3-1-2003

Technological Advances Leading to the Diminishing of Privacy Rights

Anabelle Maria D'Souza
University of Georgia School of Law

TECHNOLOGICAL ADVANCES LEADING TO THE DIMINISHING OF PRIVACY RIGHTS.

by

ANABELLE MARIA D'SOUZA

(Under the Direction of Robert Brussack)

ABSTRACT

The Purpose of my thesis is to bring about the awareness of the importance of Privacy in our lives. Privacy is an essential element of a free society without which individuals would lose the ability to interact with one another in private. With the advancement in police surveillance technology there is a clash between an individuals right to keep a secret and the State's power to penetrate that secret. State of the art technologies such as the financial crimes enforcement network, wearable computing and surveillance cameras are some of the latest devices invading privacy. These technological advances have become so deep rooted that some of the privacy invasion predicted for the future are alarming. In order to curb privacy invasions we require stricter laws regulating the government's power to interfere with our privacy rights. The shape of our future depends on how we deal with the present issues.

INDEX WORDS: Privacy, Fourth amendment, Search, Seizure, Thermal imaging, Carnivore, Echelon, Surveillance cameras, Wearable computing.

TECHNOLOGICAL ADVANCES LEADING TO THE DIMINISHING OF PRIVACY RIGHTS.

by

ANABELLE MARIA D'SOUZA

LL.B., Government Law College, India, 2000

A Thesis Submitted to the Graduate Faculty of The University Of Georgia in Partial Fulfillment of the Requirements for the Degree

MASTER OF LAWS

ATHENS, GEORGIA

2003

TECHNOLOGICAL ADVANCES LEADING TO THE DIMINISHING OF PRIVACY RIGHTS

by

ANABELLE MARIA D'SOUZA

Major Professor: Robert Brussack

Second Reader: Dan Coenen

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University Of Georgia
May 2003

DEDICATION

To my Parents, my brother Sandeep and sister Preeti.

ACKNOWLEDGEMENTS

I would like to thank Professor Robert Brussack, Professor Dan Coenen and Dean Gabriel Wilner for their guidance and encouragement during the course of my LL.M.

I would also like to thank my parents, Albert and Belinda D'Souza, my brother Sandeep and sister Preeti, for their love, support and encouragement throughout my life. I would not have come this far without you.

TABLE OF CONTENTS

Page

CHAPTER 1

INTRODUCTION

Privacy is a fundamental human right, which is recognized under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and many other international and regional treaties.[1] It embodies the values of human dignity, freedom of association and freedom of speech and has become one of the most important human rights issues of modern time.[2]

Privacy comes from the Latin word "to separate or deprive" referring to the distinction between what belongs to the individual rather than the State.[3] Over the years there have been various definitions of the term "privacy".[4] The array of definitions may be due to the variety of personal matters covered by them.[5] One scholar recognized privacy as a mechanism in three different ways, 'privacy-as-seclusion,' 'privacy-as-information-control' and 'privacy of autonomous personal life.'[6] The term "privacy" can be described as a form of power, which is a powerful tool in the hands of each individual to protect himself against the world.[7] We could ask ourselves the question - who is entitled to this power of privacy? I think every person in the world is entitled to the right

---

[1] David Banisar and Simon Davies, *Global Trends in Privacy Protection: An International Survey of Data Protection, and Surveillance Laws and Developments,* 18 J. Marshall J. Computer & Info. L. 1,1 (1999).
[2] *Id.*
[3] Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look At The Costs Of Privacy And The Benefits Of Information Exchange*, 2000 Stan. Tech. L. Rev.2, 3 (2000).
[4] Carol M. Bast, *What's bugging you? Inconsistencies And Irrationalities Of The law Of Eavesdropping,* 47 DePaul L. Rev. 837, 881 (1998).
[5] *Id.*
[6]William C. Hefferman, *Privacy Rights,* 29 Suffolk U. L. Rev. 737, 746 (1995). Tort law is usually associated with protection for the first two mechanisms of privacy, while constitutional law is associated with protection for privacy of autonomous personal life.

of privacy, be it a person living on the streets or a millionaire living in a mansion. When an individual loses his privacy, he also loses the capacity to distinguish himself from the rest of the world; he will not be able to distinguish himself from others, to maintain an independent life and be a complete and autonomous person.[8] According to Ruth Gavison, privacy comprises of three elements: secrecy, anonymity and solitude.[9] An individual loses his/her privacy "as others obtain information about the individual [loss of secrecy], pay attention to him [loss of anonymity], or gain access to him [loss of solitude]."[10] According to Roger Clark, "Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations."[11]

Drilling down into a deeper level, privacy has several dimensions:

1. Privacy of the person - this is sometimes referred to as "bodily privacy". It is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue and compulsory sterilization;

2. Privacy of personal behavior - This relates to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as "media privacy";

3. Privacy of personal communications - Individuals claim an interest in being able to communicate among them, using various media, without routine monitoring of their

---

[7] Michael Froomkin, *The Metaphor is the Key, Cryptography, The Clipper Chip, And the Constitution,* 143 U. pa. L. Rev. 709, 712 (1995).
[8] *Id.*
[9] Ruth Gavison, *Privacy and the Limits of Law,* 89 Yale L.J. 421, 433 (1980).
[10] *Id* at 428.
[11] Roger Clark, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms, available at* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

communications by other persons or organizations. This includes what is sometimes referred to as "interception privacy" and;

4. Privacy of personal data - Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as "data privacy" and "information privacy".[12]

Privacy is very important today. Ruth Gavison viewed privacy as a concept pertaining to the individual.[13] Privacy embodies the values of a healthy, liberal, democratic, and pluralistic society; individual autonomy; mental health; creativity; and the capacity to form and maintain meaningful relations with others.[14] It provides an individual with the room to grow, a safety valve and respect.[15] An individual can grow in a way that he or she has the ability to develop new ideas, contemplate past experiences and mature.[16] The loss of privacy may be voluntary or involuntary.[17] The loss is voluntary when the individual freely gives up information, anonymity, or solitude.[18] The loss is involuntary when privacy is invaded without the individual's consent.[19] Here the privacy loss is not the responsibility of the individual.[20]

---

[12] *Id.*
[13] *See supra* note 4 at 885.
[14] *Id.*
[15] *Id* at 886.
[16] *Id.*
[17] *Id* at 888.
[18] *Id* at 889.
[19] *Id.*
[20] *Id.* The case of *Commonwealth v. Louden* illustrates the voluntary loss of privacy occasioned by an individual speaking loudly so that a third party could overhear the conversation without any electronic interception device. In this case the Pennsylvania Supreme Court held that "once the conversation, threats and arguments between the Loudens and the screams of the children became audible to the neighbors,

Historically in the United States, the formal recognition of privacy was given in Samuel Warren and Louis Brandeis's article 'The Right to Privacy',[21] in which the authors defined privacy as 'The right to be let alone.'[22] Warren and Brandeis's article on privacy was considered the "most influential law review article of all."[23] Although the law did provide some protection for privacy before Warren and Brandeis wrote their famous article, the protection consisted of limited legal theories whose shortcomings outweighed their usefulness.[24] Rather than protecting individuals through legal doctrine specifically designed to safeguard their privacy interests, nineteenth century American courts and legislatures provided remedies for only a limited number of intrusions and left individuals with incomplete and inadequate protection.[25] The Fourth Amendment of the American Constitution provided for this remedy.[26] The government honored the notion that "a man's house is his castle" and in 1791 added the Fourth Amendment to preserve "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[27] But the Fourth Amendment had its limitations; it only prevented government officials from unlawfully intruding into the home or personal property, leaving private citizens free to invade the

---

through a dividing wall in their home, the Loudens lost whatever expectation of privacy of privacy they had that their secret discussions and conversations would not be overheard." 638 A. 2d 953, 959 (Pa 1994).

[21] 4 Harv. L. Rev. 193 (1890).

[22] *Id* at 195.

[23] Irwin R. Kramer, *The Birth Of Privacy Law: A Century Since Warren and Brandeis*, 39 Cath. U. L. Rev. 703, 703 (1990).

[24] *Id* at 705.

