and a representative of the industry. The teams were Advanced Intelligent Networks, Personal Communication Services, Prioritization and Technology Review, Switch Based Solutions, Interfaces, and Cellular Teams. The objective of the teams was to determine the requirements of law enforcement on telecommunication networks and to

develop the solutions for them. The teams have documented the requirements as reference to the manufacturers, carriers, service providers, standard-setting bodies, and law enforcement agencies. However, since the participation in the teams was voluntary and its recommendations were unenforceable, the teams couldn't have made a desirable impact. As a result, the ECSP Committee has concluded that legislation was necessary (Kallstrom, 1994; Office of Technology, 1995; S. Rep. No. 103, 1994).

The Communication Assistance for Law Enforcement Act of 1994

The efforts of the ECSP Committee gave rise to new comprehensive legislation. The legislation was proposed in the 103d Congress. On October 25, 1994, the Congress passed and the President approved the CALEA.

As stated in the Privacy and Technology Task Force of the Senate Judiciary Subcommittee on Technology and Law, in its legislative history, it was stated that the CALEA sought to balance three key concepts (H. Rep. No. 103, 1994; S. Rep. No. 103, 1994):

- The CALEA requires the telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement ability to lawfully intercept communications.
- The CALEA clarifies that the telecommunications industry must consider the capacity and capability requirements of the law enforcement in terms of electronic surveillance in both design and operation level.

- The CALEA doesn't prohibit introduction of new technologies, not wiretap accessible. It also doesn't have the provisions about the interception of e-mail, online services and closed networks such as PBXs and ATMs.

Below, the principle features of CALEA are outlined.

Coverage

According to § 102 of CALEA, all "telecommunications carriers", which are considered "common carriers", must comply with the requirements of the Act. The common carriers involve the telecommunications carriers, service providers as well as other companies such as cable and electric utility companies, which provide telecommunication services. The size of the carrier is not a factor for becoming a "common carrier".

On the other hand, the Act exempts from its coverage any telecommunications server whose sole purpose is the interconnection of telecommunications carriers and private telecommunication networks as well as the "information services", such as Internet service providers, electronic mail services, are excluded from the requirements of the Act.

Capability Requirements

CALEA requires that introduction of new technologies by the telecommunications carriers do not interfere with electronic surveillance activities of law

enforcement agencies. Furthermore, it requires the carriers to retrofit or design their systems to allow the law enforcement to conduct electronic surveillance.

§ 103 of CALEA explains the capability requirements that all telecommunications carriers must comply with. These are

- To provide isolation and interception of call-content to the government.
- To provide call-identifying information (i.e. origination and destination numbers of targeted communication), but not geographical information to the government, "except to the extent that the location information may be determined from the telephone number."
- To deliver call-content and call-identifying information in the appropriate format to the government in the premises other than the premise of the carrier, within the service area of the company.
- To provide interception with minimum interference to the intercept subject.

Furthermore, the CALEA explains some limitations:

- Law enforcement agencies are not authorized to require or prohibit the telecommunications industry from using any specific equipment.
- In emergency and exigent circumstances, the carrier must allow government personnel to conduct electronic surveillance at the carrier's premises.
- The carriers must inform the related law enforcement agency/agencies when the mobile intercepted subject (the subject using cellular phone) come into and go out their service areas.

§ 107 authorizes the FCC to decide if the carriers comply with the Act by their implementations. § 107 also authorizes the FCC to extend the compliance period if the Commission agrees that compliance with the capability requirements is not reasonably achievable within the specified time span. The compliance period can be extended up to two years.

Capacity Requirements

§ 104 of CALEA mandated the Attorney General to provide "actual" and "maximum" capacity requirements of the law enforcement to the telecommunications carriers. The actual capacity would be provided not later than October 25, 1995, and it would involve capacity requirements of the law enforcement until October 1998. The maximum capacity would be provided not later than October 25, 1998, and it would involve the maximum capacity requirements of law enforcement, after October 1998. In addition, § 104 mandates the Attorney General to notify the carriers about further changes in the maximum capacity requirements.

Systems Security and Integrity

§ 105 mandates the telecommunications carriers to protect their systems against unauthorized and improper interception.

Consultation and Cooperation

§ 106 of CALEA mandates the telecommunications carriers to consult, as necessary, with the manufacturers and providers to ensure that current and planned equipment, facilities, and services comply with the capability and capacity requirements (§§ 103 and 104) of CALEA.

§ 107 mandates that the Attorney General, in coordination with law enforcement, shall consult with the standard-setting organizations, appropriate associations of telecommunications industry, state utility commissions and representatives of users of telecommunication equipment, facilities and services to clarify questions related to court-authorized electronic surveillance.

Cost Reimbursement

According to § 109 of CALEA, the Attorney General has authority to reimburse the telecommunications industry for the reasonable cost of retrofitting their systems to comply with requirements of CALEA. The Attorney General is authorized for the reimbursement for cost of the equipment installed before January 1, 1995. The costs of retrofitting for the equipment installed after January 1, 1995 are reimbursed through the agreement of the FCC. The FCC agreement includes that the retrofitting could not have been "reasonably achievable" before January 1, 1995 for the specific equipment.

§ 110 appropriates $500,000,000 for reimbursement over fiscal years 1995, 1996, 1997, and 1998.

Penalty for the Violation

§ 2522 requires a civil penalty of up to $10,000 a day for any telecommunications carrier violating the Act.

The Provisions about Privacy Protection

CALEA has the following contributions to protection of privacy right.

- § 103 requires carriers to protect the privacy and security of communications not authorized to be intercepted. In fact, this entirely new requirement on telecommunications carriers directs them to design their systems in such a way as to withhold from law enforcement the content of communications that law enforcement has no authority to intercept (Center for Democracy, 1999). According to Dempsey (1997), this requirement, unlike other design requirements in the CALEA, is intended as a counterbalance to the pro law enforcement requirements of CALEA.
- § 107 allows any person, including public interest groups, to petition the FCC for review of standards implementing wiretap capability requirements.
- §§ 202 and 203 of CALEA expand the ECPA privacy protection coverage to cordless phones and certain types of radio communications.
- § 204 explicitly states that it does not limit the rights of subscriber to use encryption.

- § 206 prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to obtain unauthorized access to telecommunications services. It also prohibits possession of cloning[4] devices including the radio frequency scanners. The penalty for violating this section is imprisonment for up to 15 years and a fine of the greater of $50,000 or twice the value obtained by the offense.
- § 207 revises the granting procedure of subpoena requiring disclosure of computer-based transactional records[5]. The ECPA has authorized the law enforcement agencies to access computer-based transactional records after obtaining an administrative, grand jury, or trial subpoena. § 207 of CALEA doesn't allow granting the subpoena if the transactional record is not relevant to an ongoing criminal investigation.
- § 207 limits the use of pen registers, trap and trace devices (Schwartz, 1995).

Besides the contributions listed above, scope of CALEA eliminates some risk of invasion to privacy right, at the first place, by exempting some types of

[4] The cloning is started after obtaining the electronic serial number (ESN) of a cellular phone. ESN is assigned to the phone during manufacturing. After purchasing the phone, the service provider assigns a mobile identification number to that phone (MIN). The combination of ESN and MIN is the identification number of the cellular phone. Once obtaining an ESN, a radio scanner is used to obtain the MIN of this phone. Then obtained MIN and ESN numbers can be used to reprogram another cellular phone. The bills of reprogrammed phone are sent to the actual owner of the phone.

[5] Transactional records include the toll records and on-line service records. Toll records contain the information of city, date, time, duration, and receiving telephone numbers of the long distance call called from a specific telephone number. On-line service records include the e-mail messages, web page addresses, TCP/IP numbers of the computers, etc. (S. Rep. No. 103, 1994).

telecommunications companies from its coverage. In fact, CALEA doesn't mandate telecommunication services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers, such as PBXs, ATMs and other closed networks to comply with the CALEA. In other words, although these services can be wiretapped pursuant to warrant, they do not have to be designed so as to accommodate wiretap needs. Similarly, § 103 does not require mobile service providers to reconfigure their networks to deliver the content of communications occurring outside of their service area.

The Federal Bureau of Investigation's Interpretation of the Capability Requirements of the Act

§§ 103 and 105 of CALEA involve technical requirements describing what governments want from the telecommunications industry in design level. Because of the complexity and heavy nature of these requirements, they have been one of two major causes of debates between the government and telecommunications carriers[6].

In May 1995, the FBI issued the document entitled "Law Enforcement's Requirements for Electronic Surveillance" (Office of Technology, 1995). The FBI asserted that the requirements stated on this document were the interpretation of the capability, and system security and integrity requirements described in §§ 103 and 105 of CALEA.

---

[6] Another major cause is related to reimbursement of the compliance cost, and it is discussed in the forthcoming parts of this study.

In this section of the present study, the FBI's interpretation of §§ 103 and 105 of CALEA is explored.

The Interpretation of the Communication Access Requirements

Implementation of § 103(a)(1) and (2) allows law enforcement to access communications in order to conduct surveillance. According to the FBI, access to the communications for interception purposes requires the following (Office of Technology, 1995):

- The carrier must be able to provide multiple simultaneous intercepts of the same subject for different agencies while maintaining confidentiality among the agencies.
- If the intercepted communication is handed off to a second service provider, it is the responsibility of the second service provider to provide the access to law enforcement in order to intercept the communications.
- Each telecommunication carrier is required to activate and deactivate the intercept within 24 hours after receiving the legal notice. According to § 103(c), law enforcement may require the activation within a few hours, in emergency cases.

The Interpretation of the "Call Content" and "Call-Identifying Information"

The FBI (1997c) interpreted the "call content" and "call-identifying information", stated in §§ 103(a)(1) and 103(a)(2), respectively, as "dialing and signaling information".

Dialing information involves the numbers generated by the intercept subject to establish a telecommunication connection with the others. The FBI (1997a) interpreted that the CALEA requires carriers to provide all dialing information.

According to the FBI, the signaling information provided by the carriers is required to include at least the following information (Office of Technology, 1995):

- The information directly related to call content.
- Signaling information for initiation and termination of calls.
- Notifications of call attempts.
- Feature and service status messages associated with the intercept subject.
- Redirection numbers used for call transfer, call forward, conference call and other similar purposes.
- Connection paths between intercept subject and network, and between network and calling-party, even if the calling party is not a court ordered intercept party.
- Signaling information involving the called numbers of the calling-party, even if the calling party is not a court ordered intercept party.
- Content of complete conference calls even after dropping of the court ordered intercept subject.
- Roaming information containing the geographical location information of mobile intercept subjects.

The Interpretation of the "Delivering Intercepted Communications" Requirement

§ 103(a)(3) requires the carriers to transmit the dialing and signaling information associated with the intercept subject to the monitoring center(s) designated by law enforcement agency/agencies. According to the FBI's interpretation of § 103(a)(3) of CALEA, the transmission must satisfy the following requirements (Office of Technology, 1995):

- The monitoring center can be anywhere within the service area of the provider.
- The information must be in a standard form.
- The information cannot be altered during the transmission.

Furthermore, § 103(b)(3) requires that if the service provider provides the compression, encryption, coding and other such security features in the service, the provider must decompress, decrypt, and decode the content of the communication before transmitting the information to the designated monitoring center.

The Interpretation of the "Unobtrusive" Information Providing

In FBI Documents (1997a), it is stated that the § 103(a)(4), which explicitly requires the carriers to provide interception with minimum interference to the intercept subject, requires the carriers to provide information to authenticate linkage between the intercept subject and the intercepted communication. According to the FBI, this

information is important because it ensures the admissibility of the intercepted evidence in court.

According to the FBI (1997a), the § 103(a)(4) mandates the carriers for providing interception and transmission of intercepted information with equal reliability, quality, and transparency as those of the intercept subject's service. Transparency means that interception is undetectable to others who are outside the conversation.

Furthermore, this section also requires that the intercept should not be detectable to the intercepted parties (Office of Technology, 1995).

The Interpretation of the Systems Security and Integrity Requirements

§ 105 of CALEA mandates service providers and carriers to protect their systems against unauthorized and improper intercept. According to the OTA's report, § 105 requires the following measures (Office of Technology, 1995):

- The interception must be provided on a need-to-know basis to minimize the risk of disclosure. According to § 105 of CALEA, only one personnel must be responsible for activation and deactivation of the intercept at the service provider's side.
- The companies are required to protect their systems against unauthorized access through physical and logical security mechanisms. Logical security measures involve switching functions, database partitioning, prohibiting of remote access, accessing the systems through the logging procedures, encryption, and so forth.

Implementation Issues of the Communication Assistance

for Law Enforcement Act of 1994

Background

§ 107 of CALEA requires law enforcement personnel to consult with the telecommunications industry to facilitate industry-wide implementation of CALEA. As a result, the FBI created a Telecommunications Industry Liaison Unit (TILU) including 70-80 personnel from Federal, State and local law enforcement agencies, and the Telecommunications Contracts and Audit Unit which is the industry representative, to prepare an implementation plan for the CALEA.

Furthermore, the FY 1997 Appropriations Act required the FBI to prepare an implementation plan for the CALEA. According to the Act, the implementation plan must include the following (Center for Democracy, 1997c):

- Explanation of law enforcement capability requirements.
- The electronic surveillance capacity requirements.
- Priority list of equipment and systems to be modified by the carriers to comply with the CALEA.
- The reimbursement plan.

After enactment of the FY 1997 Appropriations Act, the FBI, as a collaborative product of its works with the industry from November 1995 to March 1997, produced an implementation plan for the CALEA. On March 3, 1997, the FBI submitted the CALEA

Implementation Plan to the Committees on the Judiciary, Committees on Appropriations, U. S. House of Representatives and the U. S. Senate (The Federal Bureau, 1997c).

On April 29, 1997, the advocates on behalf of the Cellular Telecommunications Industry Association, United States Telephone Association, Personal Communication Industry Association, and CDT prepared a response to the FBI's CALEA Implementation Plan (Center for Democracy, 1997c).

In this section, the FBI's implementation plan and the response to this plan, as well as the other implementation issues are discussed.

The Electronic Surveillance Interface Document and Implementation of Capability Requirements

In early 1995 the Electronic Communications Service Provider (ECSP) Committee requested the FBI to prepare a "safe harbor" document, describing interface between the telecommunications carriers and the designated monitoring centers. Furthermore, according to the FBI (1997c), they had also received numerous requests from the industry to describe delivery and interface methods for transmission of intercepted information. The FBI then started to work on producing a document that described a logical and physical interface between the carriers and the monitoring centers. The resulting document, called the **"**ESI Document – Issue 1.0", was produced in April 1996, after more than 200 meetings held among the industry experts and law enforcement representatives. After evaluating the feedback comments of the industry, the

document was reshaped. Then it was submitted to the industry standard groups in June and July 1996 (Federal Bureau, 1997c).

The ESI document involves the description of the interfaces for following telecommunication services and technologies (Office of Technology, 1995):

- Plain Old Telephone Service (POTS)
- Centrex Services
- Custom Calling Features
- Custom Local Area Signaling Services (CLASSSM)
- Cellular Services
- Intelligent Network (IN) Services
- Advanced Intelligent Network (AIN) Services
- Integrated Services Digital Network Basic Rate Interface (ISDN, BRI)

According to the FBI (1997c), the ESI Document complies with the capability requirements of CALEA; therefore, it must be adopted as a "safe harbor" standard by the industry. Further, the FBI (1997c) argued that the ESI Document had been widely accepted by the industry.

When the ESI Document was being prepared, the telecommunication companies under the umbrella of the Telecommunications Industry Association (TIA) also prepared their standard document. This document was called as Standard Proposal-3580 (SP-3580) and it had been intended by the industry to comply with the capability requirements of CALEA. The TIA finished drafting of SP-3580 in 1997 (Federal Bureau, 1997c).

According to the FBI (1997c), SP-3580 does not contain all capability requirements of CALEA; therefore, it is deficient. For example, it doesn't satisfy the evidentiary needs required by the courts. Furthermore, the FBI (1997c) claimed that the standards in SP-3580 were not defined specifically as compared to those defined in the ESI Document; therefore the implementations under the interpretations of the SP-3580 would not comply with the capability requirements of CALEA.

Response of Industry Advocates to the Electronic Surveillance Interface Document and the Implementation Plan on the Capability Requirements

The industry advocates have the following arguments in response to the capability requirements part of the FBI's Implementation Plan and the ESI Document (Center for Democracy, 1997c):

In the CALEA, the requirements are narrowly stated. The FBI, however, interprets the requirements broadly in both the CALEA Implementation Plan and ESI Document. Although it is not mentioned in the Act, the FBI required following from the carriers in the "CALEA Implementation Plan":

- Feature and service status messages associated with intercept subject.
- Connection path between intercept subject and the network.
- Connection path between calling party, who called intercept party, and the network.
- Signaling information containing the called numbers of calling-party who called the intercept party.

- Content of complete conference calls after intercept subject drops out.
- Roaming information and geographical location information for mobile intercept subjects.

The industry advocates argue that determining and judging the system capabilities are technical issues; therefore, they should be conducted by the industry, not by the FBI. However, the FBI prepared the ESI Document and judged the adequacy of the SP 3580. In technical issues, Congress gave power to the FCC to judge the adequacy of industry standards. In sum, the efforts of the FBI did nothing but retard the industry to comply with actual requirements of CALEA (Hull, 1996).