[25] *Id.*

[26] *Id.*

[27] U.S. CONST. amend. IV.

privacy of life at will.[28] In order to remedy those invasions committed by private citizens, the best relief that the courts in the nineteenth century could offer was an action for trespass.[29] But in order to invoke this remedy, the plaintiff had to prove a physical intrusion upon their real property and this severely limited the remedy's usefulness.[30]

In order to rectify the lack of effective legal remedies, the courts occasionally tried to compensate plaintiffs by taking existing legal doctrine to extremes as seen in the case of *Moore v. New York Elevated R.R. Co.*[31] In this case the plaintiff who was a life-tenant of a house brought an action to recover damages alleged to have been suffered by her when the defendant railroad company erected a railroad that overlooked her house.[32] The defendants were held responsible for the loss of privacy suffered by the plaintiff, and the jury found that the passengers and employees interfered with the privacy of the rooms of the plaintiff's house by looking in when standing on the station platform or when coming down the stairs along the building.[33] But the court proceeded on a trespass theory of recovery, and it did not address the damages for the emotional distress occasioned by the loss of privacy. Thus the plaintiff was not fully compensated for privacy invasion.[34]

The lack of legal redress and the increase in the number of privacy invasions over the years led to demands for improved remedies.[35] During the nineteenth century there was a common occurrence of journalistic invasions of the privacy of public figures.[36] In

---

[28] Kramer, *supra* note 23 at 705.
[29] *Id.*
[30] *Id.*
[31] 130 N.Y. 523, 29 N.E. 997 (1892).
[32] *Id* at 526.
[33] *Id* at 528.
[34] Kramer, s*upra* note 23 at 707.
[35] *Id* at 708.
[36] Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. Cal. Interdisciplinary L.J. 295, 312 (1999). With the advent of quick photography and mass-circulation newspapers, the latter part of the century saw the first invasion of privacy lawsuits in the United States.

the present day, battles over privacy reflect historical conflicts.[37] There is always tension between the individual need for privacy and autonomy, and the sense that society suffers when morality goes unregulated.[38]

Over the years the Supreme Court has developed a limited right to privacy in a string of cases: Griswold v. Connecticut,[39] Roe v. Wade,[40] Whalen v. Roe[41] and Bowers v. Hardwick.[42]

[37] *Id* at 313.
[38] *Id.*
[39] 381U.S. 479 (1965). In this case the Appellant was a licensed physician and a professor at the Yale Medical School. He gave information, instruction, and medical advice to married persons as to the means of preventing conception. The wife was examined and prescribed the best contraceptive device or material for her use. Sections 53—32 of the general statutes of Connecticut law provide that: 'Any person who uses any drug, medicinal article or instrument for the purpose of preventing conception shall be fined not less than fifty dollars or imprisoned not less than sixty days nor more than one year or be both fined and imprisoned.' The Supreme Court held that the Connecticut law forbidding use of contraceptives unconstitutionally intrudes upon the right of marital privacy.
[40] 410 U.S. 113 (1973). In this case, a pregnant single woman (Roe) brought a class action challenging the constitutionality of the Texas criminal abortion laws, which proscribe procuring or attempting an abortion except on medical advice for the purpose of saving the mother's life. The District Courts judgement was affirmed by the Supreme Court of Texas and held that the abortion statutes were void as vague and over broadly infringing the plaintiffs' Ninth and Fourteenth Amendment rights.
[41] 429 U.S. 589 (1977). Physicians and patients brought an action challenging the constitutionality of New York statutes which required that the state be provided with a copy of every prescription for certain drugs and which also provided security measures for that information in the state's possession. The Supreme Court held that the statutes were a reasonable exercise of the state's broad police power; that finding that the state had not shown necessity for the requirement was insufficient basis for holding the statutes unconstitutional.
[42] 478 U.S. 186 (1986). A Practicing homosexual brought action challenging constitutionality of Georgia sodomy statute. The Supreme Court held that Georgia's sodomy statute did not violate the fundamental rights of homosexuals.

CHAPTER 2

REASONABLE EXPECTATION OF PRIVACY

A. An Analysis of the Fourth Amendment

The Fourth Amendment[43] is an expression of an "eloquent, unequivocal principle of a democratic government."[44] The framers of the constitution intended the Fourth Amendment to protect the citizens against indiscriminate and arbitrary general authority, which had been asserted by the British against the American colonies.[45] The purpose of the Fourth Amendment was to protect the citizens against unwarranted intrusions, but was not intended as a general restraint against all police practices.[46] The modern development of the Fourth Amendment can be best summarized in the article "The Right to Privacy", in which Warren and Brandies clearly stated that "[T]he individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[47] The concept of "reasonable expectations of privacy"[48] is at the forefront of all Fourth Amendment analysis.[49] It is the starting point for any defendant

---

[43] *supra* note 27.
[44] Gerald K. Freund, *Look Up In The Sky, It's a Bird, It'd a Plane...It's Reasonableness,* 20 Sw. U.L. Rev.195, 198 (1991).
[45] *Id.*
[46] *Id.*
[47] *supra* note 21 at 193.
[48] Black's Law Dictionary defines "reasonable" as: Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view. Having the faculty of reason; rational; governed by reason; under the influence of reason; agreeable to reason. Thinking, speaking, or acting according to the dictates of reason. Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable. BLACK'S LAW DICTIONARY 1138 (5th ed. 1979).
[49] Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, And The Concept Of The Fourth Amendment Standing,* 27 U. Mem. L. Rev. 907, 908 (1997).

seeking to suppress evidence obtained in violation of the Fourth Amendment.[50] If a defendant does not have a reasonable expectation of privacy in an area searched or an item seized, he does not suffer a Fourth Amendment violation.[51] "The Fourth Amendment reflects the framers of the Constitution's determination that individuals in a democratic society be able to dwell in reasonable security and freedom from government intrusions."[52] The case of *Boyd v. United States*[53] which was decided a century after the passage of the Bill of Rights, was the first significant Supreme Court decision involving the Fourth Amendment as well as the Fifth Amendment privilege against self-incrimination.[54] It recognized that the Fourth Amendment "was to apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[55] In the absence of a search or seizure, however, the Fourth Amendment is not implicated by police action.[56] For nearly fifty years, beginning in 1928 with *Olmstead v. United States*,[57] the U.S. Supreme Court premised the existence of a search on whether a physical trespass had occurred under the local property law.[58] In this case, the petitioners were convicted in the District Court for the Western District of Washington of a conspiracy to violate the National Prohibition Act (27 USCA) by

---

[50] *Id.*
[51] *Id.*
[52] Melvin Gutterman, *A Formulation Of The Value and Means Models Of The Fourth Amendment In The Age Of Technologically Enhanced Surveillance*, 39 Syracuse L. Rev. 647, 649 (1988).
[53] 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746, 3 A.F.T.R. 2488 U.S.N.Y, (1886). In this case Justice Bradley decided that "it does not require actual entry upon premises and search for and seizure of papers to constitute an unreasonable search and seizure within the meaning of the fourth amendment; a compulsory production of a party's private books and papers, to be used against himself or his property in a criminal or penal proceeding, or for a forfeiture, is within the spirit and meaning of the amendment."
[54] Gutterman, s*upra* Note 51 at 651.
[55] *Id.*
[56] Richard S. Julie, *High-Tech surveillance Tools And The Fourth Amendment: Reasonable Expectations of Privacy In The Technological Age*, 37 Am. Crim. L. Rev. 127, 128 (2000).
[57] 277 U.S. 438, 48 S.Ct. 564 (1928).
[58] Julie, s*upra* note 56.

unlawfully possessing, transporting and importing intoxicating liquors.[59] The information, which lead to the discovery of the conspiracy and its nature and extent, was largely obtained by intercepting messages on the telephones of the conspirators by the federal prohibition officers.[60] Small wires were inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office.[61] The insertions were made without trespass upon any property of the defendants.[62] The federal officers at the wires heard the orders given for liquor by customers and the acceptances; they became auditors of the conversations between the partners.[63] All this disclosed the conspiracy charged in the indictment, and many of the intercepted conversations were not merely reports, but parts of criminal acts.[64] The Supreme Court of the United States held that the wiretapping committed by the federal prohibition officers did not amount to a search or seizure within the meaning of the Fourth Amendment.[65] The Court in the case of Olmstead, held that the only interest protected by the Fourth Amendment were those in tangible objects, such as papers, houses, and other physical possessions, and that those possessions were protected only against physical invasions.[66] Overheard conversations and other types of communicative evidence, therefore, had no specific protection, unless obtained in the violation of local property law.[67] When does a person have a reasonable expectation of privacy under the Fourth Amendment? The court in Olmstead read the Fourth Amendment in the literal