The industry started to prepare SP-3580 in spring of 1995, and finished the 170-page draft in October 1995. The advocates argued that the ESI Document has been circulated after April 1996 and it was issued in June 24, 1996, which was about 15 months after the beginning of the standard preparation process of the industry. As a result, the ESI Document has been late to contribute to the industry's process for standard preparation. In addition, the advocates contended that the ESI Document was based on the draft of the SP-3580. Even though, the industry examined the ESI Document, and they concluded that it had some technical impossibilities and it did not comply with the CALEA.

The FBI first described ESI as a "safe harbor" standard. After the criticisms based on § 107 of CALEA that authorizes the industry to develop compliance standards, the FBI described the ESI Document as a contribution document. Again, in the FBI implementation plan, the FBI described the ESI Document as a "safe harbor". Even if it

is considered a contribution document to the standard preparation process of the industry, the ESI Document confused the process, because it was incompatible with the currently used standards, rather, it was prepared as an alternative standard. From this point of view, it violated § 103 of CALEA prohibiting law enforcement to dictate the specific design and features to the industry.

In the implementation plan it was stated that the ESI Document satisfied the delivery capability requirements under § 103 of CALEA. However, delivery requirements of the ESI standards are inconsistent with those of § 103. For example, in the ESI Document, feature and service status messages are required, but these are not required by the CALEA.

In the implementation plan, it was stated that the ESI Document had been supported widely. However, the industry advocates objected to that statement and stated that the FBI ignored the objections of the industry.

According to the implementation plan, SP-3580 doesn't satisfy the "evidentiary needs" required by the courts. On the other hand, the industry advocates objected to that argument and they argued that the FBI hadn't explained what the evidentiary needs would be. SP-3580, as a technical standard, describes only the technical specifications. The courts usually accept the information obtained through court ordered electronic surveillance. In any case, the defense lawyer cannot be hindered to raise argument to the evidence obtained through the electronic surveillance. If it is known, the FBI should explain how the intercepted information, obtained under SP-3580 standards, doesn't meet the evidentiary standards.

In the implementation plan, it was stated that the standards of SP-3580 were not defined specifically as compared to those of the ESI Document. According to industry advocates, there are three reasons why the standards in SP-3580 should not be defined specifically: First, it is a general practice to define the standards generally to allow the numerous companies to participate in the implementations. Second, CALEA requires development of a standard not specification. Specification dictates only one type of solution, whereas the standard allows different means to reach the same objective to encourage the innovation. Third, § 103(b) of CALEA provides flexibility in meeting the requirements by prohibiting law enforcement agencies to require the industry to adopt any specific design of equipment and systems.

Other Implementation Issues about the Capability Requirements

According to Nylund (2000), the FBI opposed to SP-3580, since it didn't have the eleven technical capabilities of the "punch list" prepared by the FBI. The FBI believed that the punch list was mandated by CALEA. Later reduced to nine items, this list became known as the FBI "punch list." The nine-item "punch list" contains information regarding (Federal Communications, 1999a):

- Content of subject-initiated conference calls.
- Party hold, join and drop on conference calls.
- Subject-initiated dialing and signaling information.
- In-band and out-of-band signaling.
- Dialed digit extraction.

- Timing information.
- Continuity check tone.
- Surveillance status.
- Feature status.

After a few revisions to the standard, TIA, joined with the Committee T1, none of which included punch list items, published its draft standard as an interim standard named as J-STD-025. TIA and Committee T1 then adopted J-STD-025 as the accepted standard defining technical services, features, and interfaces to satisfy the safe harbor provisions of CALEA.

While the debates on capability requirements of CALEA were going on, the industry petitioned the FCC to extend the compliance due date for meeting the capability requirements of CALEA. In September 1998, the FCC, under its rulemaking authority granted by CALEA, released "Memorandum Opinion and Order FCC 98-223" extending the compliance date from October 25, 1998 to June 30, 2000, for all telecommunications carriers industry-wide (Federal Communications, 1998c).

In November 1998, the FCC, under its rulemaking authority granted by CALEA, released "Further Notice of Proposed Rulemaking FCC 98-282" to address deficiencies in J-STD-025 to comply with the capability requirements (Federal Communications, 1998). Then, to clarify the CALEA requirements, the FCC released three documents:

- "Report and Order", in March 15, 1999, to clarify system security and integrity provisions imposed in § 105 (Federal Communications, 1999a).

- "Second Report and Order", in August 31, 1999, to clarify which categories of service providers are subject to CALEA requirements (Federal Communications, 1999b).
- "Third Report and Order", in August 31, 1999, to set out capability requirements for compliance with CALEA's requirements (Federal Communications, 1999c).

Among these three documents, the "Third Report and Order" has been the most disputable document because it involves the most controversial issues between the industry and law enforcement.

The Third Report and Order essentially adopted the J-STD-025 standards plus six of the nine punch list items. These six items are information regarding: 1) party hold, join and drop on conference calls; 2) subject-initiated dialing and signaling; 3) in-band and out-of-band signaling; 4) call timing; 5) dialed digit extraction; and 6) content of subject-initiated conference calls. The other two issues, discussed in the report were the geographical location and packet-mode communication. The FCC mandated a location tracking capability that will identify cell site location at the beginning and termination of a call. For packet-mode communication the FCC required the industry representatives to deliver a report containing details about interception of packet-mode communications by September 30, 2000. In addition, the FCC also required the industry to start delivering packet-mode communications not later than September 30, 2001, under the standards that would be described by that time (Federal Communication, 1999c).

Following the FCC's adoption of the Third Report and Order in August 1999, five industry associations, three telecommunication companies, and four civil liberties groups including the U. S. Telecommunications Association (USTA), Electronic Privacy Information Center (EPIC) filed petitions for review of the "Third Report and Order" in the U. S. Court of Appeals for the District of Columbia Circuit. The central issue in the petitioners' briefs was privacy protection. The petitioners claimed that the FBI's punch list's items concerning the location of antenna towers used in wireless telephone calls, dialed digit extraction, packet-mode communications, and signaling information from custom calling features (such as call waiting and call forwarding) are not covered by the "call-identifying information" concept of CALEA, and they could be subject to Fourth Amendment privacy protections. Although the main concern was privacy protection, each argument turns on whether FCC violated the Fourth Amendment and the CALEA requirements protecting the communications privacy and minimizing the cost of compliance, by overstepping its authority, or acting in an arbitrary and capricious manner through impermissible expansion of the capability requirements defined in § 103(a)(2).

According to Nylund (2000), the Third Report and Order conveys an intention to preserve the status quo for law enforcement while strictly construing the language of CALEA so as to minimize its economic impact on the telecommunications industry. Nylund (2000) argues that exempting the punch list items from the "Third Report and Order", contravenes the primary mandate of CALEA, which is to preserve law enforcement's ability to conduct properly authorized electronic surveillance in the face of a rapidly changing telecommunications technology. Furthermore, he rejects the argument

concerning the Fourth Amendment, because he argues that the Fourth Amendment creates individual rights against certain government searches and seizures, but does not grant telecommunications carriers any rights to avoid FCC regulations. Finally, he argued that with the exception of the civil liberties groups that joined the appeal, the petitioners' privacy arguments largely seem to be pretext for economic concerns about the costs of meeting technical standards in the Third Report and Order, and the expected loss of future profit because of loss of confidence in the international marketplace which demand secure telecommunications equipment and service (Nylund, 2000).

On August 15, 2000, the U. S. Court of Appeals for the District of Columbia Circuit affirmed the FCC's decision not to remove the antenna tower location information capability and the packet-mode data capability from J-STD-025. The Court vacated and remanded to the FCC four of the punch list items that the "Third Report and Order" required. These four items are: party hold, join and drop on conference calls; subject-initiated dialing and signaling; in-band and out-of-band signaling; post-cut-through dialed digit extraction. The Court reasoned that FCC's decision to include these four items reflected a "lack of reasoned decision-making", because the FCC had not: 1) explained the basis for its conclusion that these four items are required by CALEA as "call-identifying information"; 2) identified any deficiencies in J-STD-025's definition of call-identifying information; 3) explained how its order would satisfy CALEA's requirements about minimizing the compliance cost of the Act; 4) explained how post-cut-through dialed digits would "protect the privacy and security of communications not authorized to be intercepted" (Center for Democracy, 2000b; Nylund, 2000; U. S. Telecom

Association, et al., Petitioners v. Federal Communications Commission and U. S. of America, Respondents; Airtouch Communications, Inc., et al., Intervenors, 2000). After the Court decision the FCC extended the compliance deadline for the capability requirements of CALEA until March 31, 2001 (Federal Communications, 2000a). Furthermore, on October 17, 2000, the FCC released a "Public Notice" which sought comments from the related parties and also anyone who personally wanted to make a comment on the issues identified by the court in its decision, and what actions should take to satisfy the court's concerns, by December 20, 2000 (CALEA Implementation, 2000; Federal Communications, 2000b; Federal Communications, 2000c).

Implementation of the Capacity Requirements

§ 104 of CALEA mandates the Attorney General to provide information about the "actual" and "maximum" numbers of simultaneous interceptions that law enforcement needs before and after October 25, 1998, respectively.

On October 16, 1995, actual and maximum capacity requirements were presented by TILU of the FBI, and issued in the Federal Register under the title of "Initial Notice and Requests for Comments" (1995). In the notice, geographical regions are categorized into three categories as Category I, II, and III. Category I, the highest category, represents those geographic areas where the majority of electronic surveillance are conducted. Category II is the intermediate category, and Category III is the lowest category where law enforcement needs minimum number of surveillance capacity. According to the

Initial Notice (1995), the percentage of capacity meeting the actual and maximum capacity requirements of law enforcement are:

- For Category I regions, actual capacity requirement is 0.5 % and maximum capacity requirement is 1 % of the engineered capacity of the equipment, facilities, or services.
- For Category II regions, actual capacity requirement is 0.25 % and maximum capacity requirement is 0.5 % of the engineered capacity of the equipment, facilities, or services.
- For Category III regions, actual capacity requirement is 0.05 % and maximum capacity requirement is 0.25 % of the engineered capacity of the equipment, facilities, or services.

The First Notice allowed ninety days for the comments. The received comments were evaluated and law enforcement personnel participated in more than ninety meetings with industry representatives, privacy advocates and other interested parties. After deliberations, the required capacity of law enforcement was separated as wired and wireless. The requirements were defined in terms of fixed numbers rather than percentages of full capacity of the switches. Under the illumination of the comments on the initial notice, the "Second Notice and Requests for Comments" (1997) was issued in the Federal Register on January 14, 1997. In the Second Notice (1997), a formula is presented to calculate the required capacities for each specific geographic region. The formula involved two variables: historical baseline of electronic surveillance activities in a specified geographical region and the "growth factor." To determine the historical

baseline activity, the FBI used the following methodology in the Second Notice (1997): the FBI compiled data, including combined federal, state and local surveillance activities for each county nationwide between 1993 and 1995. From this data, the 24-hour peak surveillance activity over the 26-month period is determined. Then, the FBI added the peak surveillance activities of each switch, even if these peaks did not occur simultaneously.

The Second Notice (1997) allowed a 30-day comment period, and this period was extended an additional 30 days. After assessing the comments on the Second Notice, the "Final Notice of Capacity" (1998) was issued, on March 12, 1998. The capacity requirements in the Final Notice of Capacity (1998) were calculated by using a method similar to the method described in the Second Notice (1997). In the Final Notice (1998), for wired communications, county boundaries were used to define geographic locations. This is appropriate for law enforcement because usually county boundaries are same as their jurisdiction boundaries. It is also appropriate for the carriers because they usually have county-based regulations. For the wireless carriers, wireless market service areas were designated as geographic locations. The First, Second and Final Notice of Capacity documents have also been part of the implementation of capacity requirements part of the FBI's Implementation Plan.

Response of Industry Advocates to the FBI's Capacity Requirements

The "Initial Notice and Requests for Comments" (1995) required companies in major cities to install a surveillance capacity that would allow simultaneous monitoring

of up to 1 % of customer lines in service. The notice was criticized by the industry and privacy advocates for being excessive and then the FBI withdrew it.

The second notice was also subjected to the harsh criticisms. The criticisms were (Center for Democracy, 1997b; Center for Democracy, 1997c):

- The requirements in the notice were exaggerated. In determining the capacity, it used a methodology, which assumed peak the activities of all of the switches over the course of 26 months occur simultaneously.
- The notice required the installation of useless capacity, because it required each and every carrier serving in a particular area to install the capacity to meet the total surveillance requirements in that area.
- The notice required carriers to install interception facilities for areas with zero historical interception activity.
- Although the CALEA required distinguishing interceptions of call content and call-identifying information through pen registers or trap and trace devices, these were not distinguished in the notice. On the other hand, distinguishing the interceptions of call content and call-identifying information is important in terms of the cost of the implementation.
- According to CALEA, the government reimburses the increased capacity requirements. However, in the notice, it was stated that the new capacity requirements, released after the Final Notice of Capacity, would not be paid.

Furthermore, CDT asserts that the CALEA implementation plan of the FBI has a dilemma in meeting the requirements of the second notice because, according to the

implementation plan, carriers may or may not meet the requirements of the Second Notice of Capacity depending on the negotiation with the FBI (Center for Democracy, 1999).

- The FBI exaggerated law enforcement's past surveillance requirements by aggregating activity that had occurred over many months into a single, one-day peak.
- The notice required the installation of useless capacity, because it required each and every carrier serving in a particular area to install the capacity to meet the total surveillance requirements in that area, even if the carrier served in a portion of the area.
- In the Notice, the carriers are required to install in each switch a capacity sufficient to meet the requirements projected for the entire county, or multi-county service area. To take an extreme example, the notice requires just one of the landline carriers in Los Angeles to install the capacity to perform 46,100 simultaneous intercepts.

Furthermore, although CALEA mandates that the actual capacity requirements must be published in the Federal Register not later than 1 year after the enactment date of CALEA, the "Final Notice of Capacity" has been available after more than three years of the enactment (Center for Democracy, 1999).

USTA advocates sought review of the FBI's capacity requirements in the U. S. District Court for the District of Columbia. USTA advocates contended that the capacity requirements of the FBI are inflated by the cumulative effect of the FBI's rules and

methodology in determining the requirements. In the Court, defendant, the FBI, argued that the claims should be dismissed for two reasons (U. S. Telecom Association v. FBI, 2000):

- The plaintiff failed to establish that any of its members suffered any injury "because what it alleged was an overestimation of the surveillance needs" of law enforcement.
- The FBI Director has the authority to use any measure to determine the number of electronic interceptions that law enforcement agencies need.

Finally, in U.S. Telecommunications Association, et al. v. FBI (2000), the Court held that the FBI's approach was reasonable; therefore, the Final Notice of Capacity was upheld.

The Implementation Priorities in the FBI's Implementation Plan

According to the FBI (1997c), in the CALEA implementation plan, both the priorities of law enforcement, and business processes of the industry were intended to be matched as much as possible because of two factors. First, the business process of the industry was quite straightforward, and the methods and the time frames for the developments were specific. Second, it was considered that the greater the consistency with the industrial business process, the lower the cost of the implementation (Federal Bureau, 1997d).

The business process of the industry has three steps (Federal Bureau, 1997c):

Step-1: System engineering: In this step, technical analyses and cost estimations are conducted by the manufacturer. In the implementation plan, it was estimated that system engineering for a platform would take six months. It was planned that system engineering for most of the platforms would be carried out in 1997.

Step-2: Engineering development: This step is carried out based on outcomes of the previous step. In the implementation plan, it was intended that the engineering development phase for a platform would take a year.

Step-3: System deployment: At this step, the designed item is installed.

CALEA implementation process took four priorities into account: equipment, system engineering, engineering development, and system deployment priorities. The priorities were designed as much as parallel to the business process of the industry. These priorities were the following (Federal Bureau, 1997c):

Step 1: Equipment Priorities: There were nineteen equipment platforms concerned by law enforcement. The priorities among those platforms would be determined based upon the historical interception activities during the period of January 1993 through March 1995.

Step 2: Systems Engineering Priorities: In this step, the compliance costs of the modifications for each platform would be estimated. The priorities would be determined based upon these estimated costs. The total costs of the modifications for the selected platforms were limited by the CALEA to $ 500,000,000. Within the limit of $ 500,000,000, the FBI estimated that totally 14 out of 19 platforms would be modified at the first. The selected 14 platforms would move to the next step.

Step 3: Engineering Development Priorities: In this step, the priorities would be set to determine the optimum CALEA feature set for each platform.

Step 4: System Deployment Priorities: The developed systems would be planned to be deployed to the priority counties and markets. The priority counties would be determined based on the historical interception and crime activities in the counties (Federal Bureau, 1997c).

The FBI required the industry to sign the "cooperative agreement" to ensure the consensus between the industry and the FBI on the priorities and the platforms that would be changed first. The FBI claimed that the "cooperative agreement" would facilitate development of CALEA solutions, as well as coordinating efforts of law enforcement and the industry towards the implementation of the Act (Federal Bureau, 1997c).

Response of Industry Advocates to the Priorities of the FBI's Implementation Plan

The advocates agree with the FBI that the prioritization is essential because of limited funding authorized by the CALEA.

According to industry advocates, in the implementation plan, the FBI mentioned priorities in general frame but it didn't specify them. For example, no prioritization was made among the switch platforms, services and service providers (or service areas). Similarly, the FBI didn't state the priority among the requested features. Furthermore, although the FBI stated that it would pay for the modifications of fourteen switch platforms out of nineteen, it didn't state which exactly these fourteen platforms were.