[59] *supra* note 57 at 456.
[60] *Id* at 456, 457.
[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] *Id*.
[65] *Id* at 468.
[66] Julie, *supra* note 56 at 129.
[67] *Id*.

sense as to include “persons”, “houses”, “papers” and “effects”.[68] Even literally construed, these material things that were afforded protection by the text of the Fourth Amendment did not include public telephone wires or the messages they transmitted.[69] Thus there was no deterrent to prevent the government agents from using electric devices to listen to private phone conversations.[70] But the case of *Katz v. United States*[71] changed all that. In this case, the agents of the Federal Bureau of Investigation had placed an “electronic listening and recording device” outside the phone booth that Charles Katz was using to place a bet with his bookie.[72] At trial, the District Court for the Southern District of California permitted the government, over the petitioner’s objections, to introduce evidence of the petitioner’s end of the conversations and Charles was convicted.[73] The Court of Appeals affirmed the conviction and rejected the contention that the recordings were obtained in violation of the Forth Amendment because “[T]here was no physical entrance into the area occupied by the petitioner.”[74]

According to Charles the Fourth Amendment provided a substantive right that his conversation with his bookie over the pay phone, inside the glass booth, would remain

---

[68] Jones, *supra* note 49 at 912.
[69] *Id.*
[70] *Id.*
[71] 389 U.S. 347 (1967).
[72] *Id* at 349.
[73] *Id* at 348.
[74] *Id.* 18 U.S.C. s 1084. The Statute provides in pertinent part:
'(a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined no more than $10,000 or imprisoned not more than two years, or both.’
'(b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State where betting on that sporting event or contest is legal into a State in which such betting is legal.'

private.[75] The government argued that Charles had no reasonable expectation of privacy because the agents had not physically entered the phone booth; the phone booth was open to all members of the public; and the glass made the activity inside the booth visible to the public.[76] The government stressed on the fact that the telephone booth from which Charles made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside.[77] But when Charles entered the telephone booth to make the call, what he sought to exclude was not an intruding eye but an uninvited ear.[78]

The U.S. Supreme Court ruled in favor of Charles, stating: "The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office is not subject to Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[79] The court recognized that the proscriptions of the Fourth Amendment were no longer limited to tangible things.[80] Katz now represents the "new" way of thinking about the Fourth Amendment and how it protects individuals.[81] It has now allowed the court to adopt a broad construction that allows the amendment to adapt to the changing needs of society.[82]

---

[75] *supra* note 71 at 349.
[76] *Id* at 348-354.
[77] *Id* at 351.
[78] *Id.*
[79] Jones, *supra* note 49 at 913.
[80] *Id* at 914.
[81] *Id.*
[82] *Id.*

B. Objective versus Subjective Expectation of Privacy

The Katz standard had revolutionized the court's Fourth Amendment analysis.[83] After the Katz decision there have been various judicial decisions on cases where the Courts have demarcated whether a person can anticipate a subjective or an objective expectation of privacy.[84] In *United States v. Chadwick*[85] the Supreme Court recognized that a person has an expectation of privacy in a package or a container, and the Fourth Amendment protects this privacy interest.[86] In particular the court considered whether an individual's expectation of privacy in a footlocker taken from the trunk of a car violated a reasonable expectation of privacy.[87] A subjective expectation of privacy consists of a belief that uninvited people will not intrude in a particular area, i.e., that "one may freely admit guests of one's choosing…without sacrificing one's right to expect that a space will remain secure against all others."[88] As the court stated in *United States v. Gerena,*[89] "[A] defendant must demonstrate that his or her professed subjective expectation of privacy viewed from the totality of the circumstances, is at least of a quality similar in significant respects, to the privacy expectations one would ordinarily expect an individual to have with regard to his or her home or office."[90] If a person took precautions to

[83] Madeline A. Herdrich, *California v. Greenwood: The Thrashing Of Privacy,* 38 Am. U. L. Rev. 993, 1001 (1989).
[84] *Id* at 1001.
[85] 433 U.S. 1, 97 S.Ct. 2476 (1977). The FBI agents opened the footlocker of the respondents without the respondents' consent or a search warrant and found large amounts of marijuana in it. The Supreme Court of the United States affirmed the decision of the Court of Appeals stating that the search was conducted more than an hour after federal agents had gained exclusive control of the footlocker and long after respondents were securely in custody; therefore the search could not be viewed as incidental to the arrest or as justified by any other exigency. The Respondents were entitled to the protection of the Warrant Clause and their privacy interests in the contents of the footlocker were not eliminated simply because they were under arrest.
[86] Herdrich, s*upra* note 83 at 1002.
[87] *Id.*
[88] Freund, s*upra* note 44 at 201.
[89] 662 F.Supp.1218,1218 (D.Conn. 1987).
[90] *Id* at 1237.

exclude others, this would heighten any legitimate expectation of privacy.[91] However a question will arise, when a person is trying to prevent one type of intrusion, whether the person is trying to prevent all types of intrusions.[92] This kind of determination is a question of fact for the courts.[93] A Person's actions can be used to overcome a claim that a subjective expectation of privacy existed.[94] Therefore searches conducted with the consent of the individual are exempt from the requirements of the Fourth Amendment.[95] Implied consent can be reasonably used but then strict standards would apply.[96] Hence, a person calling for help would not diminish his or her expectation of privacy, but voluntary abandonment of property would destroy any expectation of privacy.[97] If a person wants to retain his privacy interest there has to be no abandonment.[98] A person also looses his privacy when he shares information or shares the same areas with another person.[99] But as seen in the Katz decision,[100] a person will have a reasonable expectation of privacy even in areas open to the public as long as it is his intention to keep his privacy in public.[101] At the same time a person cannot maintain an expectation of privacy in an area, which is shared by others.[102] Providing property to an unknown person can completely destroy a person's subjective expectation of privacy.[103]

---

[91] Freund, s*upra* note 44 at 202.
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *supra* footnote 71.
[101] *Id.*
[102] United States v. Anderson 8598 F.2d 1171, 1177 (1988) (the trunk of the car which is shared by another).
[103] Rawlings v. Kentucky 448 U.S. 98, 106 (1980).

Unlike the subjective expectation of privacy, all objective expectations of privacy are a matter of law rather than fact.[104] The legitimacy of a person's claim to privacy is determined "in light of all the surrounding circumstances,"[105] or as the court in *United States v. Baron-Mantilla* phrased it, by "the totality of the circumstances."[106] Hence, a determination whether a search is reasonable requires an examination of the incident and the final determination of reasonableness requires balancing, on one hand, an individual's legitimate expectation of privacy, and on the other hand, the government's need for effective law enforcement.[107] In addressing this objective prong, in *Smith v. Maryland,*[108] the court considered whether the government's use of a telephone company's pen register to record telephone numbers from a suspect's home was an intrusion of his privacy.[109] The telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home.[110] The petitioner moved to suppress all information derived from the pen register.[111] The Maryland trial court denied this motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment.[112] The petitioner was convicted, and the Maryland

---

[104] Freund, *supra* note 44 at 203.
[105] Rakas v. Illinois, 43 U.S. 128, 152 (1978). In this case the petitioners were in a suspected getaway car, which was stopped by the police. Upon searching the car, the police found a box of rifle shells in the glove compartment and a sawed off rifle under the front passenger seat. The petitioners were arrested. Before trial, the petitioners moved to suppress the rifle and the shells on fourth amendments grounds, but the trial court denied the motion on the ground that the petitioners lacked standing to object to the lawfulness of the search of the car because they concededly did not own either the car or the rifle and shells. The Illinois Appellate Court and the US Supreme Court affirmed. Justice Rehnquist of Supreme Court, held that 'petitioners, who asserted neither a property nor a possessory interest in the automobile searched nor an interest in the property seized, and who failed to show that they had any legitimate expectation of privacy in the glove compartment or area under the seat of the vehicle in which they were merely passengers, were not entitled to challenge the search of those areas.'
[106] 743 F.2d 868,870 (1984).
[107] Freund, *supra* note 44 at 204.
[108] 442 U.S. 735 (1979).
[109] Herdrich, *supra* note 83 at 1004.
[110] *supra* note 108 at 735.
[111] *Id.*
[112] *Id.*

Court of Appeals affirmed.[113] In the case of *California v. Ciraolo,*[114] officers of the Santa Clara police who were trained in marijuana identification secured a private airplane, flew over respondent's house at an altitude of 1,000 feet, and readily identified marijuana plants growing in the yard.[115] A search warrant was later obtained on the basis of a photograph taken from the plane of the surrounding area, the warrant was executed and the marijuana plants were seized.[116] The California trial court denied respondent's motion to suppress the evidence of the search, and the California Court of Appeal reversed on the ground that the warrantless aerial observation of respondent's yard violated the Fourth Amendment.[117] But the Supreme Court reversed the order of the Court of Appeals and held that the warrantless aerial observation of a fenced-in backyard within the curtilage of a home was not unreasonable under the Fourth Amendment.[118]

C. Concept of Seizure

A person is said to have been "seized" within the meaning of the Fourth Amendment anytime when an officer conveys to that individual that he is no longer free "to walk away" or " to ignore the police presence and go about his business."[119] A person does not have to be handcuffed and taken to the police station in order to have been seized.[120] The police authority can affect a seizure by applying physical force or by a show of authority.[121] In *Michigan v. Chesternut*, the defendant argued that he was

[113] *Id.*
[114] 476 U.S. 207 (1986).
[115] *Id* at 207.
[116] *Id.*
[117] *Id.*
[118] *Id* at 215.
[119] Jones, *supra* note 49 at 927.
[120] *Id.*
[121] *Id.*

unlawfully seized during police pursuit.[122] Four police officers riding in a marked police cruiser were engaged in routine patrol duties in metropolitan Detroit.[123] The defendant was standing on the curb.[124] The defendant noticed the police car and started running away.[125] The officers followed the defendant in the patrol car, caught up with him and drove alongside him for a short distance.[126] As they drove beside him, the officers observed respondent discard a number of packets he pulled from his right-hand pocket.[127] An officer got out of the cruiser to examine the packets.[128] He discovered that they contained pills.[129] When the officer was engaged in the inspection, the respondent who was running a few paces ahead stopped.[130] Surmising on the basis of his experience as a paramedic that the pills contained cocaine, the officer arrested the respondent for the possession of narcotics and took him to the station house.[131] During an ensuing search, the police discovered in the respondent's hatband another packet of pills, a packet containing heroin, and a hypodermic needle.[132] The Respondent was charged with knowingly and intentionally possessing heroin, tablets containing codeine, and tablets containing diazepam, in violation of Mich.Comp.Laws § 333.7403(2) (1980).[133] Justice Blackmun of the Supreme Court held that "no seizure of defendant occurred when police officers in an automobile observed, the defendant upon seeing the automobile, started to run, and officers accelerated to catch up to defendant and then drove alongside him

[122] 486 U.S. 567 (1988).
[123] *Id* at 567.
[124] *Id*.
[125] *Id*.
[126] *Id*.
[127] *Id*.
[128] *Id*.
[129] *Id*.
[130] *Id*.
[131] *Id*.
[132] *Id*.
[133] *Id*.

before he discarded a pack of pills, which the officers then seized."[134] The Court disagreed with the defendant finding that no Fourth Amendment "seizure" occurred by the officers' conduct preceding the physical custody because a reasonable person would not have felt compelled to stop.[135]

In the case of *California v. Hodari*,[136] the defendant fled at the approach of an unmarked police car.[137] The police gave chase and when the policeman was about to tackle the defendant, the defendant tossed away a small rock of crack cocaine.[138] The main issue in this case was whether, the defendant was seized within the meaning of the Fourth Amendment.[139] The exact moment of the seizure had to be determined.[140] If the seizure occurred when the defendant was tackled, the abandoned drugs would be admissible.[141] If the seizure occurred by the show of authority in chasing the suspect while wearing police jackets, then the evidence would be inadmissible.[142] In order for "seizure" to have occurred, there must either be some application of physical force, even if extremely slight, or a show of authority to which the subject yields; a show of authority, without any application of physical force, to which the subject does not yield is not a seizure.[143] In this case, there was no application of physical force by the police.[144] The defendant did not stop at the show of authority constituted by the chase of the police

---

[134] *Id* at 572.
[135] *Id*.
[136] 499 U.S. 621 (1991).
[137] *Id* at 621.
[138] *Id*.
[139] *Id*.
[140] Jones, *supra* note 49 at 929.
[141] *Id*.
[142] *Id*.
[143] U.S.C.A. Const. Amend. 4.
[144] Jones, *supra* note 49 at 930.

and was therefore not "seized" when tackled.[145] The Court held that the cocaine abandoned while the defendant was running was not the fruit of a seizure.[146]

In situations involving a police chase, a two part inquiry must be satisfied: (1) Was there a display of authority, or application of physical force, sufficient to convey to a reasonable person that he is no longer free to leave, and (2) Did the show of authority and/or application of physical force actually produce a stop?[147] The protections of the Fourth Amendment apply when both questions are confirmed in the affirmative.[148]

D. Concept of a Search

The concept of a search is also grounded in the determination of " reasonable expectation of privacy."[149] However, unlike the "seizure" cases, discussions of reasonable expectations of privacy are most often found in cases dealing with searches.[150] Search activity carries a lot more potentiality for the invasion of a person's privacy expectations

[145] *Id.*
[146] *Id*. Also see Hughes v. State. 588 S.W. 2d 296 (1979) In this case the police officer smelled the odor of marijuana coming out from the vehicle when the respondent Hughes lowered his window. The police took the respondent and put him in the back of a police vehicle. The Tennessee Supreme Court held that even though the respondent was assured by the police that he was not under arrest, a reasonable person would not feel free to leave after being asked to step outside a store, to produce a driver's license, and "invited" to sit in the back of a patrol car which could not be opened from the inside. The Court held that the officer's approach to the vehicle and his request to roll down the window constituted a seizure within the meaning of the fourth amendment. The determination of whether a person has been "seized" depends entirely upon the particular facts of each independent case. Sometimes a person's freedom to walk away is not so easily determined. For example, a seizure is not likely to have occurred when uniformed police officers board a bus stopped at Fort Lauderdale on its way from Miami to Atlanta, and ask a passenger for his bus ticket and license, and if they explain that they are narcotics officers and request consent to search his luggage. Similarly there would be no seizure of the workers in a factory when armed, badge-carrying INS agents stand at the exits and roam around the factory asking citizenship questions. Nor does a seizure occur when an officer approaches a group of people, asks for identification, calls a police dispatcher to see if one of the individuals is wanted for questioning, and, upon finding the suspect is wanted, asks if he will stay and wait for the other detective to arrive.
[147] Jones, s*upra* note 49 at 930.
[148] *Id.*
[149] Jones, s*upra* note 49 at 935.
[150] *Id.*

than does a seizure.[151] An individual whose reasonable expectation of privacy has not been violated has not, by definition, been subjected to a Fourth Amendment "search" or "seizure".[152] Therefore in order to determine whether a Fourth Amendment "search" has occurred, the Court must determine whether the accused's reasonable expectation of privacy has been violated.[153] As a general rule, "looking at what is already exposed to view" is not considered a "search".[154] Asking the question whether the item was in the plain view when observed leads to the question whether the Fourth Amendment applies to all.[155] In the case of *Florida v. Riley*[156] the Florida Supreme Court stated that "[T]he police may see what may be seen from a public vantage point where (they have) a right to be. Once the police are lawfully in a position to observe an item firsthand, the owner's privacy interest in that item is lost. The owner can retain the title and possession of that item but not its privacy."[157] The issue would, however, become more complex if the police observation goes to such an extreme that it would be questionable as to whether it is reasonable to assume that any member of the public would ever make an observation despite the fact that the public could legally make the same.[158]

---

[151] *Id*. *See* Segura v. United States, 468 U.S. 796,806 (1984); United States v. Chadwick, 433 U.S. 1, 13-14 (1977). The greatest potential for violating a privacy expectation exists in bodily intrusions.