The advocates argued that, by failing to determine the priorities, the industry was led to believe that the FBI aimed to get the industry to implement all the platforms and features without priority. The industry was also led to believe that there would be no sufficient reimbursement for the costs of the implementation. Furthermore, the lack of prioritization caused more confusion for the small companies because of their limited budget and their hesitations about the reimbursement.

In the plan, the FBI stressed the importance of the "cooperative agreement". Since the "cooperative agreement" imposes the obligations, which are not mandated in the CALEA, no carriers wanted to sign the agreement (Center for Democracy, 1997c).

Implementation of the Reimbursement

The FBI planned $100 million for the reimbursement in fiscal year 1997 and additional $100 million for each year of following four years.

According to the FBI Implementation Plan (1997c), signing the "cooperative agreement" for the carriers is essential to receive the reimbursement because it is a requirement of § 109 of CALEA. The business process would begin, after starting the "cooperative agreement". The specific amount of reimbursements would be determined after the cost analyses carried out in system engineering phase of the business process, and the reimbursement received would be depend on the responsiveness of the industry to the process.

In the CALEA Implementation Plan, the FBI also stated that the costs of capacity requirements, released after the Final Notice of Capacity, would not be reimbursed (Federal Bureau, 1997c).

Response of Industry Advocates to the Reimbursement Plan of the FBI

The responses and arguments of the industry advocates to the Reimbursement Plan section in the FBI Implementation Plan are the following (Center for Democracy, 1997c):

- The FBI had no base in reimbursement plan. It simply spreads $ 500 million equally over five years. There is no way that the estimation reflects the real figures because the FBI didn't obtain any cost information from the industry. In fact, the industry would fail to make an accurate cost estimation because the FBI had not provided the exact capability and capacity requirements as well as the priorities to the industry.
- The FBI plan required the "cooperative agreement" for the reimbursement, although the CALEA does not require the "cooperative agreement" or any other form of agreement.
- "The Cost Recovery Rules" and "Final Cost Recovery Rules" documents prepared by the FBI, hide the true costs of CALEA requirements and shifted the charge of the implementation from government to the industry as much as possible. For example, the entire cost of the transition period was supposed to be imposed on the carriers.

- In the implementation plan, another problematic issue was the required modifications on the equipment deployed after January 1, 1995. In the implementation plan, the FBI had presumed this equipment would comply with the CALEA. However, CALEA allows the companies to petition the FCC to determine if the compliance was reasonably achievable or not for the equipment installed after January 1, 1995.
- In the plan, it was stated that the system-engineering phase took 6 months and engineering development phase took 12 months, then the production and deployment would follow. According to these estimations of the FBI, the equipment complying with the CALEA would not be manufactured until 1999. However, the implementation plan didn't include the information about the reimbursement of costs of modifications for the equipment installed after January 1, 1995. Another result drawn from this time calculation is that the compliance date, October 25, 1998, was not reasonable.

In U.S. Telecommunications Association, et al. v. FBI (2000), another argument of industry advocates was that the FBI's cost recovery rules failed to comply with the reimbursement provisions of CALEA. In Court, defendant, the FBI, argued that the claims should be dismissed for two reasons:

- The plaintiff had "failed on their merits."
- The plaintiffs were "not ripe."

The Court declined to address this issue at that time because no member of the plaintiff organization had incurred any reimbursable costs of modifying equipment to comply with CALEA.

The Last Figures of the Reimbursement

For the implementation of CALEA, total amount of funds appropriated by Congress was $ 499,557270 as of September 30, 2000. Congress appropriated $ 200,977,000 in FY 2001 (CALEA Implementation, 2000).

CHAPTER 4

EXPLORATION OF WIRETAPPING LAWS OF BRITAIN, CANADA, GERMANY, FRANCE, TURKEY, AND ANALYSIS OF THEM WITH THE UNITED STATES WIRETAPPING LAW

This chapter aims to explore the legal positions of Britain, Canada, Germany, France and Turkey in terms of wiretapping and then analyze those positions with U. S. wiretapping regulations.

In this chapter, five countries were selected for the discussion and comparison for their widely acclaimed leadership and focus on wiretapping issues (South Africa. South African Law Commission (SALC) Report, 1998). The major limitation in the selection and studying of these countries is lack of written documentation in English and Turkish. As well as language, the second factor addressed during the selection of countries was whether they had a common or a civil law system.

Britain and Canada, like the U. S., have a common law system, which is derived mainly from judicial decisions. The German, French, and Turkish legal systems, derived from the Romano-Germanic legal tradition, differ completely from the Anglo-American common law concept: it is based on the civil law tradition of continental Europe, which has its origin in Roman law and is based on statutes and legislations (Fairchild & Dammer, 2001; Statsky, et al., 1984; Terrill, 1984; Unal, 1999).

By the criteria used in the selection of the countries, it is assumed that this chapter will provide a broader perspective in understanding the relationship between wiretapping and the law, given differing law concepts.

Background

The law of communication privacy has roots as far back as 1361, when the English Justices of Peace Act provided for the arrest of eavesdroppers. In 1858, France prohibited the publication of private facts. In 1890, American lawyers Samuel Warren and Louis Brandeis wrote a historical paper and described the right to privacy as the "right to be left alone" (Banisar, et al., 1999)

There are two major Directives, and two major institutions, which have motivated the European countries to enact communication and data protection laws.

The first data protection law in the world was enacted in the Land of Hesse in Germany in 1970. It was followed by national laws in Sweden (1973), the U. S. (1974), Germany (1977), and France (1978) (Flaherty, 1989). From these laws, the Council of Europe's (COE) 1981 Convention for the Protection of Individuals has evolved (Council of Europe, 1981). The 1981 Convention produced the Data Protection Directive and the Telecommunication Directive (Buttarelli, 1997; Council of Europe, 1995). These two have been major documents to provide European people with broad data and communications protections. The Data Protection Directive required the European Union (E. U.) member countries to enact data protection legislation by October 1998 (Council of Europe, 1995). The Telecommunication Directive imposes provisions on carriers and

service providers to ensure the privacy of users' communications, including Internet related activities (Buttarelli, 1997).

In addition to the Data Protection and Telecommunication Directives, the European Commission of Human Rights and the European Court of Human Rights created by the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms to oversee enforcement of the requirements of the convention have been the two major institutions to enforce the European countries to enact communication and data protection laws (Strossen, 1990).

Legal Position in Britain

British Constitutional and Legal Framework Concerning Privacy and Wiretapping

British legal history has a long and very rich tradition in the human rights field, from the Magna Carta in 1215, onwards through the Justices of Peace Act of 1361, the Habeas Corpus Act of 1679, and the Bill of Rights of 1689 (Banisar, & Davies, 1999; Unal, 1999). According to Unal (1999), such developments were so influential throughout the world that they were the motivating force behind the Declaration of Independence (1776) and the French Revolution (1789), which were milestones in the history of human rights, which led to the recognition of "the eternal and inviolable rights of man as a citizen."

Despite its great history in human rights, according to the SALC Report (1998), British common law has no general constraints to prohibit privacy invasion, and it has

failed to produce a remedy to protect the people from the invasion of communication privacy.

On the other hand, in recent years, the British legislation system has produced new legislation regarding the protection of communication privacy. The British Parliament approved the Interception of Communications Act (ICA) in 1985, which has been effective since April 10, 1986 (Britain. ICA, 1985). The main components of the Act involve a warrant system to authorize the interception, renewal and cancellation provisions, the establishment of the tribunal who is charged with processing the complainants, and the appointment of the commissioner who is responsible for reviewing the wiretapping activities. The Act was amended in 1997 to allow bugging of homes with only the permission of a chief constable or police commissioner (Banisar, et al., 1999).

In 1998, the British Parliament approved the Human Rights Act (1998) that would incorporate the European Convention of Human Rights into domestic law, a process that would establish an enforceable right of privacy (Britain. The Secretary of State, 1999). The Act went into force in October 2000. In May 1999, to ensure adherence with the European Convention on Human Rights incorporation into British law, the National Criminal Intelligence Service published a series of codes about interception, surveillance, use of informants, undercover operations and use of intelligence materials. In June 1999, the Home Office issued a consultation paper on wiretapping proposing many changes to the existing law. The papers require Internet service providers to facilitate wiretappings, lengthen the times for taps to six months, and authorize the use of roving wiretaps (Britain. The Secretary of State, 1999).

British Wiretapping Criminal Procedure

Offenses Subject to Wiretapping

§ 2 of the ICA addresses the offenses subject to wiretapping. According to § 2, the Secretary of State can issue the warrant only "…in the interests of national security…" or; "…for the purpose of preventing or detecting serious crime…" or; "…for the purpose of safeguarding the economic well-being of the United Kingdom" (Britain. ICA, 1985).

Exhaustion Principle

Before issuing the warrant, the Secretary of State considers investigation methods other than wiretapping (Britain. The Secretary of State, 1999).

Warrant and Related Issues

According to § 2 of the Act, The Secretary of State issues the wiretapping warrant (Britain. ICA, 1985).

Wiretapping Duration

§§ 4 and 5 require that the wiretapping warrant be issued for a maximum period of two months. In case of emergency, the official can issue the warrant for two working days (Britain. ICA, 1985).

Wiretapping Oversight

§§ 6 of the Act requires the establishment of an Interception of Communications Tribunal containing five members. Each of the members has to be a lawyer with at least

ten years of experience. According to § 7, each member serves for five years (Britain. ICA, 1985).

Any person who suspects that his communications may have been wiretapped has the right to apply to the tribunal. The tribunal, upon receiving the application, launches an investigation to determine whether there is a wiretapping, and then if there is one, whether it is done in accordance with the ICA. If the tribunal determines that there is a wiretapping conducted in accordance with the Act, they let the applicant know about it, but without stating whether it is in compliance with the Act or not. In cases where the wiretapping does not comply with the Act, the tribunal has the responsibility for presenting a report to the Prime Minister, and the authority to notify and compensate the complainant. The tribunal does not have an obligation to explain the reasons for its decisions and there is no appeal from its decisions.

The Act also mandates the Prime Minister to appoint a Commissioner. According to §§ 2, 3, 4, and 5, the Commissioner's functions include reporting the wiretapping breaches as well as presenting an annual report to the Prime Minister about the exercise of his/her functions (Britain. ICA, 1985). This report generally indicates the quantitative and qualitative measurements of the wiretaps which have been executed throughout the year, and the justifications and breaches for wiretappings. The Prime Minister has the power to exclude some part of the reports from the publication due to issues pertaining to national security, the well-being of the United Kingdom, or the prevention or detection of serious crimes. If anything is exempted from the publication, this is stated in the published version of the report (South Africa. SALC Report, 1998).

Exclusionary Principle

§ 9 of the ICA (1994) has the effect of prohibiting the use of wiretapped evidence obtained under a warrant issued under the Act[7]. The reason for such prohibition is the fear of law enforcement with the exposure of its wiretapping capabilities (Britain. The Secretary of State, 1999).

Since the apparent use of legally obtained wiretapped evidence is prohibited in trials, it is difficult to decide if there is a practice of exclusionary principle or not in Britain. However, according to Gottlieb, Levy, McAllister, Peck & Yenisey (1997), Britain does not have an exclusionary rule, in practice.

Mandatory Assistant Requirement and Property Right Issues

The Interception of the Communications Act has required telecommunications service providers to design their systems to be able to comply with wiretapping warrants. In a Consultation Paper, it is proposed that the communication service providers be required to take reasonable steps to ensure that their system is capable of being wiretapped each time when they introduce new services. In the paper, reasonable cost of compliance is proposed to be reimbursed by the government, but there is no information about what kind of costs would be reasonable (Britain. The Secretary of State, 1999). §§ 12 and 13 of the Regulation of Investigatory Powers Act 2000 (RIPA) provides some solutions to the costs problem (Britain. The Technical Advisory, 2000). According to § 12, the government pays the entire cost for the interception capability for small communication service providers. In the case of larger companies, the government makes

a contribution depending on the resources of the company and the technology involved (Britain. The Section 12 Order, 2000; Britain. The Technical Advisory, 2000).

Legal Position in Canada

Canadian Constitutional and Legal Framework Concerning Privacy and Wiretapping

Although there is no explicit right to privacy in the Canadian Constitution and Charter of Rights and Freedoms (1982), § 8 of the Charter, guaranteeing the right of individuals to be secure against unreasonable search and seizure has been interpreted as to protect an individual's right to a reasonable expectation of privacy (Canada. Hunter v. Southam, 1983).

The Privacy Act was enacted to strike a reasonable balance between the right of the state to intrude on privacy to carry out its responsibilities for law enforcement and the right of individuals to privacy. The Act restricted the Canadian law enforcement agencies on their discretion to intercept and disclose private communications. In fact, § 4 of the Act provides a civil action in damages against the government for unlawful interception of private communications (Canada. The Privacy Act, 2000).

Canadian Wiretapping Criminal Procedure

According to § 26 of the Canadian Security Intelligence Service Act (2000), the Canadian Security Intelligence Service Act governs the wiretapping of communications for national security cases, and Part IV of the Canadian Criminal Code governs the

[7] This prohibition must be interpreted as the prohibition of the explicit use of wiretapped evidence because,

wiretapping of communications other than those related to the threat to the security of Canada.

Offenses Subject to Wiretapping

The offenses in respect to which wiretapping may be used in Canada are mentioned in § 183 of the Canadian Criminal Code. These offenses are breach of duty, breach of trust, prison breach, bribery, fraud, fraudulent bankruptcy, corruption, perjury, obstructing justice, child pornography, uttering threats, forgery, money counterfeiting, sedition, hijacking, extortion, theft, robbery, arson, mischief, aggravated assault, sexual assault, murder, using or possessing explosives or prohibited weapon, kidnapping, hostage taking, abduction, advocating genocide, drug offenses, smuggling, keeping a gaming or betting house, endangering safety of aircraft or airport, offences against maritime navigation or fixed platforms, sabotage, spying, secret commissions, treason, unlawful interception, possession of an intercepting device, unauthorized use of a computer, possession of property obtained by crime, threat or attack on premises, residence or transport of internationally protected persons, participation in criminal organizations, or any other offenses that may be sentenced to imprisonment for five years (Canada. The Criminal Code, 1992).

Exhaustion Principle

In the affidavit, the applicant officer must state that other investigative methods have been tried and have failed or that other investigative methods are likely to fail or that the urgency of the matter makes the other methods impractical.

---

otherwise, conducting wiretapping does not make sense.

Before issuing the warrant, the judge must be satisfied with two issues. First, the judge must be satisfied that electronic surveillance is the last available investigation method or that the other methods have failed or have little chance of success. Second, the judge must be satisfied that there are reasonable and probable grounds to believe that an offense is being or has been committed and the electronic surveillance will be a useful investigation tool to obtain the evidence. Mere suspicion does not provide sufficient grounds for the judge to issue the warrant (South Africa. SALC Report, 1998).

Warrant and Related Issues

According to § 184.2(2) of the Criminal Code, an application for an authorization for wiretapping must be made by a peace or a public law enforcement officer, ex parte and in written form to a designated judge[8] and must be supported by an affidavit. The affidavit involves either swearing an oath or a belief statement that the matters contained in the application are true to belief or knowledge of the applicant. Furthermore, the affidavit includes the information about the existence of reasonable and probable grounds to believe that an offense has been or will be committed, the names, addresses, and occupations of the target person(s), type of private communications subject to wiretapping, the period for which the authorization is requested, and an explanation about why the other investigative techniques aren't preferred. The application form involves the belief that the communications subject to wiretapping are related to the offense.

All documents relating to an application are "confidential" and put in a package and sealed by a designated judge. The package is kept in the custody of the court and it is

[8] The designated judge is a judge of the superior court of criminal jurisdiction or a judge defined in § 552.

unavailable to the public. The sealed package can be opened and examined only upon a judicial order for the purpose of renewal and reexamination. One copy of the application and authorization documents is provided to the prosecutor upon request.

After authorization, the court order is transmitted to the applicant by means of telecommunication, and then the wiretapping is carried out within the framework of the order. The order includes the offense in respect to which the communications may be wiretapped, the type of communications subject to wiretapping, identity of the subject, duration of the wiretapping, and, if known, the place and manner of wiretapping.

After 90 days of the expiration of the authorization, the Crown lets the target subject know about the surveillance by a written notification stating that an authorization had been issued, executed, and delivered by the Crown (Canada. The Criminal Code, 1992).

Wiretapping Duration

The wiretapping warrant is issued for less than 60 days. § 186(6) contains the requirements for renewals of an authorization. In the renewal application, the officer makes the application to the designated judge, accompanied by an affidavit containing the reason and length of time the renewal is required, obtained information from the previous wiretap(s), date and time of previous application for wiretapping, the results, and the names of the judges who authorized the previous wiretaps. The renewal period is issued for less than 60 days. The total period of wiretapping must not exceed one year (Canada. The Criminal Code, 1992).

Wiretapping Oversight

An application for an authorization must be signed by either the Attorney General or Deputy Attorney General of the province, or Solicitor General of Canada or Deputy Solicitor General of Canada.

§ 195(1) of the Criminal Code mandates that the Solicitor General of Canada prepare an annual report, submit it to Parliament, and publish it to the public. The report involves the number of applications made for both authorizations and renewal of authorizations; number of applications granted and rejected; the numbers of persons both identified and not identified against whom proceedings arose; the average period for which authorizations and renewals were granted; the number of authorizations valid for more than 60, 120, 180, and 240 days; the number of offenses in respect to each type of offense; general description of the wiretapping methods in each wiretap; the number of persons arrested whose identity became known as a result of authorized wiretapping; and the number of criminal proceedings commenced because of the wiretapped evidence and the proceedings resulting in a conviction; the number of unauthorized wiretappings; and a general assessment about the role of the wiretapping of private communications for the investigation, detection, prevention and prosecution of offenses.

§ 195(4) of the Code mandates that the Attorney General of each province prepare and make available to the public an annual report concerning the wiretapping activities throughout the immediate preceding year (Canada. The Criminal Code, 1992).

Exclusionary Principle

In the SALC report (1998), it is stated that evidence obtained from unauthorized wiretapping cannot be used in the court. However, in the Criminal Code, many exceptions of the exclusionary rule appear.

§ 193(2) of the Criminal Code makes the evidence obtained without warrant or the consent admissible in any civil or criminal or any other proceedings where the person may be required to give evidence on oath (Canada. The Criminal Code, 1992).

In R. v. Duarte (1990), the Supreme Court of Canada decided that the simple consent of one party could not eliminate the need for the judicial warrant for private wiretapping; however, § 184.1(1) of the Canadian Criminal Code allows it. In fact, § 184.1(1) authorizes the wiretapping of private communication without warrant if the peace officer believes on reasonable grounds that such wiretapping is immediately necessary to prevent an unlawful act that causes serious harm to any person or to property, or the one party of the communication claims that he/she is an intended victim of the harm. § 184.2 of the Canadian Criminal Code permits the use of evidence obtained from the wiretapping pursuant to 184.1(1) if actually attempted or threatened bodily harm occurs (Canada. The Criminal Code, 1992).

Of the Criminal Code, § 188(1) governs the emergency wiretapping up to thirty-six hours with the consent of specially appointed judges. § 188(5) authorizes the trial judge to decide admissibility of the evidence obtained from wiretapping of communications pursuant to a subsequent authorization given under § 188 (Canada. The Criminal Code, 1992).

Mandatory Assistance Requirement and Property Rights Issues

In Canada, the telecommunications service providers have to assist law enforcement in the execution of wiretapping warrants (Britain. The Secretary of State, 1999).

Legal Position in Germany

German Constitutional and Legal Framework Concerning Privacy and Wiretapping

In the Constitution, Article 10 explicitly protects the communication secrecy (Constitution of Germany, 1998). In 1983, the Federal Constitutional Court interpreted Article 2 of the German Constitution in such a way as to provide protection to personal rights. In April 1998, German parliament amended § 13 of the Constitution so as to authorize the police to place bugging devices even in private domiciles (Banisar, et al., 1999).

In July 1999, the Supreme Court authorized warrantless screening of international communications by the German intelligence service (BND) to prevent terrorism and illegal drug and weapon trafficking. The court also held that the screening violated the privacy of communication secrecy protected by the Basic Law, but the screening could continue provided that the intelligence service did not pass on the information to the local police, and that the Parliament must enact new rules by June 2001 (Karacs, 1999).

German Wiretapping Criminal Procedure

Wiretapping is regulated by the G10-Law in Germany.

Offenses Subject to Wiretapping

The crimes in respect to which wiretapping may be used in Germany are mentioned in Article 108 of the Code of Criminal Procedure, and they include criminal association, murder, manslaughter, currency related offenses, robbery, extortion, illegal weapon and drug trafficking, terrorism, treason, and espionage (South Africa. SALC Report, 1998).

Exhaustion Principle

It must be proved that monitoring is the last available investigation method or that other methods have failed (South Africa. SALC Report, 1998).

Warrant and Related Issues

Any judge in German courts can issue the warrant (South Africa. SALC Report, 1998).

Wiretapping Duration

The investigative judge has the authority to issue the warrant for a maximum period of 90 days. In case of an emergency, when a judge is not available, a prosecutor has the authority to issue the warrant for a period of 3 days. If the initial wiretapping is successful, the wiretapping period can be extended for 90 days (South Africa. SALC Report, 1998).

Wiretapping Oversight

There is a parliamentary oversight body consisting of five political officials who oversee wiretapping activities targeting German citizens. Foreign surveillance activities

are oversight by The Federal Parliament (i.e. Bundestag) (South Africa. SALC Report, 1998).

Exclusionary Principle

Germany does not have an exclusionary principle (Gottlieb, et al., 1997).

Mandatory Assistance Requirement and Property Rights Issues

The Telecommunication Act mandates all the telecommunication service providers to install the required hardware and software in their switches to assist law enforcement for wiretapping of communications and to activate the wiretapping upon the request. According to the Act, the licenses of the providers who do not comply with the assisting requirements of the Act can be revoked (Britain. The Secretary of State, 1999; South Africa. SALC Report, 1998).

As well as the assistance requirement, the Act also mandates the service providers to provide call related data as old as eighty days, upon request.

In order to avoid legal problems concerning the governmental taking of private property, the Department of Justice pays the wiretapping cost, including 125 DM as well as the manpower costs of the service provider for each wiretapping. The government also has to pay 40 DM for each telecommunication line. Furthermore, according to the Telecommunication Act, buying the recording equipment is the responsibility of the police (South Africa. SALC Report, 1998).

Legal Position in France

French Constitutional and Legal Framework Concerning Privacy and Wiretapping

The protection of privacy provided by the French government traces back to 1858 when the French government prohibited the publication of private facts. However, the right of privacy is not explicitly protected in the French Constitution of 1958. The Constitutional Court ruled in 1994 that the right of privacy was implicit in the Constitution (Banisar, et al., 1999).

The Data Protection Act was enacted in 1978 and covers personal information held by government agencies and private entities. In addition to it, there are other protections incorporated in the Penal Code (Banisar, et al., 1999).

French Wiretapping Criminal Procedure

Electronic surveillance is regulated by an Act enacted in 1991 (Banisar, et al., 1999). According to the Act, there is a dual system of authorization of wiretapping in France. A legal wiretapping is authorized either by the administration or the investigative judge (South Africa. SALC Report, 1998). If enough evidence is obtained from the administratively authorized wiretapping, the wiretapping is transformed to the judicially authorized wiretapping by obtaining a wiretapping warrant from the judge. The statistics have shown that fifty percent of administrative wiretapping is transformed to judicial wiretapping. On the other hand, the judicial wiretapping cannot be transformed into administrative wiretapping (South Africa. SALC Report, 1998).

Offenses Subject to Wiretapping

According to the Act passed in 1991, administratively authorized wiretapping is used to protect democracy, economy and important information related to national security, to fight terrorism, organized crime, subversion, and espionage. Judicially authorized wiretapping is permissible for the offences punishable with imprisonment for at least two years (South Africa. SALC Report, 1998).

Exhaustion Principle

There is an exhaustion principle in the French regulations (Hong Kong. The Law Reform, 1996).

Warrant and Related Issues

Any judge in the French courts can issue the warrant (South Africa. SALC Report, 1998).

Wiretapping Duration

The duration of administrative wiretapping is four months and it can only be extended one more time upon strict scrutiny of the fresh application.

A judicial wiretapping is executed for less than twelve months (South Africa. SALC Report, 1998).

Wiretapping Oversight

The Act of 1991 created the Commission National de Control des Interceptions de Securite (CNCIS), which sets rules and reviews administrative wiretaps each year. The member of CNCIS is appointed for six years and it works independently.

The Prime Minister submits an annual report to the CNCIS. The CNCIS prepares an annual report and publishes it at the end of January every year. It has the power to instruct the Prime Minister to terminate any wiretapping. In the past, the Prime Minster has followed the recommendations of CNCIS (South Africa. SALC Report, 1998).

Exclusionary Principle

The evidence obtained through administratively authorized wiretapping is not admissible in the court; therefore, such wiretapping is executed less often and usually it is executed for preliminary investigation purposes (South Africa. SALC Report, 1998).

Mandatory Assistant Requirement and Property Right Issues

In France, telecommunication service providers have the responsibility to assist the law enforcement in the execution of wiretapping (Britain. The Secretary of State, 1999).

Legal Position in Turkey

Turkish Constitutional and Legal Framework Concerning Privacy and Wiretapping

The right to privacy in general and the right to privacy of communications in particular are explicitly protected in the Turkish Constitution of 1984. Article 20 of the Constitution requires that everyone have the right to privacy. This article prohibits the search of a person and the search and seizure of his/her papers and belongings. Article 22 declares that everyone has the right to privacy and the freedom of communications and that this right cannot be hindered without probable cause (Constitution of the Republic of Turkey, 1984).

Criminal penalties for the invasion of personal freedoms and privacy appear under §§ 174 through 201 of the Turkish Criminal Code. The §§ 195 through 200 concerning freedom of communications govern the communications through letters, parcels, telegram, and telephone (Turkey. Turk Ceza, 1926).

§ 94 of the Code of Criminal Procedure regulates the criminal procedures relating to search and seizure. However, it doesn't have detailed procedure regarding wiretapping (Turkey. Ceza Muhakemeleri, 1929)

Turkish Wiretapping Criminal Procedure

Turkey does not have a statute entirely devoted to wiretapping or communication privacy. A significant part of wiretapping criminal procedures appears in the Code of Racketeering and Corrupted Organizations of 1999 (CRCO) (Turkey. Cikar Amacli, 1999). In fact, §§ 2, 3, 4, and 10 of the CRCO are devoted to the wiretapping criminal procedure and the search of both governmental and private computer records.

Offenses Subject to Wiretapping

The offenses in respect to which wiretapping may be used in Turkey are mentioned in §§ 2 and 3 of CRCO and include the offenses related to racketeering and corrupted organizations (Turkey. Cikar Amacli, 1999).

Exhaustion Principle

According to § 2 of CRCO, wiretapping is based on the probable cause, and it is carried out as a last resort.

Warrant and Related Issues

The judge on-duty from the highest court that exists in a given city other than the capital city of the country, may issue a warrant; judges from other courts in a given city are not authorized to issue a warrant. In the capital city, the judge on-duty from the national security court is authorized to issue a warrant.

§ 2 of CRCO describes the wiretapping criminal procedure. § 2 authorizes the judge to issue wiretapping for investigative purposes. In case of emergency, the District Attorney is authorized to issue a wiretapping warrant for 24 hours. CRCO also makes the District Attorney responsible for ordering the cessation of wiretapping upon the end of the duration mentioned in the warrant, or upon the obsolescence of probable cause (Turkey. Cikar Amacli, 1999).

Wiretapping Duration

The warrant is issued for up to three months, and this duration can be extended up to three months, but not more than twice.

Wiretapping Oversight

There is no permanent oversight body for wiretapping in Turkey.

Exclusionary Principle

A 1992 amendment to the Code of Criminal Procedure requires the exclusion of unlawfully obtained evidence (Turkey. Ceza Muhakemeleri, 1999).

Mandatory Assistance Requirement and Property Rights Issues

§ 2 of CRCO mandates that the telecommunications industry assist the law enforcement personnel authorized by the District Attorney in execution of the warrant. In

Turkey, there is no regulation about the reimbursement of compliance expenses of the telecommunications industry.

Analysis of the Legal Positions of the United States, Britain, Canada, Germany, France and Turkey in Terms of Privacy and Wiretapping Criminal Procedure

Constitutional and Legal Framework Concerning Privacy and Wiretapping

Despite its historical legal roots as far back as 1361, the right to privacy is not defined explicitly in the constitutions of the U. S., Canada, Germany, and France. Thus, the judicial branch has attempted to clarify the existence of privacy rights. In Pavesich v. New England Life Insurance Co. (1905), the Georgia Supreme Court linked privacy to the Bill of Rights. In this decision, Justice Cooley argued that the privacy right was guaranteed by the Fourth Amendment; therefore, the privacy right should be protected by the common law system (Craig, 1997).

In 1958, in the Luth decision, the German Court extended individual privacy protection into the civil field through the interpretation and application of the Civil Code (Gottlieb, et al., 1997). According to Craig (1997), the American and German approaches to privacy protection are similar in three ways. In both countries, the right of privacy was identified by constitutional expression; it has been judicially developed; and it has been approached indirectly. On the other hand, there is one significant difference between the German and American approaches to privacy protection. In the U. S. privacy was linked to the constitutional protections of liberties against governmental intrusion, in the Pavesich case (1905). In Germany, on the other hand, privacy was linked to the

constitutional protection of human dignity and personality (Banisar, et al., 1999). Like the U. S., and Germany, France has not explicitly stated the right to privacy in its Constitution.

Like the U. S. and Germany, Canada also chose the Constitutional approach through the Charter values. However, as opposed to the "indirect effect" approaches of the U. S. and Germany, the Canadian approach is direct. In other words, by the Charter-values approach, the general tort of invasion of privacy was introduced to common law through the role of the judiciary to develop common law on the principled basis formed by § 8 of the Charter (Barnhorst, 1997).

Since it has no written constitution, Britain attempted to find a remedy to privacy invasion in its common law system. However, according to Craig (1997), rigid and conservative approaches of British judicial interpretation of common law hinder Britain in providing privacy protection to its citizens. Craig (1997) criticizes the rigid approach of British judges as producing absurd and unjust verdicts rather than producing remedies.

Turkey has an explicit definition of the right to privacy in its Constitution. Furthermore, the Turkish Constitution has a separate article devoted to the protection of communication privacy. Despite the clear definition of such a constitutional right, there have been long debates about the right to privacy in Turkey (Civaoglu, 1996). Such debates lead to the conclusion that the protection of communication and data privacy is a controversial issue because of the intangible, subjective, and broad nature of privacy. Privacy varies in accordance with the environment and the subjective perceptions.

Moreover, it is a broad concept encompassing the privacy of information, communications, physical belongings, and the territory of individuals.

Like the other sides of European governments, wiretapping regulations have also been greatly influenced by the recommendations, judicial orders and the practices of the E. U. In fact, Article 8 of the 1950 Convention for the Protection of Human Rights requires respect for the privacy of individuals (Council of Europe, 1950). For example, wiretapping regulations in France were prepared and enacted upon the condemnation by the European Court of Justice, in April 1990 (South Africa. SALC Report, 1998). Similarly, to ensure adherence with the European Convention on Human Rights incorporation into British law, the British National Criminal Intelligence Service published a series of codes of practice on interception, surveillance, use of informants, undercover operations and use of intelligence materials in May 1999 (Banisar, et al., 1997).

In accordance with Data Protection and the Telecommunication Directives, produced by the 1981 Convention of the Council of Europe, Britain enacted the Data Protection Act in July 1998; and Turkey, a candidate member of E. U., has been working on the Code of Protection of Personal Data.

Article 11 of the American Convention on Human Rights has a similar meaning to Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms. Based on Article 8, the U. S. incorporated the requirement of Article 11 into Title III of Omnibus Crime Control and Safety Streets Act in 1968 (Banisar, et al., 1999).

The privacy provisions of Title III were updated through the relevant amendments of the ECPA of 1986 and the CALEA of 1994.

According to Craig (1997), the Canadian judicial system has drawn on the jurisprudence of the U. S., France, Germany and Quebec. The Protection of Privacy Act of 1996, modeled on the Title III of the U. S., has proved Craig's argument.

Although there is no clear division, the major motivation for Britain, Germany, France and Turkey to enact data and communication privacy acts is different from the motivation of Canada and the U. S. The major motivation for the U. S. and Canada to enact the communication and data privacy protection acts is more economical, such as promoting electronic commerce, producing more secure equipment and service to make more money. On the other hand, the major motivation of the European countries and Turkey is to have laws consistent with the Pan-European regulations (Banisar, et al., 1999).

Offenses Subject to Wiretapping

Part IV of the Canadian Criminal Code and Title III of the U. S. are similar in that the offenses subject to wiretapping are defined comprehensively. Furthermore, in the Canadian Criminal Code, there is a general statement allowing wiretapping for offenses punishable by at least five years of imprisonment, and Title III allows the wiretapping for offenses punishable by at least one year in prison (Canada. The Criminal Code, 1992; Electronic Frontier, 2000). A similar general statement appears in the French wiretapping

act of 1991. In the French act, wiretapping is allowed for offenses punishable by at least two years in prison (South Africa. SALC Report, 1998).

In the U. S., Title III was enacted at or about the same time as the Racketeering Influenced and Corrupted Organizations Act (RICO) as part of a federal legislation package, which targeted organized crime (Gottlieb, et al., 1997). In practice, it has been articulated that wiretapping has predominantly been used in fighting organized crime (Colbridge, 2000; Dempsey, 1997; Freeh, 1999). This is also apparent in the statistics that appeared in the 1997 Wiretapping Report (Administrative Office, 1997). Like the U. S., Turkey tied wiretapping to fighting organized crime.

Among the regulations of the concerned countries, Turkey has the poorest wiretapping regulation in terms of definitions of offenses subject to wiretapping. This is expected because Turkey is the only concerned country without a statute entirely devoted to wiretapping or communication privacy.

Generally, wiretapping is used to maintain national security, to prevent and detect serious crimes, and to protect the economic well being of the country. Although, in the American, British, and French codes, wiretapping is allowed when being used to protect the economic well being; such use of wiretapping is not explicitly stated in the codes of Canada, Germany and Turkey.

Exhaustion Principle

Inherently, wiretapping violates the right to privacy. The exhaustion principle is a tool to justify wiretapping. It implies that wiretapping is used if other investigative

methods have been tried and failed, or other investigative methods are likely to fail, or the urgency of the matter makes the other methods impractical.