[152] *Id.* However, an infringement of a reasonable expectation of privacy means only the Fourth Amendment has come into the picture. It is not a determination that the Fourth Amendment has been violated. In order to make that determination, the Court must determine whether the search or seizure was "reasonable" under the Fourth Amendments standards. *See* Jones, s*upra* note 49 FN 102.

[153] *Id.*

[154] Arizona v. Hicks, 480 U.S. 321, 328 (1987). This rule is based upon the 'plain view doctrine'. The meaning of both the phrases is the same, but the doctrine of 'plain view' is technically different from the reasonable expectation privacy analysis. Also see Texas v. Brown, 460 U.S. 730, 738 (1983). The plain view doctrine is an exception to the warrant requirement. It allows the police to seize any item without a warrant if the police officer can see the object in plain view from a position, which he can legally occupy, and the evidentiary value of the item in proving a crime is immediately present.

[155] Jones, s*upra* note 49 at 936.

[156] 488 U.S. 445, 449 (1989).

[157] *Id.*

[158] Jones, s*upra* note 49 at 937.

In the case of *California v. Ciraolo*[159], for example the Court held that the police officers' warrantless aerial observation, from an altitude of 1,000 feet, during which the plants were readily visible to the naked eye, did not violate homeowner's Fourth Amendment rights.[160] Since airplanes routinely fly at such high altitudes in general, any member of the public flying at that altitude could have observed the defendant's backyard.[161] But in this case the question would arise whether the public would ever make such an observation of the defendant's backyard.

The police have a right to be in any place where the public may go.[162] In the case of *Florida v. Riley,*[163] the Court made the observation that "if a police officer can observe anything in a person's home while in a position where any member of the public can make the same observation, then the object which is seen by the officer is said to be clearly visible or has been knowingly exposed to the public."[164] In this case the defendant did not have any reasonable expectation of privacy from aerial surveillance. "[A]ny member of the pubic could have legally been flying over Riley's property in a helicopter at an altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more….[W]e would have a different case if flying at that altitude had been contrary to law or regulation."[165]

---

[159] s*upra,* note 113.
[160] *Id* at 207.
[161] *Id.*
[162] Jones, *supra* note 49 at 938.
[163] 488 U.S. 445 (1989).
[164] *Id* at 451.
[165] *Id.* Also see State v. Bowling. 867 S.W.2d 338 (1993). In this case the police officers arrived at the defendants house on the suspicion that the defendant was involved in a hit and run accident, which resulted in the death of the victim. When the officers did not receive any response after knocking on the door, they looked into the window of the garage and saw the defendant's car, which was the suspected vehicle, the officer went down on his hands and knees and observed that the hood of the car was damaged. It is apparent that the defendant did not knowingly expose the truck to the public. His truck was behind a solid, completely closed garage door. While the only other garage door was open, it had been raised a mere one and a half feet to allegedly enable the dog to come and go from the garage. Therefore, the defendant clearly

While a person does not have a reasonable expectation of privacy from another's view if the object is exposed to the public, the opposite is also true: one does have a reasonable expectation of privacy if the item or area is not exposed to another's view.[166] Consequently, if an object has to be moved in order to view evidence, the evidence is not exposed and there is a reasonable expectation of privacy.[167] In the case of *Arizona v. Hicks,*[168] the police officers had entered the respondent's apartment to find the person who fired a bullet through the floor of the apartment.[169] The respondent had fired a bullet through the floor, which had injured a man on the floor below.[170] While the policemen were in the apartment they noticed two sets of expensive stereo components and, suspecting that they were stolen, read and recorded their serial numbers.[171] They moved some of the equipment, including a turntable, to do so and phoned in the numbers to headquarters.[172] Upon learning that the turntable had been taken in an armed robbery, the officer seized it immediately.[173] The Supreme Court had to determine whether the act of moving the property to view the serial number was a "search" activity within the Fourth Amendment.[174] The court held that a reasonable expectation of privacy had been infringed by a "search".[175] By touching the property and moving it, the police officer "exposed to view concealed portions of the apartment and its contents."[176] As such, the court did not take into consideration that the officer was only looking for a non-private

---

manifested a subjective expectation of privacy. The Court held that that the officer's actions constituted a warrantless search, which violated the personal and societal values, protected by the Fourth Amendment.
[166] Jones, s*upra* note 49 at 941.
[167] *Id.*
[168] 480 U.S. 321 (1987).
[169] *Id* at 321.
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] Jones, s*upra* note 49 at 942.
[175] *Id.*

serial number on the property and nothing else was revealed by his actions.[177] What mattered to the court was that the officer's act exposed an area to the officer's senses that would otherwise have not been exposed.[178] The Court stated: "It matters not that the search uncovered nothing of any great personal value….A search is a search, even if it happens to disclose nothing but the bottom of a turntable."[179]

[176] *Id*.
[177] *Id*.
[178] *Id*.
[179] s*upra* note 167 at 325.

CHAPTER 3

ADVANCEMENT IN THE FIELD OF POLICE TECHNOLOGY

One hundred years ago, Brandeis and Warren had the foresight to state: "The intensity and complexity of life…have rendered necessary some retreat from the world, and man…has become more sensitive…so that solitude and privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[180] Since that time, the advancement in the field of technology and the increasing complexities of society have posed serious questions about rightful intrusions of the government on the privacy of citizens.[181]

Information technology, communications and computer technology are characterized by dramatic innovations.[182] Automated teller machines, computerized reservation systems, full text databases and a myriad of other developments represent great advances in convenience and human capabilities.[183] With the recent developments in police surveillance technology there is a clash between an individual's right to keep a secret and the state's power to penetrate that secret.[184] Modern technology has advanced to such an extent that the cases dealing with the impact of this technology have become very diverse and complex.[185] The court has been faced with the issues of arising out of the use of, among other things, aircraft, medical technologies, electronic listening devices

---

[180] Brandeis & Warren, s*upra* note 21 at 196.
[181] *Id.*
[182] Steven A. Bercu, *Towards Universal Surveillance In An Information Age Economy: Can Police Handle Treasury's New Police Technology?,* 34 Jurimetrics J. 383, 383, 384 (1994).
[183] *Id.*
[184] Froomkin, *supra* note 7 at 712.
[185] Brandeis & Warren, s*upra* note 21 at 209.

and devices which provide for visual enhancement.[186] Generally technology provides police with a vantage point that most individuals cannot share.[187] Since police observation often depends on the use of expensive and sophisticated machinery, the ability to intrude is often unexpected.[188]

Advances in the field of information technology are rendering obsolete traditional processes and frameworks for the regulation of law enforcement surveillance methods.[189] As of today, surveillance is no longer limited by darkness, whispers or distance.[190] As criminals have grown more sophisticated, criminal investigators have resorted to state-of-the-art technologies in order to curb criminal activity.[191]

Below is a description of some of the latest police technologies, which have given rise to some serious privacy concerns.

A. The Financial Crimes Enforcement Network

First conceived in 1981, the Financial Crimes Enforcement Network (FinCEN) got official life in 1990.[192] The mission of FinCEN is to support law enforcement investigative efforts and promote interagency and global cooperation against domestic and international financial crimes and to provide the United States policy makers with strategic analyses of domestic and worldwide trends and patterns.[193] FinCEN works toward those ends through information collection, analysis and sharing, as well as

[186] *Id*.
[187] *Id* at 208.
[188] *Id*.
[189] Bercu, s*upra* note 181 at 383.
[190] *Id* at 384.
[191] *Id*.
[192] Bercu, s*upra* note 181 at 389.
[193] Financial Crimes Enforcement Network. *available at* http://www.ustreas.gov/fincen/af_mission.html.

technological assistance and innovative, cost-effective implementation of the Bank Secrecy Act and other Treasury authorities.[194]