As it is apparent in its definition, it is difficult to have a "cookie cutter" implementation of the exhaustion principle. Sometimes exhaustion is equated with the meaning of "national security". According to the former U. S. Attorney General Griffin Bell, the term, "national security" has become a "talismanic phrase" and it has been used to "ward off any questions about the legitimacy of any governmental conduct to which the phrase was applied" (Hong Kong. The Law Reform, 1996). The U. S. Foreign Intelligence Surveillance Act (FISA), which does not require the use of the exhaustion principle in surveillance of the offenses related to national security, proves the argument of Bell.

The implementation of exhaustion has a lot of difficulties because of its flexible nature. Although all of the countries of concern in this chapter have an exhaustion principle in the wiretapping regulations, in the French and British Acts, exhaustion is not stated as explicitly as it is stated in the other countries. In the U. S., FISA excluded surveillance of foreign nationals living both inside or outside of the U. S. from exhaustion.

Warrant and Related Issues

All countries of concern require either a judicial or administrative order for legal interception. Although, usually, consent of one party does not constitute a sufficient ground to bypass the judicial or administrative order, there are some exceptions. For

example, according to the Canadian Criminal Code a warrant is not required to monitor the conversations between the undercover agent and the drug traffickers, to protect the agent (Canada. The Criminal Code, 1992).

In Germany and France, a specific judge or judges have been appointed to consider applications. According to the SALC Report (1998), in France and Germany, this function is exercised by a political functionary, with respect to security related investigations.

As opposed to the other countries, in Britain, the Secretary of State is authorized to issue wiretapping warrants. Authorizing politicians to issue a warrant creates questions about the use of wiretapping as a political power, as well as questioning the violation of Montesquieu's separation of powers doctrine for democratic states.

Parallel with globalization and convergence, the countries have a tendency to create dual wiretapping systems. The components forming the dual system are the wiretappings concerning the criminal and national security issues. The U. S., France, Britain and Germany still have such dual systems. In the U. S., Title III and FISA regulate the different wiretappings; in France, administrative and judicial wiretappings have different regulations (South Africa. SALC Report, 1998); in Britain, some of the warrants are issued by the Home Secretary, the others are issued by the Secretary of State; in Germany, the 1994 decision of the Supreme Court made a warrant unnecessary for the screening of international communications (Banisar, et al., 1999). Perhaps the countries' need for surveillance of international communications through global networks such as the Internet contributes to the tendency to create dual wiretapping systems.

Wiretapping Duration

The wiretapping laws of the countries limit the wiretapping periods. Upon the completion of such a period, the warrant is renewed. The wiretapping durations are tabulated below. In the table, in the "United States" column, 30 & 90 days are the durations for Title III and FISA wiretappings, respectively. Similarly, in the "France" column, 120 and 365 days are the durations for administrative and judicial wiretappings, respectively. For the sake of articulation, the periods mentioned as months in the Britain, France and Turkey codes are converted to days while assuming that one month has 30 days.

Table 1: Wiretapping Durations

Country:	United States	Britain	Canada	Germany	France	Turkey
Duration:	30 & 90	60	60	90	120 & 365	90

Wiretapping Oversight

Each country has its own oversight system over wiretapping activities. In Britain, the commissioner appointed by the Prime Minister prepares an annual wiretapping report to the Prime Minister. Then the Prime Minister makes the report available to the public after required censorship. The France oversight system is the reverse of the British system. In France, the Prime Minister is responsible for presenting an annual wiretapping report to a designated committee, which has the authority to instruct the Prime Minister.

In Canada, the Solicitor General prepares an annual report and submits it to the Parliament as well as publishing it to the public. Like Canada and Britain, the U. S. also makes annual wiretapping reports available to public. Germany has the parliamentary oversight body. In Turkey, there is no designated oversight authority over wiretapping.

Exclusionary Principle

The exclusionary principle is important in that it deters law enforcement from obtaining evidence through illegal methods. In other words, it deters law enforcement from conducting warrantless wiretapping.

In the SALC report, it is stated that evidence obtained from unauthorized interception cannot be used in the Canadian courts (South Africa. SALC Report, 1998). However, there are a lot of exceptions. § 193(2) of the Canadian Criminal Code, for instance, it makes the evidence obtained without a warrant or consent admissible in any civil, criminal, or any other proceedings where the person may be required to give evidence on oath (Canada. The Criminal Code, 1992).

Canada, France, Turkey and the U. S. also have exclusionary principles in their regulations. The exclusionary rule was incorporated into the Turkish Code of Criminal Procedure with an amendment in 1992. According to Gottlieb (1997), incorporation of the exclusionary principle into Turkish regulations reflects the American influence on the Turkish criminal justice system that was originally modeled more on the continental European one than Anglo-American norms.

Britain and Germany do not have an exclusionary principle in their regulations. Section 9 of the British ICA (1985) prohibits the use of legally obtained evidence in the trial. This provision can be interpreted in such a way as to prohibit the use of wiretapped evidence but without letting the defendant know about the use of it. Otherwise, it wouldn't make sense to have interception regulations for Britain. This provision automatically eliminates the existence of the exclusionary principle in practice. Furthermore, this provision violates Article 6 of the European Convention on Human Rights, which requires the "equality of arms" between the prosecution and the defense in criminal proceedings. In fact, Article 6 requires that the defense have the right to know the evidence used against him to have a chance to defend himself/herself properly (Council of Europe, 1950). According to Banisar, et al. (1997), exclusion of the evidence is rarely practiced in these countries. It is probable that such practices of exclusionary rule be motivated by Article 6 of the Convention.

Mandatory Assistance Requirement and Property Right Issues

Assistance of the telecommunications industry is essential to conduct wiretapping in most of the telecommunication systems that have emerged in the last two decades. All countries concerned in this chapter, as well as the U. S. have legal provisions to mandate that the telecommunications industry assist law enforcement agencies in wiretapping. The assistance provisions in Canada, French and Turkish regulations require telecommunications service providers to activate the interception upon the request. The U. S. CALEA, British RIPA, and German Telecommunication Act mandate all the

telecommunication service providers to install the required hardware and software in their switches to assist law enforcement for wiretapping of communications, and to activate the interception upon the request. In addition, CALEA requires a $ 10,000 fine per day for the companies that do not comply with the act, and the German act requires revoking the licenses of the companies, which do not comply with the act.

The major difference between the American/British/German and Canadian/French/Turkish approaches is that the former approach requires structural changes, if necessary, in the design level of the telecommunication systems. The structural changes require considerable costs and exacerbate the property rights violation. To eliminate the property rights violation, in CALEA, the compliance cost was guaranteed to be paid $ 500,000,000 in the years from 1995 to 2000. To eliminate the same problem, German law mandates the government to pay 125 DM per line for system costs plus 40 DM for each line costs and manpower costs of wiretapping. British law doesn't specify the exact amount of money, and it requires the case-by-case calculation of the cost reimbursement. In fact, British law guarantees the full reimbursement for the interception capability for small communication service providers. In the case of larger companies, government makes a contribution depending on the resources of the company and the technology involved (Britain. The Section 12 Order, 2000). The British approach produces a question about complying with the equality principle in law.

According to Ward (1996), and the Center of Democracy and Technology (1997c), another property right issue with the implementation of CALEA is that it hinders the competitive ability of the U. S. telecommunications industry in the global

marketplace by mandating heavy design requirements and diminishing the attractiveness of the U. S. equipment which is designed in such a way that it is extremely vulnerable to interception.

CHAPTER 5

THE PROBLEMS OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994 AND THE RECOMMENDATIONS

In this chapter, after identifying the stakeholders of CALEA, the problems related to CALEA are determined. Furthermore, in this chapter, some recommendations are made toward the resolution of the problems identified. In the recommendations, as well as the literature, the wiretapping regulations of Canada, Britain, Germany, France and Turkey are used.

Identifying the Stakeholders in the CALEA Process

Welsh & Harris (1999) defined the stakeholder as "any person, group, or agency who has a legitimate interest" in the problem or intervention.

In the legislative history of CALEA, it was stated that the Act sought to bring balance among law enforcement, telecommunications industry, and privacy concerns (H. Rep. No. 103, 1994; S. Rep. No. 103, 1994). From this intention of the legislators three stakeholders are identified: privacy advocates, the telecommunications industry, and law enforcement. Hull (1996) agrees that these three are the major stakeholders in the struggle surrounding the CALEA implementation. According to Nylund (2000), the FCC is another player in CALEA.

As well as the industry, the FCC, privacy groups, and law enforcement, there are two other major stakeholders: The legislator, which is Congress, and the American society affected by the implementation. In sum, there are six major stakeholders in the CALEA process:

The U. S. Congress

The U. S. Congress enacted CALEA; therefore it is the "change agent" in the CALEA process.

Law Enforcement Agencies

Law enforcement has "change agent", and "initiator," and "action" roles in the CALEA process. According to CALEA, law enforcement agencies were handed the task of identifying problems both with existing technology and the technical standards proposed by the industry for CALEA compliance (Nylund, 2000). The motivation of them is to keep pace with technological challenges for more effective crime fighting (Hull, 1996).

The Federal Communication Commission

The FCC is another "change agent" of the CALEA process. The assistance capability provisions of CALEA impose duties upon the FCC as a referee in the dispute, over implementation, between law enforcement agencies and the telecommunications industry (Nylund, 2000).

Telecommunications Industry

The industry has both "action" and "target" roles in the CALEA process. According to CALEA, the industry had the initial responsibility for developing technical standards that met the Act's statutory requirements (Nylund, 2000). In addition, the industry is the major implementer of CALEA. On the other hand, the industry argues that CALEA constitutes a government taking of private property without compensation; therefore, it violates their property right guaranteed by the Fifth Amendment (Hull, 1996).

Privacy Advocacy Groups

They are the "targets" in the process because the implementation of the Act influences privacy issues. Privacy advocates argue that CALEA is both unnecessary and legally suspect in terms of rights guaranteed by the Fourth Amendment (Hull, 1996).

The American Citizens

The U. S. citizens are the "clients" of the process. They are supposed to benefit from the implementation of the Act.

Exploration of the Problems

At the beginning, the FBI initiated the CALEA process with the intention of overcoming all the then and future problems to conduct effective electronic surveillance.

This intention entailed a project of enormous properties. In fact, CALEA was a product of tremendous efforts involving the formation of tens of commissions and hundreds of meetings. Finally, CALEA was enacted on October 25, 1994. However, because of disputable and heavy provisions of CALEA, the enactment of CALEA has not been sufficient to stop the efforts of the FBI to overcome the problems related to electronic surveillance. In fact, until October 25, 1998, the official compliance due date, almost nothing has been implemented, and the compliance date was extended first to June 30, 2000, and then to March 31, 2001. From the reimbursement figures, it is understood that, the implementations done so far are extremely below what was expected and planned at the very beginning of the CALEA process.

In short, it is apparent that the CALEA implementation has been seriously retarded, and its implementation is in a state of uncertainty. In this section, the problems, retarding the implementation of CALEA is discussed.

Exploration of the Problems Sourced by Congress

Vagueness in the Act and the Privacy Right Problems

The legislators of CALEA made it flexible enough to handle new technologies (Freiwald, 1996). One may justify the flexible definitions in the acts, because the acts, usually, determine the general framework, not the detailed specifications. On the other hand, this flexibility has been producing vagueness in CALEA's interpretation. The legislators must have foreseen the vagueness in the act; therefore, in CALEA, the FCC is ordered as a technical supervisor in the disputes over the technical issues of CALEA.

However, this is not sufficient because the FCC is only mandated to supervise upon receiving a petition from the stakeholders.

CALEA represents the American wiretapping regulations. The secret nature of wiretapping threatens the privacy right in the first place. Besides this general problem, there are two general privacy invasion problems related to CALEA.

- The vague definition of the "call identifying information" authorizes the law enforcement agencies to access some private information under the low standards.
- CALEA doesn't contribute to the privacy protection of Title III in wiretapping criminal procedure.

The vague definition of pen register together with technological innovations, and judicial permissiveness allows law enforcement agencies to acquire much call identifying information by fulfilling the minimal pen register procedures (Freiwald, 1996). The use of pen registers, and trap and trace devices are not covered in the Fourth Amendment search and they require strikingly low standards. To use pen registers, and trap and trace devices 1) one must have an administrative, grand jury, or trial subpoena, and 2) the targeted information must be relevant to an ongoing investigation (Electronic Frontier, 2000; Schwartz, 1995). Furthermore, the subpoena doesn't require probable cause.

According to the FBI's interpretation, packet mode data, and geographical locations information, as well as the punch list items, is call- identifying information; therefore, they don't require a wiretapping order, but a subpoena (Office of Technology, 1995). As a result, for instance, the acquisition of the full content of a conversation, or a

video clip or a written file stored on the Internet can be acquired through the interception of pocket mode data communication under the low standards of pen registers, which don't require probable cause. This situation provides a great threat to privacy.

Another CALEA problem related to the privacy right is that it doesn't sufficiently contribute to the privacy protection provisions of Title III. Title III has some requirements to minimize the privacy invasions. These requirements involve the list of offenses subject to wiretapping, the exhaustion principle, wiretapping warrant, maximum wiretapping duration allowable on the warrant, wiretapping oversight and the exclusionary principle.

The List of Offenses Subject to Wiretapping: In terms of specifying the offenses subject to wiretapping to limit the privacy invasion, Title III, seems to be inefficient because it allows wiretapping of almost all types of offenses. In fact, in Title III, about a hundred offenses were listed. Besides there is a general statement allowing wiretapping for all offenses punishable by a year in prison.

Exhaustion Principle: According to Dempsey (1997), "to inform the issuing judge of the difficulties in the use of conventional techniques" has been sufficient to use wiretapping. Besides, FISA excluded surveillance of foreign nationals living both inside or outside of the U. S. from the exhaustion. In conclusion, the exhaustion principle is not sufficiently practiced.

Wiretapping Warrant: Since wiretapping is considered to be a search under the meaning of the Fourth Amendment, it requires a court order. According to the Center for Democracy (1997a), Judicial authorization has not served as an effective regulator on the

use of electronic surveillance. Between 1989 and 1995, no judge, state or federal, denied a single government request for wiretapping. The FISA court in its 17-year entire history (i.e. between 1978 and 1995) has never turned down a government electronic surveillance request.

Wiretapping Duration: Limiting the duration of wiretapping by statute is another requirement to limit the privacy invasion. Title III requires a 30-day limit for wiretapping of American citizens.

Wiretapping Oversight: In the U. S., annual wiretapping reports are prepared. The reports are also made available to the public. However, there are questions about the accuracy of these annual reports. For example, in the 1997 annual report, the total number of wiretaps authorized by federal and state courts was reported as 24 in Los Angeles throughout the year. Furthermore, it was reported that 13 of them were extended. In the report, the average length of both original authorization and extension was 30 days (Administrative Office, 1997). On the other hand, in the "Final Notice of Capacity" (1998), the FBI required just one of the landline carriers in Los Angeles to install the capacity to perform 46,100 simultaneous intercepts. The difference between the numbers in the annual report and the notice shows that the report mechanism doesn't work well.

Exclusionary Principle: Prohibiting the use of illegally obtained evidence is another principle limiting the illegal wiretapping. On the other hand, the U. S. Supreme Court decisions accepting the wiretap evidence obtained through the warrantless pen register (in Smith v. Maryland (1979)) and warrantless beeper surveillance (in United States v. Knotts (1983)), wiretapping with a warrant which doesn't include the name of

subject, wiretapping by the wiretap warrant without involving the name of the subject (in United States v. Donovan, et al. (1977)), and so forth show that the criminal justice system is reluctant to ignore the evidence relevant to the indictment of the suspicion (Albanese, 1984; Craig, 1997). According to Dempsey, between 1985 and 1994, 138 suppression motions out of 3060 cases, have been held. In other words the suppression rate has been 4.3 % between 1985 and 1994.

The Property Right Problems

The CALEA reimbursement requirement possesses a potential threat to the telecommunications industry's property right guaranteed by the Fifth Amendment. There are three Fifth Amendment issues articulated surrounding the CALEA process.

- The first issue is whether CALEA's system design requirements amount to a governmental taking that must be compensated under the Fifth Amendment.
- The second issue is that the telephone carriers argue that since, theoretically, law enforcement can at all times access the carriers' equipment, such access amounts to a permanent occupation requiring compensation (Hull, 1996).
- The last issue regarding the Fifth Amendment is the expected loss of future profit because of loss of confidence in the international marketplace which demands secure telecommunications equipment and service (Nylund, 2000).

Indeed, in CALEA, it is stated that $ 500,000,000 was allocated for the implementation of it. On the other hand, the Center for Democracy and Technology (1999) estimated the compliance cost to be $ 3-5 billion, and Farber in his testimony in

the Congress (1994), estimated it as around $1.5 billion per year. As a result, the telecommunications industry is dissatisfied with this insufficient compensation.

Exploration of the Problems Sourced by the Law Enforcement Excessive Desires and False Interpretations of the FBI

Some of the requests of the FBI drafted in the original proposal were too excessive to be implemented within the Constitutional framework. For example, the original proposal (BeVier, 1999):

- Provides no imbursement for cost of retrofitting of existing equipment, and for the reasonable costs of capacity demanded by the FBI.
- Requires the carriers to decrypt the messages encrypted.
- Does not permit the industry in the process of technical standard setting.
- Permits the government to dictate or prevent the development of any equipment.
- Offers less protection to transactional data.

These requirements as well as some others stated in the original proposal which was prepared under the control of the FBI, didn't pass in Congress (Digital Privacy, 1997). This caused the dissatisfaction of the FBI with CALEA. Then the FBI tried to enforce its requirements that were limited by the U. S. Congress by interpreting the provisions of CALEA broadly, and falsely and by giving a word in a given phrase multiple meanings.

For example, to support its demand for interception of conference calls after dropping the targeted party, the FBI reads into the statute the words "supported by the subscriber's service or facility." The statute, however, does not cover communications, "supported by" the subscriber's service or facility. Instead, the statute only covers communications "to or from" the subscriber's facility, equipment or service.

The FBI also supports its argument on interception of conference calls after dropping the targeted party, by the legislative history of CALEA. In the legislative history of CALEA, the purpose of CALEA is defined as to preserve the government's ability pursuant to lawful authorization, to intercept communication including advanced technologies, while protecting the communications' privacy and without impeding the introduction of new technologies (H. Rep. No. 103, 1994). This purpose contains a conflict in that it states both "to preserve the government's ability" and "conference calling". This confliction also complicates the interpretation.

Another example of the FBI's false interpretation is about the "party join, hold and drop messages" item of the FBI's punch list. To justify its claims that party join, hold and drop messages are mandated by CALEA, the FBI reads the Act as requiring call-identifying information on each "leg of a call." The statute, however, does not require carriers to break down calls into "legs." CALEA only requires carriers to provide "dialing and signaling information that identifies the origin, direction, destination, or termination of each communication" (Center for Democracy, 1998a)

The 103rd Congress, in H. Rep. No. 103 (1994) defined call-identifying information as information identifying " the origin, direction, destination or termination

of each communication." According to industry advocates, origin refers to the number of the calling party, and destination refers to the number of the called party. But in the case of wireless calls, the FBI interpreted the "destination" as not only the number of the called party, but also the cell site of the calling party (Office of Technology, 1995; Center for Democracy, 1998a).

Indeed, the confusion in the interpretation is even more complicated than described above. According to the FBI's interpretation, "destination" would mean the cell site of the called party when the called party is the subject of the surveillance. But "destination" would mean the number of the called party when the calling party is the subject of the surveillance (Office of Technology, 1995).

Another example of the FBI's false interpretation is the geographical location issue. In the legislative history of CALEA, it was explicitly stated that the call identifying information does not contain any information that may disclose the physical location of the subscriber except to the extent that the location may be determined from the telephone number (S. Rep. No. 103, 1994). However, in the "CALEA Implementation Plan" and in the "ESI Document", the FBI (1997c) claimed that the carriers were required to provide the geographical location information of the subscribers to the LEA.

According to Dempsey, in his speech in the U. S. House of Representatives, the problem caused by the FBI is more than a broad and false interpretation of the Act. In fact, the FBI has sought to dominate the industry standards process and sought to assume for itself the type of design control over the nation's telecommunications system that Congress expressly denied it during the legislative process of CALEA. Dempsey asserted

that the FBI exploits the potential of new digital technology to enhance rather than merely preserve its surveillance capability as opposed to the intentions of the legislators (Oversight Hearings, 1997).

In Weil's (1999) perspective, the FBI's attitude toward the expansion of use of criminal law exemplifies a trend that conflicts with the careful arrangement of power in the Constitution. Such expansion conflicts with the Articles of Confederation, which doesn't provide for any criminal law authority. Weil (1999) argues that the Framers were suspicious of any ability of the central government to act directly upon individual citizens; therefore wouldn't support the national police force infringing upon the rights of Americans.

Delay in Publishing the Capacity Requirements

Although CALEA mandates that the actual capacity requirements must be published in the Federal Register no later than one year after the enactment date of CALEA, the "Final Notice of Capacity" (1998) has been published after about three and half years of the enactment.

Exploration of the Problems Caused by the Federal Communication Commission

§ 107 (b) of CALEA authorizes the FCC to resolve technical conflicts upon petition of the industry, standard organizations or other related bodies. Despite the problematic inconsistencies between interpretation of the industry and the FBI, neither the FBI nor the industry has filed a petition regarding the interpretations of the technical requirements of CALEA until 1998. In 1998, industry representatives filed a petition to

shift the compliance date of CALEA. In this petition, the technical inconsistencies were superficially mentioned only as excuses to shift the compliance date (AT & T Wireless, 1998). In sum, from the enactment of CALEA to 1998, the FCC has been out of the CALEA process. This contributed to the complexity of the conflict on technical standards between law enforcement and the industry.

Furthermore, the FCC, in the Third Report and Order, complicated the process by accepting some items of the "punch list" without "reasoned decision making" (U. S. Telecom Association, et al. v. Federal Bureau of Investigation, 2000).

Exploration of the Problems Caused by the Telecommunications Industry

It is apparent that CALEA puts a heavy burden on the industry. Redesigning the large and complex Plain Old Telephone System is not easy or inexpensive. Such a large scale redesigning process possesses a threat to the economy and well being of the country through decreasing reliability of the systems. If we pay attention to bugs we come across in well tested and much similar systems, such as Internet Explorer or Microsoft Word, we can predict the likelihood for chaos in the American telecommunication network – and it would be take four years according to CALEA. As a more dramatic example, think about the chaos in the area of money transfers. Today, the system is working with almost 100 percent reliability and accuracy, but we do not know it will be working with the same reliability and accuracy as it is today, after the redesigning of the system (Farber, 1994). In the CALEA process, it is strange that the industry advocates have not addressed this issue.

Indeed, the unwillingness of the telecommunications industry in addressing the real issues is not restricted to the problem of redesigning the old telephone system. For example, in the issue of providing the geographical location of a mobile target, the industry advocates deem themselves more the advocates of privacy rights than the advocates of the telecommunications industry, and just argued that this requirement invades the privacy rights. But, they don't predominantly articulate that providing location information decreases the revenue through degrading the market reputation, so that it violates the property rights. In sum, the industry doesn't clearly address the problems.

On the other hand, there are two motivations behind the privacy advocacy roles of the telecommunications industry. First, they might have thought that they didn't have a strong justification in their cause against the law enforcement needs for electronic surveillance. Second, according to Freiwald (1996), the carriers are afraid of being exposed to civil litigations by the customers whose privacy rights are invaded because of inadvertent actions of the carriers toward the compliance with CALEA.

Summary of the Problems Identified

The problems identified in this thesis can be categorized into two groups: The problems for which the solution can be recommended, and the problems for which there is no need for recommending a solution because the time is overdue.

The problems for which the solution can be recommended are:

- Vagueness in the CALEA provisions and the privacy rights problems.

- The property rights problems.
- Excessive desires and false interpretations of the FBI.
- Unwillingness of the industry to address the real issues.

The problems for which there is no need for recommending a solution because the time is overdue are following:

- Delay in publishing the capacity requirements.
- Procrastination of the FCC.

Recommendations

What Congress should Do?

Recommendations for the Vagueness in the CALEA Provisions and the Privacy Right Problems

- Congress should make it clear that neither the FBI, nor the industry, but the FCC is the dominant authority to make a precise interpretation of the technical provisions of CALEA.
- Congress should specifically order the FCC to prepare a technical document involving the comprehensive and precise explanation of the capability requirements in general, "call identifying information" in particular.
- Congress should make a regulation classifying the "call identifying information" into appropriate categories and it should identify some of these categories as a search under the Fourth Amendment (Freiwald, 1996).

- Continuing technological developments and increases in technology use in daily life require new privacy protection regulations. For example, computerized switching systems generate more information about calling parties, and the increase in global networking has been facilitated to access this information. Under current law, the government has access to this information under minimal privacy standards. Therefore, Congress should take action to produce new privacy regulations to keep pace with the global, networked nature of communications and information storage (Oversight Hearings, 1997). While taking action, the government should consulted with technology experts (Yung, 1996).
- As well as taking immediate action, Congress should also periodically examine the balance between the individual rights to privacy, the industry's rights to property, and societal needs to wiretapping as an investigative crime-fighting tool.

For the problem arguing that CALEA doesn't contribute to the privacy protection of Title III in wiretapping criminal procedure, the following enhancements in the wiretapping criminal procedure is recommended:

- In Title III, wiretapping is allowed for investigating the offenses punishable by at least one year in prison. This one-year limit is recommended for reexamination because it is relatively low with respect to the similar limits stated in the wiretapping laws of France and Canada.

- The annual wiretap reports should carefully and accurately be prepared to be an effective oversight tool. As well as careful and accurate reports, an establishment of a tribunal, like the one in Britain, devoted to accepting and investigating citizen's complaints related to wiretapping is recommended because it may facilitate the resolutions of wiretapping abuses and enhance the privacy protection over society.

Recommendations to Solve the Property Right Problems

In the legislative history of CALEA, it is stated that any equipment, feature or service of a telecommunications carrier deployed before the date of enactment shall be considered to be in compliance with the capability requirements unless they are replaced or significantly upgraded (S. Rep. No. 103, 1994). This can be interpreted in such a way that the government is unwilling to pay the costs of retrofitting the equipment installed before October 1994 (Dempsey, 1997). Indeed, in general, in electronic designs, retrofitting is a more complicated and expensive solution than adding the same features to the new equipment; therefore, if the government pays the costs of future designs, it is a very logical expectation that the government pay for the retrofitting costs. As a result, Congress should make clear that the retrofitting costs are paid, as well as the costs of future designs.

Regarding the manner of reimbursement of the compliance cost, there are several alternatives. In CALEA, $ 500,000,000 is appropriated for the compliance cost in the years from 1995 to 2000. However, according to the industry, this amount is not enough. German law, to avoid legal problems concerning the governmental taking of private

property, mandates the German Department of Justice to pay 125 DM per line for system costs plus 40 DM for each line costs and the manpower cost of wiretapping. The British law requires the government to pay the entire cost for the interception capability for small communication service providers. In the case of larger companies, the British government makes a contribution depending on the resources of the company and the technology involved (Britain. The Section 12 Order, 2000).

The German type of reimbursement does not offer an appropriate solution for the CALEA property rights problems, because it does not consider the costs of retrofitting and new design requirements. Because, in the annual wiretap reports prepared by the Administrative Office of the U. S. Courts, there have been approximately less than 1500 wiretaps in a year. When we multiply this maximum number with the amount of compensation per line which logically cannot be more expensive than $ 1000, the cumulative compensation will be less than $ 500,000,000 which has been a harshly criticized figure for being insufficient by the industry advocates.

The British approach produces a question about complying with the equality principle in law as well as being excessively flexible and vague.

According to Nylund (2000), the subscriber will end up paying for CALEA through either higher taxes or increased telecommunications service rates. Hull (1996) proposes a federal "communications tax" imposed on consumers' telephone calls for the resolution of property right debates. This tax has additional attributes. First, without tax it is likely that carriers would pass any additional system design costs onto the customers in the form of higher rates. Second, if law enforcement decides that there is no need for

wiretapping in some areas, it will decrease the expense of the entire program. Finally, if the cost of compliance is too much, small carriers will not face a competitive disadvantage when upgrading their system (Hull, 1996). In this thesis, the "communications tax" proposed by Hull is recommended in terms of a resolution of property rights problems.

As well as the recommendation about compensation, it is recommended that Congress should limit the excessive capacity demands of the FBI to reduce the costs of compliance on the capacity requirements of CALEA.

In sum, it is assumed that all types of problems related to property rights be solved by appropriate reimbursement. To this end, in sum, the following are recommended in this section:

- Congress should make clear that the retrofitting costs are paid, as well as the costs of future designs.
- Congress should adopt a "communications tax" proposal similar to one proposed by Hull (1996).
- Congress should limit the excessive capacity demands of the FBI.

<u>What Law Enforcement should Do</u>

- The FBI should not try to be a dominant authority in the interpretation of CALEA. Instead, it should follow the FCC's interpretations.

- For its surveillance needs to come up with the technological innovations in the last few years, the FBI should prepare a new proposal to Congress rather than try to find a solution through the broad and false interpretation of CALEA.

What the Federal Communication Commission should Do?

The FCC should clearly determine what is in and what is outside the scope of CALEA (Center for Democracy, 1998c). While doing this, the FCC should adhere to the words of the statute.

What the Telecommunications Industry should Do?

- The industry should address that real issues. For example, industry advocates should act like advocates of the industry, not advocates of privacy.
- Like the FBI, the industry should not try to be a dominant authority in the interpretation of CALEA, either. Instead, it should follow the FCC's interpretations.

What Courts should Do?

- Judges of courts dealing with the CALEA problems, should reflect flexibility when interpreting the Constitution and CALEA because of the rapidly changing and flexible nature of telecommunications technology. To achieve the flexibility, the judges should not stick the literal meaning of words and should not merely consider the legislative intent (Carter, 1994; Statsky, 1984).

- The courts should be aware of the fact that they are not a rubber stamp authority, but they are the warrant issuing authority. Before issuing the wiretapping warrants, they should scrutinize the exhaustion.

CHAPTER 6

SUMMARY CONCLUSION AND IMPLICATIONS

A Summary Conclusion

Wiretapping is widely considered one of the most useful investigative techniques within the law enforcement community (Freeh, 1999).

CALEA, the last U. S. wiretapping law, came about because of the need for law enforcement agencies to keep pace with emerging telecommunications technologies while maintaining a delicate balance between public and private liberties (Hull, 1996).

CALEA involves two major sets of requirements: mandatory assistance requirements and privacy protection requirements. However, the assistance requirements are predominant, as it is also understood from the title of the act.

In the legislative history of CALEA, it was stated that CALEA sought to balance among law enforcement interests individual privacy rights and telecommunications industry's concerns (H. Rep. No. 103, 1994; S. Rep. No. 103, 1994). From this statement, it is understood that the CALEA process involves three major stakeholders: law enforcement, privacy advocates and the industry. In addition, Congress, the FCC and American society are the other major stakeholders. Although there are six major stakeholders, the most active players of the disputes over CALEA are held among the FBI, the FCC, the industry and privacy advocates.

From the perspective of law enforcement, protecting society against criminal activities has the highest priority. Especially, in recent years, the need to crack down on

crime has produced an atmosphere in which public officials suppose that wiretapping is a prerogative of the state and they have been willing to do anything including wiretapping, without regarding individual constitutional rights such as privacy, and property (Sheptycki, 2000; Weil, 1999).

On the other hand, the privacy groups claimed that the protection of privacy is as important as the physical protection of people. They argue that the corrosion of trust between human beings, corrosion of self-esteem, the undermining of the basis of social order, and the creation of paranoia and alienation are the major projections of the ubiquity of wiretapping; therefore, wiretapping has to be used only as a last resort in fighting serious crime, and use of it should be examined periodically (Dempsey, 1997; Marx, 1988).

Privacy advocates have two major complaints about the constitutionality of CALEA. First, they contend that the vague definition of the "call identifying information authorizes law enforcement agencies to access some private information under the low standards. Indeed, the FBI's interpretation of "call-identifying information" exacerbates the privacy invasion. In fact, the FBI has tried to enforce its requirements that were limited by the U. S. Congress during the legislative process of CALEA, by interpreting the provisions of CALEA broadly, falsely and by giving a word in a given phrase multiple meanings. The second complaint of the privacy advocates is that CALEA doesn't contribute to the privacy protection of Title III in wiretapping criminal procedure.

The CALEA provisions require the telecommunications industry to install equipment enabling law enforcement to maintain and facilitate its wiretapping abilities.

These provisions require undue burden over the industry. Despite CALEA's reimbursement provision aiming to mitigate the burden over the industry, the industry asserts that the reimbursement required by CALEA is not adequate because it fails to take into account all corners of the burden. For example, CALEA doesn't consider the loss of future profits of the industry because of loss of confidence in the international marketplace which demands secure telecommunications equipment and service (Nylund, 2000).

In the CALEA process, it is strange that the industry is unwilling to address the real issues. Instead, they act like privacy groups. There may be two motivations behind the privacy advocacy roles of the telecommunications industry. First, they may have believed that they didn't have a strong justification in their cause against the law enforcement needs for electronic surveillance. Second, according to Freiwald (1996), the carriers are afraid of being exposed to civil litigations by the customers whose privacy rights are invaded because of the carrier's inadvertent actions toward compliance with CALEA.

As well as the problems concerning privacy rights, property rights, false interpretations of the statute and the unwillingness of the telecommunications industry in addressing the problems, there are other problems contributing to the complexity of CALEA chaos and delay of CALEA implementation process. One of the factors retarding the implementation of CALEA is the procrastination of the U. S. Attorney General in publishing the capacity needs of law enforcement. In fact, publication has been put off by

about two and half years. Another procrastination in the implementation is the FCC's procrastination in the resolution of the conflict over capability requirements of CALEA.

As it is apparent, there are many variables and factors contributing to the complexity of CALEA problems. The courts and the FCC have been trying to solve these problems.

While the debates on capability requirements of CALEA were going on, the industry petitioned the FCC to extend the compliance due date for meeting the capability requirements of CALEA. In September 1998, the FCC extended the compliance date from October 25, 1998 to June 30, 2000, for all telecommunications carriers industry-wide (Federal Communications, 1998a).

To clarify the capability requirements of CALEA, the FCC released the Third Report and Order in August 31, 1999. Following the FCC's adoption of the Third Report and Order, industry and privacy groups filed petitions for review of it in the U. S. Court of Appeals for the District of Columbia Circuit. On August 15, 2000, in its decision, the court vacated and remanded to the FCC some of the requirements of the report (U. S. Telecom Association, et al. v. Federal Bureau of Investigation, 2000). After the Court decision, the FCC extended the compliance deadline for the capability requirements of CALEA until March 31, 2001 (Federal Communications, 2000a). Furthermore, on October 17, 2000, the FCC released a "Public Notice" which sought the comments from related parties and also anyone who personally wanted to make a comment on the issues identified by the courts in its decision, and what actions should be taken to satisfy the

court's concerns, by December 20, 2000 (CALEA Implementation, 2000; Federal Communications, 2000b).