FinCen's main mission is (1) to gather financial and related records and data from federal, state, local and foreign agencies (2) to analyze collected records for evidence of money laundering and other financial crimes and (3) to disseminate its findings to law enforcement agencies in the United States and abroad.[195] FinCen is a unique kind of enforcement tool.[196] It is a hybrid between a database and a focused surveillance tool and combines qualities of many surveillance technologies.[197] It embodies the qualities of a tracking device, pen register, a bloodhound, a hidden camera, wiretap, a high powered telescope or even a parabolic microphone. It can be used to observe individuals without even alerting them of its presence of surveillance.[198] FinCEN is not like any common law enforcement technology; it has a certain measure of intelligence.[199] The FinCEN's database is linked via computer networks to computers at other agencies, which comb through a vast amount of data routinely by way of vigilant software.[200] It is like a human detective; the case based expert system conducts a focused inquiry, seeking leads, hunting traces of illicit behavior, combining related pieces of information, and attempting to connect individual suspects to a pattern of suspected criminal activity.[201]

Why would FinCEN cause a threat to privacy? When records of our everyday transactions are stored in massive databases and periodically searched for unspecified

---

[194] *Id.*
[195] Organization, Functions and Authority Delegation, 55 Fed. Reg. 18,433 (1990).; Matthew N. Kleiman, *The Right to Financial Privacy versus Computerized Law enforcement: A New Fight in an Old Battle*, 86 NW. U.L. Rev. 1169, 1190-91 (1992); Bercu, *supra* note 181 at 388.
[196] Bercu, *supra* note 181 at 397.
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *Id.*

patterns thought to signal illicit activity, individuals are constrained in their thoughts, choices and acts.[202] We should have the right to enlarge our conception of the personal domain to not only include our body, but also a certain amount of breathing space around our body.[203] Every individual has the right to make his own choices and decisions and decide what personal information to disclose to others and what to conceal. FinCEN threatens privacy by revealing a broad range of personal information never disclosed in any meaningful sense by its subjects.[204] Continuous data base surveillance by an expert-system computer network has a chilling effect on legitimate activity.[205] By contracting the sphere of autonomy, it threatens to "deprive us of that liberty on which our humanity fundamentally rests."[206]

B. Global Positioning System.

To know one's location and how to navigate to particular places are concerns that have affected generations for years.[207] Since the 1950s, a number of positioning technologies have been developed.[208] These include two very popular marine navigation systems based on transmission of radio signals: OMEGA and Loran-C.[209] The primary disadvantages of these systems were lack of precision, global coverage, and inaccuracy in areas of rugged terrain.[210] During the 1980's, the first Global Positioning System (GPS)

---

[201] *Id* at 398.
[202] *Id* at 401.
[203] Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?,* 58 Notre Dame L. Rev. 445, 453 (1983).
[204] Bercu, s*upra* note 181 at 401.
[205] *Id*.
[206] *Id* at 402.
[207] Robert Puterski, *The Global Positioning System—Just Another Tool?,* 6 N.Y.U. Envtl. L.J.93, 94 (1997).
[208] *Id* at 94.
[209] *Id.*
[210] *Id*.

signals became available for use by non-military researchers.[211] The cost of equipment was very high and it was assumed that civilian uses requiring high precision would be limited to geodesy and civil engineering.[212] As low-grade field units for the military became physically smaller and less expensive, the manufacturers of receivers began to look at other potential markets.[213] At the same time, the rapidly expanding geographic information systems (GIS) profession developed needs for inexpensive and rapid methods of capturing high quality spatial information.[214] With the full development of the GPS constellation of satellites in 1993, a new tool for general use arrived.[215] GPS receivers are now another $200 electric commodity, which is often found in the sporting goods section of a local department store.[216] GPS is based on satellite ranging.[217] If a person knows the location of the satellite, he will be able to derive another location by using basic trigonometry.[218] In order to determine a person's position accurately, one must know the exact location of several satellites.[219] A receiver needs four satellites to pinpoint any spot on the globe, one for each of the variables, i.e., longitude, latitude, elevation and time.[220] GPS is a huge success as the satellite clocks are so accurate that a location can be determined within centimeters.[221] The Global Positioning System allows a person (as well as others) to know where they are at all times.[222] If you go to an unfamiliar city and rent a car which has a Global Positioning System (GPS) installed in it,

---

[211] *Id* at 93.
[212] *Id*.
[213] *Id*.
[214] *Id*.
[215] *Id*.
[216] *Id*.
[217] *Id* at 95.
[218] *Id*.
[219] *Id*.
[220] *Id*.
[221] *Id*.

you can program your destination into the dashboard-mounted computer and listen to the computer generated voice which will help you make all the proper turns to get to your destination.[223] What happens is that there are a series of satellites that send signals to help the onboard computer determine the position of the car, and the computer coordinates the signals with a mapping program, which gives the accurate driving instructions.[224] This is a unique form of an Intelligent Transportation System (ITS), which serves as a personal navigation assistance device.[225] Along with route guidance, GPS is also able to provide real-time information about traffic congestion and adverse weather conditions between a driver's current location and his destination.[226] GPS, in conjunction with the internet, can guide people to their destination, find lost people, send emergency aid to those in trouble and track a person's whereabouts instantaneously.[227] It was used by the U.S. military after the war in Vietnam and was designed to track the exact location of U.S. military troops in the fields.[228]

But this unique Intelligent Transportation tool poses a strong privacy risk. If you scroll down the menu for the GPS unit, there is a function that shows past history.[229] For example, you can see how fast the previous renter of the car traveled,[230] or the driving record of the renter could be revealed. The Illinois Tollway Authority is conducting a feasibility study to use GPS technology to replace motorists tossing coins into the toll

---

[222] Richard C. Balough, *Global Positioning System and the Internet: A Combination With Privacy Risks*, 15-OCT CBA Rec. 28, 28 (2001).
[223] *Id* at 28.
[224] *Id*.
[225] Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology,* 11 Santa Clara Computer & High Tech. L.J. 151, 153 (1995).
[226] *Id*.
[227] Balough, *supra* note 221 at 28,29.
[228] *Id* at 29.
[229] *Id* at 28.
[230] *Id*.

baskets.[231] Instead, motorists using the Illinois tollways would be billed for actual miles driven based on information in onboard computers logging the roadway use through GPS.[232] If this system becomes a reality the state tollway authority will be able to collect vast amounts of information and the question is: How will they use it?[233] Personal data could be given or sold to third parties, which could adversely affect the renter, or it could be given to law enforcement officials.[234] Returning to the car rental example, would there be any potential privacy rights violations by the installation of GPS?[235] Assuming that the GPS requires activation by the renter, there may not be any personal rights violated; it would be a voluntary decision whether to activate the system or not.[236] But the user may not be aware that the system maintains information long after its use.[237] GPS is such a sophisticated tool that it may become a substitute for an individual itself.[238] The GPS generated travel profiles will threaten privacy, as this type of profiling will be dehumanizing to the individual.[239] If the profile is different from the individual's own image, the separation can be psychologically damaging.[240] An individual will loose his self-respect, as the tendency of GPS is to reduce the complexity of an individual's human personality to ciphers and formulas.[241] It makes no difference that the information gathered is not personal or private, when compared, for example, with data about a person's health or financial status.[242] Individuals will be concerned when a

---

[231] *Id*.
[232] *Id*.
[233] *Id*.
[234] *Id* at 31.
[235] *Id* at 30.
[236] *Id.*
[237] *Id*.
[238] Glancy, s*upra* note 224 at 165.
[239] *Id*.
[240] *Id*.
[241] *Id*.
[242] *Id*.

comprehensive information profile is constructed about any aspect of their life.[243] Also, in a way, the transportation information collected will be likely to reveal some aspects of a person's private life. It might reveal, for example, where the person shops, works, worships, reads, views movies or buys books.[244]

C. Mobile Telecommunications.

The greatest feature of wireless communications is the ability to send and receive messages from anywhere.[245] Many people can be tracked today without the use of cameras or other devices.[246] In order to carry or receive calls, cellular phones must communicate their location to a base station.[247] Therefore, whenever a cell phone is in use, or set to receive calls, it effectively identifies the location of its user every few minutes (within an area defined by the tolerance of the phone).[248] There are numerous consumer benefits from technologies that track the location of mobile phone users. For example, consider the following situation: Suppose an individual's purse has just been stolen.[249] His partner's one-button mobile call to an emergency service immediately pinpoints the individual's location for the police, and the mobile phone inside the purse allows the police to quickly track down the culprit.[250] Your always-on mobile phone produces a signal that allows the police to follow your every movement with pinpoint