Implications

When I note problems in the general frame, I see that it is Congress that made the major mistakes in the first place. Congress approached the CALEA process as being a "credulous observer," or an entity embracing the "scientific management theory" of Frederick Taylor. The "credulous observer" assumes that the policy goals are perfectly determined, are embodied in the statutory directives and are complied by all relevant entities. This perspective disregards the technical realities as well as the politics, personalities and incentives of the participants. When one notes the time sequence and timing of the implementation process of CALEA from the determination of capacity needs and the schedule of publishing capacity requirements to the reimbursement procedures, it becomes apparent that the legislators assumed that we lived in a frictionless world. They didn't forecast the problems, despite the dependent stages of the implementation and imprecise and flexible requirements. For example, the legislators didn't forecast that the implementation process would be retarded at the first step by the Attorney General by missing two and half year deadline for publishing the capacity requirements of law enforcement (BeVier, 1999).

On the other hand, it is not fair to accuse Congress of being a pure "credulous observer." For example, they predicted the possibilities of dispute over the technical capability requirements of the act; therefore, they authorized the FCC as a referee in

disputes over the technical capability requirements. The FCC was a good choice for dispute resolution in the CALEA process because "it has technical expertise ability and rulemaking authority and it is a disinterested but publicly accountable mediator" between law enforcement and the telecommunications industry (BeVier, 1999).

In this thesis, I identify the CALEA problems not from perspective of a "credulous observer", but from perspective of a "skeptical analyst", and I found that the CALEA process involves many flaws: It fails to identify the frame of the law enforcement concept, the privacy rights guaranteed by the Bill of Rights, the abilities, incentives and property rights of the industry. Furthermore, it wastes the public resources.

Between 1992 and 1994, the FBI conducted a series of surveys at the state and federal level and found 183 technology-based problems. The most common problem, identified by the FBI, accounted for 30 % of all problems, was the lack of sufficient capacity in cellular systems to accommodate the surveillance. The second common problem was the inability of certain cellular systems to provide call-identifying information to law enforcement on a real-time basis. (The cellular systems stored call identifying information, but there was a delay before the information could be accessed.) The third most common set of problems involve the special dialing features, such as speed dialing by pressing one key, not the full number it represents. The fourth problem was call forwarding. All of these problems are not uniquely digital problems; they exist in the analog world, as well. As a conclusion, from the skeptical analyst's perspective, the findings of the FBI survey cannot serve as a reasonable and feasible ground for a comprehensive redesign of the nation's telecommunication system that requires several

billion dollars and degrade the international reputation and competitive ability of the American telecommunications industry (Oversight Hearings, 1997).

Although someone may give credibility to the conclusion of skeptical perspective, I don't defend the pure skeptical perspective; therefore, I don't recommend a solution involving destroying everything, which has been done toward the CALEA implementation. I approach the problem under the illumination of practical realities making me believe that there have been lots of efforts in the CALEA process; therefore I cannot easily recommend eradicating all efforts toward the implementation of CALEA. Instead, I suggest making recommendations to find a common ground among the different interests of stakeholders of CALEA and to speed up the CALEA implementation process.

Since the greatest wrongdoer in the CALEA process is Congress, and it has power of law making, the majority of CALEA problems can be solved by Congress. Congress should consider the CALEA problems as an opportunity for the reexamination of wiretapping and related privacy laws as well as an opportunity to take into account the new nature of technology. In this solution and the reexamination process, Congress should be consulted by technology experts who have broad and up to date knowledge about technology and the capabilities of the industry and by the law enforcement representatives who are perfectly aware of wiretapping needs of law enforcement and by privacy advocates. In addition, Congress should keep in mind that the technologies have a flexible, decentralized, interactive, convergent and global nature. Accordingly, the laws concerning these technologies have to have the same characteristics as much as possible.

The law makers also know that preparing a law with a flexible, decentralized, interactive, convergent and global nature is an extremely painful process, and it requires the hands of the other nations; therefore, some regulations should be prepared at least in accordance with the E. U. Conventions and Directives as well as the regulations of the neighbor countries.

Today, neither the U. S. Bill of Rights nor Title III, or the U. S. Constitution offer explicit privacy protection against foreign government interception of the communications of U. S. citizens living abroad. Furthermore, the U. S. wiretap statutes have no extraterritorial application. Therefore, Congress should consider applying the court order requirements of Title III and FISA to interceptions of communications by the U. S. government abroad for use in U. S. criminal cases (Dempsey, 1997). In order to implement all of these activities, lawmakers should take into account wiretapping and other related legal documents of the other countries as well as the international regulations.

Indeed, there are some attempts toward promotion of the adoption of worldwide wiretapping standards. In June 1993, the FBI hosted an international conference on communications interception at Quantico. In 1995, the E. U. Council adopted a set of interception requirements for telecommunications systems similar to the requirements developed by the FBI and urged Member States to implement the requirements with respect to systems and service providers in their own countries. In 1996, the Telecommunication Standardization Sector of the International Telecommunication Union (ITU) was urged by Australia to include the E. U. surveillance requirements in its

recommendations (Center for Democracy, 1997a). Between 1993 and 1999, ITU met four times to determine worldwide wiretapping standards on telecommunications equipment.

According to Banisar, et al. (1999), there are four types of privacy protection practiced throughout the world:

- Comprehensive laws: There is a comprehensive law for privacy protection. There is also an agency or official that oversees enforcement of the act. E. U. countries, Canada and Australia have this model.
- Sectoral laws: Some countries such as the U. S. have avoided general data protection rules in favor of specific sectoral laws governing privacy. There are two drawbacks of that approach. First, it requires introducing the new legislation with each new technology so protections usually lag behind. Second, there is a lack of an oversight agency.
- Self-Regulations: Data protection is supposed to be achieved through self-regulations. Such policy is currently promoted by the U. S., Japan, and Singapore. It has drawbacks of inadequacy and enforcement.
- Technologies of Privacy: Privacy protection has moved into the hands of individuals through the privacy technologies, such as encryption, proxy servers, smart cards, and so forth.

This classification is useful in terms of laws governing technology.

Among these four ways of privacy protection, in my opinion, the last two are more attractive because of their more flexible, decentralized, interactive, convergent and

global nature. Probably, the privacy complaints surrounding CALEA can be solved by Congressional support to technologies of privacy.

For the property rights issues, Congress should reexamine the capability and capacity requirements and precisely determine and classify the concept of "call-identifying information" to minimize the cost of compliance with the Act. I argue that the lower the cost of compliance, the fewer the complaints about property right invasions.

§ 109 of CALEA requires reimbursement for the cost of the carrier's compliance for the equipment installed before 1995 and, to reimburse the cost that couldn't have been "reasonably achievable" after 1995. In the House Report, the "reasonably achievable" condition is defined as "the cost to the carrier of compliance compared to the carrier's overall cost of developing or acquiring … the feature …" (H. Rep. No. 103, 1994). In this statement, it is apparent that Congress aimed to minimize the cost of compliance for the telecommunications industry in order not to take private property guaranteed by the Fifth Amendment.

For the solution of problems hindering the competitive ability of the telecommunications industry, it is expected that worldwide standards in wiretapping will be a first step. In other words, if all telecommunication companies in the world are mandated to design their systems so as to provide the same interception capabilities, such design requirements will no longer constitute a disadvantage for the American telecommunications industry.

In addition to Congress, the solution of CALEA problems requires the hands of other stakeholders. The FBI, the industry, and the privacy advocates should stop the

interpretation of CALEA and should follow the FCC's interpretations and court decisions.

Like Congress, the judges of courts dealing with the CALEA problems should reflect flexibility when interpreting the Constitution and CALEA because of the rapidly changing and flexible nature of telecommunications technology. According to Craig (1997), such flexibility is more justifiable than conservatism because common law is judicially created, and it has an evolutionary character in response to changing social conditions. Craig (1997) argued that since the British judges have not shown flexibility in their decisions, they have produced absurd and unjust verdicts rather than producing remedies.

In this thesis, I agree with Socrates who argues that no matter how one answers the last question, there are more questions (Teaching Legal, 2001). Therefore, I don't claim that the recommendations made in the present study completely solve CALEA's problems. However, I expect that they speed up the CALEA implementation process.

Resolution of the issues surrounding CALEA will have important implications in two areas: First, they will make the law enforcement community keep pace with the technologies; second, the implications will offer a template for the balance of interests between the private and public liberties in the digital age.

Regardless of the debates over CALEA, technology is moving in directions so as to change the balance of powers (Oversight Hearings, 1997). The major responsibility of the stakeholders is to establish a reasonable ground to ensure that they are efficiently used for legitimate purposes.

REFERENCES

Administrative Office of the United States Courts. (1997). 1997 Wiretap Report [On-line]. Available: http://www.uscourts.gov/wiretap/report.pdf [2000, August 8].

Albanese J. S. (1984). Justice, Privacy, and Crime Control. Lanham: University Press of America, Inc.

AT&T Wireless Services, Inc., Lucent Technologies Inc., & Ericsson Inc. (1998). Petition for Extension of Compliance Date [On-line]. Available: http://www.cdt.org/digi_tele/extensionfile.html [2000, March 21].

Banisar, D., & Davies, S. (1999). Global Trends in Privacy Protection: an International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. John Marshall Journal of Computer, & Information Law, 18, 1-111.

Barnhorst, S. (1997). Criminal Law and the Canadian Criminal Code. Canada: McGraw Hill Publishing Co.

Beaney, W. M. (1966). The Right to Privacy and American Law. Legal and Contemporary Problems [On-line Serial], 31(253), 15437 words. Available: http://www.lexis-nexis.com [2000, October 10].

Berger v. New York, 388 U.S. 41 (1967).

Berk, R. A., & Rossi, P. H. (1999). Thinking About Program Evaluation (2nd ed.). Newbury Park: Sage Publications, Inc.

BeVier, L. R. (1999). The Communication Assistance for Law Enforcement Act of 1994: A Surprising Sequel to Break Up of AT&T. Stanford Law Review. [On-line Serial], 51(1049), 45779 words. Available: http://www.lexis-nexis.com [2000, December 14].

Britain. Human Rights Act. (1998). [On-line]. Available: http://www.legislation.hmso.gov.uk/acts/acts1998/19980042.htm [2000, November 21].

Britain. Interception of Communications Act. (1985). [On-line]. Available: http://www.swarb.co.uk/acts/1985InterceptionCommunicationsAct.html [2001, January 27].

Britain. Police Act. (1997). [On-line]. Available: http://www.legislation.hmso.gov.uk/acts/acts1997/97050--a.htm#1 [2000, November 21].

Britain. The Secretary of State for the Home Department. (1999). A Consultation Paper: Interception of Communications in the United Kingdom. [On-line]. Available: http://www.cyber-rights.org/inte rception/ioca99.htm [2001, January 27].

Britain. The Section 12 Order. (2000). [On-line]. Available: htttp://www.homeoffice.gov.uk/ripa/1213cons.htm [2000, February 13].

Britain. The Technical Advisory Board. (2000). Public Consultation on the Section 12 and 13 Orders or the Regulation of Investigatory Powers Act 2000. [On-line]. Available: htttp://www.homeoffice.gov.uk/ripa/1213cons.htm [2000, February 13].

Buttarelli, G. (1997). The European Telecommunications Directive. [On-line]. Available: htttp://www.privacyexchange.org/iss/confpapers/buttarelli97.html [2000, November 21].

CALEA Implementation Section – Regulatory. [On-line]. (2000). Available: http://www.askcalea.net/regulatory [2001, February 4].

Canada. Hunter v. Southam Inc. 2 S. C. R. 17569. (1983). [On-line]. Available: http://www.lexum.umontreal.ca/csc-scs/en/publies/1984/vol2/html/1984scr2_0145.html [2000, November 21].

Canada. Michaud v. Quebec, 3 S. C. R. 23764 (1996). [On-line]. Available: http://www.lexum.umontreal.ca/csc-scc/en/pub/1996/vol3/html/1996scr3_0003.html [2000, October 26].

Canada. R. v. Duarte, 1 S. C. R. 20542 (1990). [On-line]. Available: http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol1/html/1990scr1_0030.html [2000, November 21].

Canada. R. v. Wong, 3 S. C. R. 20549 (1990). [On-line]. Available: http://www.lexum.umontreal.ca/csc-scc/en/pub/1990/vol3/html/1990scr3_0036.html [2000, November 21].

Canada. The Criminal Code, Chapter C-46. (1992). [On-line]. Available: http://www.mobrien.com/ccc.html [2000, November 21].

Canada. The Freedom of Information and Protection of Privacy Act. (1996). [On-line]. Available: http://www.oipcbc.org/BCLAW.html [2000, December 13].

Canada. The Privacy Act. (2001). [On-line]. Available: http://www.privcom.gc.ca/english/02_07_e.htm [2001, January 27].

Canada. The Security Intelligence Service Act. (2000). [On-line]. Available: http://emmaf.isuisse.com/emmaf/base/csisact.html#Short_Title [2001, January 27].

Carter, L. H. (1994). Reason in Law. (4th ed.). New York: Harper Collins College Publisher.

Center for Democracy and Technology. (1997a). Communications Privacy in the Digital Age (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/9706rpt.html [2000, March 20].

Center for Democracy and Technology. (1997b). Electronic Surveillance Report on the FBI's Publication of the Second Notice of Capacity (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/970114fbi1.html [2000, March 20].

Center for Democracy and Technology, Cellular Telecommunications Industry Association, United States Telephone Association, & Personal Communication Industry Association. (1997c). Industry and Privacy Advocates Response to FBI Implementation Plan (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/970429_resp.html [2000, March 20].

Center for Democracy and Technology. (1998a). Comments of the Center for Democracy and Technology (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/filing121498.html [2000, February 21].

Center for Democracy and Technology. (1998b). Petition for Extension of Compliance Date (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/extensionfile.html [2000, February 21].

Center for Democracy and Technology. (1998c). Reply Comments of the Center for Democracy and Technology (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/cdreplycom.html [2001, February 8].

Center for Democracy and Technology. (1999). FBI Seeks to Impose Surveillance Mandates on Telephone Systems: Balanced Objectives of 1994 Law Frustrated (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/status.html [2000, March 20].

Center for Democracy and Technology. (2000, August 15). CDT Policy Post. [On-line Serial], 6, 15. Available: http://www.cdt.org/publications/pp_6.15.shtml [2001, February 8].

Center for Democracy and Technology. (2001). Comments of the Center for Democracy and Technology in Response to the Public Notice DA 00-2342 (CC Docket No. 97-213). [On-line]. Available: http://www.cdt.org/digi_tele/001116cdt.shtml [2001, February 8].

Chilton B. S. (1991). Prisons Under the Gavel. Columbus: Ohio State University Press.

Civaoglu, G. (1996, December 1). Demokrasinin Irzina Gectiler. Milliyet, p.1, 18.

Colbridge, T. D. (2000). Electronic Surveillance: A Matter of Necessity. Law Enforcement Bulletin. 69(2), 25-32.

Communication Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, § 102, 108 Stat. 4279 (1994).

Constitution of Canada [Online]. (1982). Available: http://canada.justice.gc.ca/Loireg/charte/const_en.html [2001, February 2].

Constitution of Germany [On-line]. (1998). Available: http://www.uni-wuerzburg.de/law/gm00000_.html [2001, January 27].

Constitution of the Republic of Turkey [Online]. (1984). Available: http://mfa.gov.tr/grupa/ac/aca/constitution.htm [2000, October 23].

Council of Europe. (1950). Convention for Protection of Human Rights and Fundamental Freedoms (ETS No. 5). [On-line]. Available: http://www.pfc.org.uk/legal/echrtext.htm [2000, November 21].

Council of Europe. (1981). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108). [On-line]. Available: http://www.coe.fr/engl/legaltxt/108e.htm [2000, November 21].

Council of Europe. (1995). Directive 95/46/EC of the European Parliament and of the Council (ETS No. 281). [On-line]. Available: http://europa.eu.int/ISPO/legal/en/dataprot/compenfr.html [2000, November 21].

Craig, J. D. R. (1997). Invasion of Privacy and Charter Values: The Common- Law Tort Awakens. McGill Law Journal. [On-line Serial], 42(355), 28451 words. Available: http://www.lexis-nexis.com [2000, September 10].

Creamer, J. S. (1980). The Law of Arrest, Search and Seizure. Philadelphia: Holt, Rinehart and Winston, Inc.

Dempsey, J. X. (1997). Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy. Albany Law Journal [On-line Serial], 8, 65, 27533 words. Available: http://www.lexis-nexis.com [2000, September 10].

Diffie, W., & S. Landau. (1998). Privacy on the Line. Cambridge: The MIT Press.

Edwards v. Bardwell, 632 F. Supp. 584 (M. D. La. 1986). [On-line]. Available: http://www.lexis-nexis.com [2001, February 4].

Einbinder, S. D. (2000). Policy Analysis. [On-line]. Available: http://www.uncp.edu/home/marson/348_policy_analysis.html [2001, January 11].

Electronic Frontier Foundation. (2000). U. S. Federal Wiretapping Laws as of Jan. 2000. [On-line]. Available: http://eff.org/pub/Privacy/CALEA/200001_U. S._fed_wiretap_laws.html [2000, Feb 19].

Fairchild, E., & Dammer, H. R. (2001). Comparative Criminal Justice Systems (2nd ed.). Belmont: Wadsworth, Thomson Learning, Inc.

Federal Bureau of Investigation. (1997a). Assistance Capability. [On-line]. Available: http://www.fbi.gov/programs/calea/capablty.htm [2000, March 22].

Federal Bureau of Investigation. (1997b). Capacity. [On-line]. Available: http://www.fbi.gov/programs/calea/capacity.htm [2000, March 22].

Federal Bureau of Investigation. (1997c). Communication Assistance for Law Enforcement Act Implementation Plan. [On-line]. Available: http://www.cdt.org/digi_tele/CALEA_plan.htm [2000, March 22].

Federal Bureau of Investigation. (1997d). Cost Recovery. [On-line]. Available: http://www.fbi.gov/programs/calea/cost.htm [2000, March 22].

Federal Bureau of Investigation. (1997e). Flexible Deployment. [On-line]. Available: http://www.fbi.gov/programs/calea/flexible.htm [2000, March 22].

Federal Bureau of Investigation. (1998). Overview. [On-line]. Available: http://www.fbi.gov/programs/calea/overview.htm [2000, March 22].

Federal Bureau of Investigation. (1999). Press Releases: Ameritech and Nortel Networks to Begin Providing Software to Local Carriers. [On-line]. Available: http://www.fbi.gov/programs/calea/doj990914.htm [2000, March 22].

Federal Bureau of Investigation. (2000a). Press Releases: Justice Department Statement Regarding the FCC's CALEA Standards. [On-line]. Available: http://www.fbi.gov/programs/calea/doj990827.htm [2000, March 22].

Federal Bureau of Investigation. (2000b). Regulatory Issues. [On-line]. Available: http://www.fbi.gov/programs/calea/reglatry.htm [2000, March 22].

Federal Communications Commission. (1998a). FCC Adopts of CALEA Compliance Date. [On-line]. Available: http://www.cdt.org/digi_tele/FCCstatement.html [2000, March 22].

Federal Communications Commission. (1998b). Further Notice of Rulemaking (FCC 98-282). [On-line]. Available: http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc98282.txt [2000, March 14].

Federal Communications Commission. (1998c). Memorandum Opinion and Order (FCC 98-223). [On-line]. Available: http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc98223.txt [2000, March 14].

Federal Communications Commission. (1999a). Report and Order (FCC 99-11). (1999). [On-line]. Available: http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc9911.txt [2000, March 14].

Federal Communications Commission. (1999b). Second Report and Order (FCC 99-229). [On-line]. Available: http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc99229.txt [2000, March 14].

Federal Communications Commission. (1999c). Third Report and Order (FCC 99-230). [On-line]. Available:http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc99230.txt [2000, March 14].

Federal Communications Commission. (2000a). Public Notice: CALEA Section 107 (c) Extension Petitions Receiving Preliminary Extensions from the Common Carrier Bureau. [On-line]. Available: http://www.cdt.org [2001, February 4].

Federal Communications Commission. (2000b). Public Notice: Commission Seeks Comments to Update the Record in the CALEA Technical Capabilities Proceeding. [On-line]. Available: http://www.cdt.org [2001, February 4].

Federal Communications Commission. (2000c). Public Notice: The Common Carrier Cable Services, International and Wireless Telecommunications Bureaus Extend the Deadline for CALEA Section 107 (c) Extension Petitions Until June 23, 2000. [On-line]. Available: http://www.cdt.org [2001, February 4].

Final Notice of Capacity, 63 Fed. Reg. 12218 (1998).

Flaherty, D. (1989). Protecting Privacy in Surveillance Societies. North Carolina: University of North Carolina Press.

Freeh, L. J. (1999). A Report to the American People on the Work of the FBI 1993-1998. [On-line]. Available: http://www.fbi.gov/library/5-year/5-year_rpt.htm [2000, March 22].

Freiwald, S. (1996). Uncertain Privacy: Communication Attributes After the Digital Telephony Act. California Law Review. [On-line Serial], 69, 949, 42182 words. Available: http://www.lexis-nexis.com [2000, December 19].

Gavison, R. (1980). Privacy and the Limits of the Law. Yale Law Journal. [On-line serial]. 89, 448, 6524 words. Available: http://www.lexis-nexis.com [2000, October 10].

Goldstein, S. (1999). Twenty-Eighth Annual Review of Criminal Procedure: Electronic Surveillance. Georgetown Law Journal. [On-line Serial], 87, 1201, 23958 words. Available: http://www.lexis-nexis.com [2000, September 10].

Gordon, P. (1999a). An Overview of Legal Research. [On-line]. Available: http://www.vcsun.org/~djordan/law34s99chp2notes.htm [2000, November 11].

Gordon, P. (1999b). Putting Your Question into Legal Categories. [On-line]. Available: http://www.vcsun.org/~djordan/law34s99chp4notes.htm [2000, November 11].

Gottlieb, D. J., Levy R. E., McAllister, S. R., Peck, J. C., & Yenisey, F. (1997). Comparative Law: Recent Developments in European, American, and Turkish Law: "Team Kansas" Goes to Turkey. Kansas Law Review. [On-line serial], 25, 671, 16499 words. Available: http://www.lexis-nexis.com [2000, November 9].

Gruda, J. (2000). Twenty-Ninth Annual Review of Criminal Procedure. Georgetown Law Journal. [On-line serial], 88, 990, 24625 words. Available: http://www.lexis-nexis.com [2000, November 9].

Gurwitt, R. (1993). Communitarianism: You Can Try It at Home. Governing, 6, 33-39.

H. Rep. No. 103, 103rd Cong., 2nd Sess. 827. (1994). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Hensley, T. R., Smith, C. E., & Bough, J. A. (1997). The Changing Supreme Court: Constitutional Rights and Liberties. St. Paul: West Publishing.

Hong Kong. The Law Reform Commission of Hong Kong. (1996). Consultation Paper: Privacy, Regulating Surveillance and the Interception of Communications. [On-line]. Available: http://info.gov.hk/info/pricon.htm [2000, May 25].

Hull, Andrew R. (1996). The Digital Dilemma: Requiring Private Carrier Assistance to Reach Out and Tap Someone in the Information Age – An Analysis of the Digital Telephony Act. Santa Clara Law Review. [On-line serial], 37, 117, 20994 words. Available: http://www.lexis-nexis.com [2000, October 9].

Initial Notice and Requests for Comments, 60 Fed. Reg. 53643 (1995).

Karacs, I. (1999, July 15). German Phone Taps are Routine. The Independent. [On-line]. Available: http://library.northernlight.com/PG19990716010037174.html?cb=0&sc=0#doc [2000, November 15].

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

Knowlton, D. R. (2000). Congressional Statement of the FBI on Electronic Surveillance. [On-line]. Available: http://www.fbi.gov/pressrm/congress/congress00/knowlton.htm [2000, November 11].

Koppell, T. (Executive Producer). (1992, May 22). Nightline: FBI, Pushing for Enhanced Wiretap Powers. United States: ABC Television Broadcast. [On-line]. Available: http://www.lexis-nexis.com [2000, October 10].

Lusky, L. (1972). Invasion of Privacy: A Clarification of Concepts. Columbia Law Review. [On-line serial] 72, 693, 34278 words. Available: http://www.lexis-nexis.com [2000, October 10].

Majchrzak, A. (1984). Methods for Policy Research. Newbury Park: Sage Publications, Inc.

Marx, Gary T. (1988). Undercover: Police Surveillance in America. Berkeley: University of California Press.

Morley, M. (1993). The Supreme Court and Electronic Surveillance. [On-line]. Available: http://www.tscm.com/SupremeCourt9.html [2000, March 22].

Nagel, S. S., & Neef, M. G. (1977). Legal Policy Analysis. Lexington: D.C. Heath Company.

Nelson, J. (1994). Sledge Hammers and Scalpels: The FBI Wiretap Bill and Its Effect on Free Flow of Information and Privacy. UCLA Law Review. [On-line serial]. 41, 1139, 25423 words. Available: http://www.lexis-nexis.com [2000, October 10].

Notice of Inquiry, 63 Fed. Reg. 70160 (1998).

Notice of Proposed Rulemaking, 63 Fed. Reg. 23231 (1998).

Nylund, J. J. (2000). Fire with Fire: How the FBI Set Technical Standards for the Telecommunications Industry Under CALEA. Commlaw Conspectus. [On-line serial], 8, 329, 17015 words. Available: http://www.lexis-nexis.com [2000, October 9].

Office of Technology Assessment. (1995). Electronic Surveillance in the Digital Age. Washington D. C.: U. S. Government Printing Office.

Olmstead v. United States, 277 U.S. 438 (1928). [On-line]. Available: http://supct.law.cornell.edu/supct/cases/topic.htm [2000, August 8].

Oversight Hearings on the Implementation of the Communications Assistance for Law Enforcement Act of 1994: Testimony before the House Committee on the Judiciary Subcommittee on Crime. 104th Cong., 1st Sess. (1997) (testimony of James X. Dempsey). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Parker, R. B. (1974). A Definition of Privacy. Rutgers Law Review. [On-line serial]. 27, 275, 22874 words. Available: http://www.lexis-nexis.com [2000, October 9].

Patton, C. V. (2001). Steps for a Successful Policy Analysis. [On-line]. Available: http://trochim.human.cornell.edu/tutorial/barrien/barrien.htm [2001, February 20].

Pavesich v. New England Insurance Co. et al., 127 Ga. S. Ct. (1905). [On-line]. Available: http://qsilver/queensu.ca/law/lahey/law122/pavesich.htm [2000, November 21].

Policy Analysis. (2001). [On-line]. Available: http://plsc.uark.edu/book/books/policy/analysis/analysis.htm (2001, February 20).

Rowe, S., Busharis, B., & Kuhlman, L. Legal Research Methods and Organization. [On-line]. Available: http://www/law.fsu.edu/library/write/chap5.html [2000, November 11].

S. Rep. No. 103, 103rd Cong., 2nd Sess. 402. (1994). [On-line]. Available: http://ww.lexis-nexis.com [2000, December 14].

Scanlon, E. (2000). Suggestions for Case Study Methods. [On-line]. Available: http://www.gwbweb.wustl.edu/Users/csd/evaluation/casestudy/caseguide.html (2000, November 11).

Scarisbrick, G. (1996). Introduction to Case Study Method. [On-line]. Available: http://uidaho.edu/ag/agecom391/casestudmeth.html [2000, November 11].

Schuman, D. (1993). Communitarian Search and Seizure. The Responsive Community, Spring, 32-41.

Schwartz, D. A. (1995). Digital Telephony Legislation of 1994: Law Enforcement Hitches a Ride on the Information Superhighway. Criminal Law Bulletin, 31, 195-210.

Scott v. United States, 436 U. S. 128 (1978). [On-line]. Available: http://caselaw.lp.findlaw.com/scripts/getcase.html [2001, February 4].

Second Notice and Requests for Comments, 62 Fed. Reg. 1902 (1997).

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103d Cong., 2d Sess. (1994)

(testimony of Clinton C. Brooks). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103d Cong., 2d Sess. (1994) (testimony of David J. Farber). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103d Cong., 2d Sess. (1994) (testimony of Dorothy E. Denning). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103d Cong., 2d Sess. (1994) (testimony of James K. Kallstrom). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103rd Cong., 2d Sess. (1994) (testimony of Jerry J. Berman). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Security Issues in Computers and Communications: Capitol Hill Hearing Testimony before the Subcommittee on Technology, Environment, and Aviation of the Committee on Science, Space, and Technology. 103d Cong., 2d Sess. (1994) (testimony of Raymond G. Kammer). [On-line]. Available: http://www.lexis-nexis.com [2000, December 14].

Seperich, G. J, Woolverton M. J., Beierlein, J. G.& Hahn D. E. (1996). Introduction to the Case-Study Method. [On-line]. Available: http://www.uidaho.edu/ag/agecon/391/casestudmeth.html [2000, November 12].

Shapo, H. S., Walter, M. R., & Fajans, E. (1989). Writing and Analysis in the Law. New York: The Foundation Press, Inc.

Sheptycki, J. (2000). Surveillance, CCTV and Social Control. Policing and Society, 9, 429-434. Edinburgh: Harwood Academic Publisher.

Smith v. Maryland, 442 U. S. 735 (1979). [On-line]. Available: http://www.lexis-nexis.com [2001, February 4].

South Africa. South African Law Commission. (1998). Discussion Paper 78: Review of Security Legislation. [On-line]. Available: http://cryptome.org/za-esnoop.htm [2000, May 29].

State v. Delaurier. 488 A.2d 688 (S. Ct. R.I. 1985). [On-line]. Available: http://www.lexis-nexis.com [2001, February 4].

Statsky, W. P. (1984). Legislative Analysis and Drafting (2nd ed.). St. Paul: West Publishing Co.

Statsky, W. P., & Wernet, R. J. (1984). Case Analysis and Fundamentals of Legal Writing (2nd ed.). St. Paul: West Publishing Co.

Strossen, N. (1990) Recent U.S. and International Judicial Protection of Individual Rights. Hastings Law Journal. [On-line Serial]. 41, 805, 35973 words. Available: http://www.lexis-nexis.com [2000, November 21].

Teaching Legal Analysis. (2001). [On-line]. Available: http://www.wvu.edu/~law/soweb/10teaching%20legal%20analysis.html [2000, Feb 20].

Terrill, R. J. (1984). World Criminal Justice Systems: A Survey. Cincinnati: Anderson Publishing Co.

Turkey. Ceza Muhakemeleri Usulu Kanunu (1412). (1929). In A. Safak, V. Bicak, & A. S. Safak (Eds.). (pp. 261-341). Guvenlik Kuvvetleri ve Polis Mevzuati. Ankara: Yardimci Ofset.

Turkey. Cikar Amacli Orgutlerle Mucadele Kanunu (4422). (1999). In A. Safak, V. Bicak, & A. S. Safak (Eds.). (pp. 849-851) . Guvenlik Kuvvetleri ve Polis Mevzuati. Ankara: Yardimci Ofset.

Turkey. Turk Ceza Kanunu (765). (1926). In A. Safak, V. Bicak, & A. S. Safak (Eds.). (pp. 137-261). Guvenlik Kuvvetleri ve Polis Mevzuati. Ankara: Yardimci Ofset.

Unal, S. (1999). Turkish Legal System and the Protection of Human Rights. SAM Papers, 3, 99. [On-line]. Available: http://mfa.gov.tr/grupa/ac/aca/acad/hmrghts.htm [2000, October 23].

U. S. Telecom Association, et al. v. Federal Bureau of Investigation, 98 F. Supp. 2010. (D. Ct. D.C. 2000). [Online]. Available: http://www.lexis-nexis.com [2001, February 4].

U. S. Telecom Association, et al., Petitioners v. Federal Communications Commission and U. S. of America, Respondents; Airtouch Communications, Inc., et al., Intervenors. 227 F. 3d 450 (D.C. Ct. App. 2000). [On-line]. Available: http://supct.law.cornell.edu/supct/cases/topic.htm [2001, February 4].

United States v. Donovan et al., 429 U. S. 413 (1977). [On-line]. Available: http://www.lexis-nexis.com [2001, February 4].

United States v. Giordano, 416 U. S. 505 (1974). [On-line]. Available: http://caselaw.lp.findlaw.com/scripts/getcase.html [2001, February 4].

United States v. Kahn, 415 U.S. 143 (1974). [On-line]. Available: http://supct.law.cornell.edu/supct/cases/topic.htm [2000, August 8].

United States v. Knotts, 460 U. S. 266 (1983). [On-line]. Available: http://www.lexis-nexis.com [2001, February 4].

United States v. Ojeda Rios, 495 U. S. 257 (1990). [On-line]. Available: http://caselaw.lp.findlaw.com/scripts/getcase.html [2001, February 4].

United States v. United States District Court, 407 U.S. 297 (1972). [On-line]. Available: http://supct.law.cornell.edu/supct/cases/topic.htm [2000, August 8].

Ward, D. (1996). Sisyphean Circles: The Communication Assistance for Law Enforcement Act. Rutgers Computer and Technology Law Journal. [On-line serial], 22, 267, 15512 words. Available: http://www.lexis-nexis.com [2000, October 9].

Weil, T. K. (1999). Roving Wiretaps: For Your Ears Only. Loyola Law Review. [On-line serial]. 45, 745, 9983 words. Available: http://www.lexis-nexis.com [2000, October 9].

Welsh, W. N., & Harris, P. W. (1999). Criminal Justice Policy and Planning. Cincinnati: Anderson Publishing Co.

Whitebread, C. H.& Slobogin, C. (1993). Criminal Procedure. Westbury: The Foundation Press, Inc.

Wintersheimer, L. A. (1988). Privacy versus Law Enforcement – Can the Two be Reconciled? University of Cincinnati Law Review. [On-line Serial], 57, 315, 17392 words. Available: http://www.lexis-nexis.com [2000, September 10].

Wood, D. D. (1997). The Emergence of Cellular and Cordless Telephones and the Resulting Effect on the Tension Between Privacy and Wiretapping. Gonzaga Law Review. [On-line serial]. 33, 377, 10493 words. Available: http://www.lexis-nexis.com [2000, October 9].

Wren, C. G., & Wren, J. R. (1986). The Legal Research Manual. (2nd ed.). Madison: A-R Editions, Inc.

Yin, R. K. 1984. Case Study Research: Design and Methods. Newbury Park: Sage Publications, Inc.

Yung, A. W. (1996). Regulating the Genie: Effective Wiretaps in the Information Age. Dickinson Law Review. [On-line Serial], 101, 95, 17684 words. Available: http://www.lexis-nexis.com [2000, October 9].