[243] *Id.*
[244] *Id.*
[245] Charlene L. Lu, *Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy With the Need for Effective Law Enforcement*, 17 Hastings Comm/Ent L.J. 529, 532 (1995).
[246] Michael Froomkin, *The Death of Privacy?*, 52 Stan. L. Rev. 1461, 1479 (2000).
[247] *Id.*
[248] *Id.*
[249] Kurt Wimmer, *Privacy and Mobile Telecommunications*, 19_SUM Comm.Law. 20, 20(2001).
[250] *Id.*

precision.[251] In January 1997, Karen Nelson got lost while driving through a blizzard on a remote stretch of South Dakota highway and drove her truck off the road into a snow bank.[252] Nelson had a cellular phone with her and was able to call 911 for help, but she did not know her location.[253] Since the emergency workers had no way of accurately determining her location, it took almost 40 hours and a massive rescue operation involving snow mobiles and airplanes before searchers finally located Nelson's truck.[254] In order to provide the same level of 911 service to cellular telephone users as is currently available to regular telephone users, the Federal Communications Commission (FCC) requires cellular telephone companies to have the capability of determining the location from which a cellular phone call originates to within 125 meters.[255] If Karen Nelson's accident had happened today, the South Dakota 911 operators could reduce the time taken it took to rescue Karen from hours to minutes.[256]

The enhanced 911, or E911 service has several stages.[257] At the most basic level, the FCC requires emergency calls to be routed to a central processing center and to be transmitted without regard to validation of the caller's status as a subscriber.[258] At the more advanced level, the FCC requires the carriers to provide location information of all wireless 911 callers to these processing centers.[259] The Phase I of the FCC rules require carriers to provide information on the base station handling the call, which may narrow down the

---

[251] *Id.*
[252] Matthew Mickle Werdegar, *Lost? The Government knows where you are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 Stan. L. & Pol'y rev. 103,103 (1998).
[253] *Id.*
[254] *Id.*
[255] *Id.* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 emergency Calling Systems, Memorandum Opinion and Order, Fed. Comm. Commm'n, CC Docket No. 94–102, Dec. 23, 1997.
[256] *Id.*
[257] Wimmer, s*upra* note 248 at 22.
[258] *Id.*
[259] *Id.*

location of the caller to a few city blocks in a dense area or a few miles in the case of a rural analogue cellular system.[260] The phase II rules, requires carriers to provide location information with much greater precision.[261] According to the FCC timetable, U.S. wireless carriers will have significant mobile location capabilities by 2005.[262]

The cellular telephone call location technology now mandated by the FCC will turn each of the more than fifty million cell phones in the United States into a tracking device.[263] This poses a major privacy hazard. The very thought that your cell phone is a giveaway of your location is frightening. Consumers clearly will be concerned about securing their privacy against revealing location information without their consent.[264] In the United States, in response to concerns expressed by the Federal Bureau of Investigation that new telecommunications technologies could hinder criminal investigations, Congress passed the Communications Assistance For Law Enforcement Act (CALEA).[265] During the brief congressional debate leading up to CALEA's passage, then FBI director Louis Freeh stated that the FBI did not wish to turn wireless phones into location-tracking devices. He stated: "There is no intention whatsoever to acquire anything that could properly be called 'tracking information'."[266] However, *United States Telecommunications Ass'n v. Federal Communications Comm'n,*[267] in implementing CALEA, the FCC agreed to permit law enforcement agencies such as the FBI to have

---

[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] Werdegar, s*upra* note 252 at 104.
[264] Wimmer, s*upra* note 248 at 23.
[265] For a more comprehensive overview of the passage and implementation of CALEA, see David Sobel, *Privacy and Law Enforcement In The Digital Age,* 18 COMMUNICATIONS L., at 3 (Winter 2001); *Id*
[266] *See* Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375, 103d cong., 2d Sess. at 29 (1994) (statement of Louis Freeh, Director, Federal Bureau of Investigation); Wimmer, s*upra* note 245 at 24.
[267] 227 F.3d 450 (D.C. Cir. 2000).

access to caller's locations at the beginning and end of each call.[268] The District of Columbia Circuit responded by holding that law enforcement would need more than a mere pen-register--an order that can be obtained without a search warrant.[269] Mobile location technologies promise a dramatic improvement in the safety and convenience available to subscribers to wireless telecommunications services.[270] But at the same time consumers will be apprehensive to subscribe to these services without adequate assurances for their privacy.[271] All over the world the burden of demonstrating adequate assurances for privacy is likely to fall upon mobile telecommunications carriers who wish to offer their services to their subscribers.[272]

D. Wearable Computing and Surveillance Cameras.

" I AM A CAMERA".[273] Wearable Computing promises to become the fourth wave of computing following the developments of the mainframe, minicomputers and personal computers.[274] A wearable computer is a computing device that is worn on the body consisting of some type of output display, such as a small, eyeglass-size monitor, and some input device, such as a one-handed keyboard or speech recognition system.[275] At the McLuhan Symposium on Culture and Technology,[276] Professor Steve Mann[277] stated:

---

[269] *Id* at 453.
[270] Wimmer, *supra* note 248 at 23.
[271] *Id*.
[272] *Id*.
[273] *" Many Dimensions: The Extensions of Marshall McLuhan."* Keynote address at the McLuhan Symposium on Culture and Technology on October 23, 1998. *available at* http://wearcam.org/mcluhan-keynote.htm
[274] Amy M. Intille, *Video Surveillance and Privacy: Implications for Wearable Computing*, 32 Suffolk U. L. Rev. 729, 751 (1999).
[275] *Id*.
[276] McLuhan, *supra* note 87.

"Just as the wheel is an extension of the leg, and radio is an extension of the voice, so too, is the camera an extension of the eye, the computer [is] an extension of the brain, and wiring, circuits, and the internet an extension of the nervous system."

A wearable computer has the following characteristics:

(1) It is portable when operational - The most distinguishing feature of a wearable is that it can be used while walking or otherwise moving around.[278] This is a distinguishing feature between wearables and desktop and laptop computers.[279]

(2) Hands free use - Military and industrial applications for wearables especially emphasize their hands-free aspect, and concentrate on speech input and heads-up display or voice output.[280] Other wearables might also use chording-keyboards, dials, and joysticks to minimize the tying up of a user's hands.[281]

(3) Sensors – The wearable computer incorporates sensors such as wireless communications, GPS, cameras, or microphones.[282]

(4) Always on and always running - By default a wearable is always on and working, sensing, and acting.[283] It is also 'Proactive' i.e. it is able to convey information to its user

---

[277] Professor Steve Mann, the inventor of WearComp (wearable computer and personal imaging system), is currently a faculty member at the University of Toronto, Department of Electrical and Computer Engineering. Dr. Mann's WearComp invention dates back to his high school days in the 1970's and early 1980s, where he was experimenting with wearable computing and personal imaging as a personal hobby. He brought his inventions and vision to the Massachusetts Institute of Technology and founded the MIT wearable computing effort in 1991, which was officially recognized by faculty members later in the mid 1990s, and subsequently grew from himself initially, to several others. He received his PhD degree from MIT in 1997. His previous degree is Master of Electrical Engineering (MEng) from McMaster University. Dr. Mann also holds undergraduate degrees in physics (BSc) and electrical engineering (B.Eng). More information on Dr. Mann's work is *available at* http://www.wearcam.org and more of his articles at http://wearcam.org/ieeecomputer.html and http://wearcam.org/procieee.html.

[278] Bradley J. Rhodes, *The Wearable Remembrance Agent: A System For Augmented Memory, available at* http://web.media.mit.edu/~rhodes/Papers/wear-ra-personaltech/index.html also see http://www.media.mit.edu/ rhodes/

[279] *Id.*

[280] *Id.*

[281] *Id.*

[282] *Id.*

[283] *Id.*

even when not actively being used.[284] For example, if your computer wants to let you know that you have new email and whom the email is from, it will be able to communicate this information to you immediately.[285]

Video surveillance and wearable computing share a critical component part i.e. the video camera, which is a powerful technology tool that can significantly invade privacy.[286] Video technology has changed the way people view the world around them and the way people are viewed.[287] Over the years the camcorder has had numerous advantages; there have been well-publicized and famous examples of surreptitious filming serving the public good.[288] The most celebrated was George Holliday's videotape of Los Angeles police officers beating Rodney King.[289] Other well-publicized examples include an environmentalist who filmed fishermen slaughtering dolphins caught in tuna nets, a suspicious parent who taped his baby sitter abusing his child, and a gay man in California who, fed up with abusive taunting from his neighbor, set up a camcorder and filmed the neighbor assaulting him in his front yard.[290] However these instances of positive, surreptitious videotaping are overshadowed by many more situations when video cameras have intruded unreasonably upon and individual's privacy.[291] Voyeurs have frequently used the video camera to surreptitiously record people in private settings.[292] In the United States, over sixty urban centers use video surveillance in public

---

[284] *Id.*
[285] *Id.*
[286] Intille, s*upra* note 273 at 757.
[287] *Id.*
[288] Andrew Jay Mcclurg, *Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. Rev. 989, 1022 (1995).
[289] *Id.*
[290] *Id.*
[291] Intille, *supra* note 284 at 758.
[292] *Id.*

places for law enforcement purposes.[293] Television broadcasting corporations and viewers in the United States seem addicted to the vicarious thrill of watching invasions of others' privacy.[294] The number of surveillance cameras of all types in America is overwhelming and growing every day.[295] Recently, the New York Civil Liberties Union sent a survey team into Manhattan to count surveillance cameras.[296] The team counted more than 2,400 cameras monitoring the movements of pedestrians, drivers, shoppers, and anyone else who wandered into their range.[297] Great Britain is the world's pioneer of closed circuit television surveillance and over one million cameras are in place.[298] Three hundred different cameras on thirty different networks monitor an average person in London during the course of a single day.[299]

The ubiquitous use of the video camera, both through public and private surveillance, and the pervasive use of video camcorders have raised privacy concerns, and similarly, the use of wearable computers will also raise privacy issues.[300] The ability of the wearable computer to constantly record audio and video from the user's environment is the source for these privacy concerns.[301] In addition to the privacy concerns raised by pervasive monitoring in video surveillance and wearable computing, tracking abilities associated with video surveillance and wearable computers also threaten

---

[293] See Milligan, s*upra* note 36 at 301.
[294] *Id.* (There is an abundance of "real life" television programs that make use of video surveillance and CCTV programming – COPS and Rescue 911, among others. Investigative news programs like 60 minutes make use of hidden cameras, while local network affiliates replay footage from police and liquor store video cameras on their nightly news broadcasts. Apparently broadcasters will continue to have plenty of footage, as the use of CCTV systems will undoubtedly continue to increase).
[295] Bob Barr, *A Tyrant's Toolbox: Technology and Privacy in America*, 26 J. Legis. 71, 72 (2000).
[296] *Id.*
[297] *Id.*
[298] *Id.*
[299] *Id.*
[300] Intille, *supra* note 88 at 759.
[301] *Id.*

an individual's privacy.[302] An increasing number of police departments in American cities have set up video surveillance cameras, which in addition to pervasive monitoring also have the ability to track an individual's movement as they walk on a public street.[303] Like video surveillance systems, wearable computers represent a new threat to privacy rights because this powerful new technological tool can constantly record and store everything about a user's environment through sensors.[304] While wearable computers are a relatively new technology, it will become a pervasive toll used by almost all computer users in the near future.[305] Currently there are no statutes or decisions regulating a wearable computer's intrusion into personal privacy rights.[306] But eventually, the wearable computer's ability to record video and audio communications will encroach on an individual's privacy.[307]

E. Facial Recognition System.

An individual's face is an important part of who he is and how people identify him.[308] It would be very hard to recognize an individual if all faces looked the same.[309] Except in the case of identical twins, the face is arguably a person's most unique physical characteristic.[310] While humans have had the inherent ability to recognize and distinguish different faces for millions of years, computers are just now catching up.[311]

---

[302] *Id*.
[303] *Id* at 760.
[304] *Id* at 765.
[305] *Id*.
[306] *Id*.
[307] *Id*.
[308] Kevin Bonsor, *How Facial Recognition Systems Work*, *available at* http://www.howstuffworks.com/facial-recognition1.htm.
[309] *Id*.
[310] *Id*.
[311] *Id*.

A ticket to the January 2000 Super Bowl XXXV in Tampa Bay, Florida, didn't just get the spectators a seat at the biggest professional football game of the year.[312] Those who attended the event were also part of the largest police lineup ever conducted, although they may not have been aware of it at the time.[313] The Tampa Police department was testing out a new technology, called 'FaceIt', that allows snapshots of faces from the crowd to be compared to a database of criminal mug shots.[314] Facial recognition software can be used to find criminals in a crowd, turning a mass of people into a big lineup.[315] If you look in the mirror, you can see that your face has certain distinguishable landmarks.[316] These are certain peaks and valleys that make up the different facial features.[317] Visionics defines these landmarks as 'nodal points'.[318] There are about 80 nodal points on a human face.[319] The software measures a few of the nodal points, to name a few: The distance between the eyes, width of the nose, depth of the eye socket, cheekbones, jaw line and chin.[320]

Facial recognition systems would be very beneficial to law enforcement agencies, in their efforts to catch law violators and terrorists. But several government agencies have abandoned facial-recognition systems after finding they did not work as advertised. These agencies include the Immigration and Naturalization Service (INS), which experimented

[312] Bonsor, s*upra* note 306.
[313] *Id*.
[314] *Id*.
[315] *Id*.
[316] *Id*.
[317] *Id*.
[318] *Id*.
[319] *Id*.
[320] *Id*. (These nodal points are measured to create a numerical code, a string of numbers that represents the face in a database. This code is called a 'faceprint'. Only 14 to 22 nodal points are needed for the FaceIt software to complete the recognition process).

with using the technology to identify people in cars at the Mexico-U.S. border.[321] Face-recognition software is useless in huge areas like the airports, as the technology simply isn't reliable enough for such an important security application.[322]

The Facial Recognition system threatens privacy in a number of ways.[323] One threat is the fact that facial recognition, in combination with wider use of video surveillance, would be likely to grow increasingly invasive over time.[324] This kind of system can rarely be confined to its original purpose.[325] New ways of using it will suggest themselves, the law enforcement authorities will find them to be an irresistible expansion of their power, and an individuals privacy will be destroyed.[326] Ultimately, the threat is that widespread surveillance will change the character, feel, and quality of a human being's life.[327]

Another problem that can arise is that of abuse of the system.[328] The use of facial recognition in public places -- for example: airports -- depends on widespread video monitoring, which is an intrusive form of surveillance that can record in graphic detail personal and private behavior.[329] Over the years there have been numerous cases where video monitoring has been misused.[330] After all, a human being eventually operates the

---

[321] American Civil Liberties Union, *Q & A on Facial Recognition, available at* http://www.aclu.org/issues/privacy/facial_recognition_faq.html.
[322] *Id.* (It would work especially poorly in the frenetic environment of an airport, where fast-moving crowds and busy background images would further reduce its already limited effectiveness. The evidence suggests that these systems would miss a high proportion of suspects included in the photo database, and flag huge numbers of innocent people - lessening vigilance, wasting precious manpower resources, and creating a false sense of security).
[323] *Id.*
[324] *Id.*
[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*

video camera.[331] In Great Britain, for example, which has experimented with the widespread installation of closed circuit video cameras in public places, camera operators have been found to focus disproportionately on people of color, and the mostly male operators frequently focus specifically on women.[332] The question is "How necessary is facial recognition system for the security and safety of individuals?"[333] With the recent terrorist attacks in the United States and around the world, the Government will always be justified in installing the new and latest surveillance devices for the protection of its citizens. But the law enforcing agencies should ask themselves two questions: First, how effective is the face recognition technology?[334] If the answer is no, then any further discussion is pointless.[335] If the answer is yes, then the second question is whether the technology violates the appropriate balance between security and liberty.[336] In reality, facial recognition fails on both counts: as it does not work reliably and it doesn't significantly protect an individual's security.[337]

F. Thermal Imaging.

Thermal imaging is one of the latest technological tools in the government's arsenal to identify and eliminate illegal indoor cultivation of marijuana.[338] The indoor cultivation of marijuana has rendered the traditional methods of detecting it obsolete, thus

[331] *Id.*
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] Daniel J. Polatsek, *Thermal Imaging and the Fourth Amendment: Pushing the Katz Test Towards Terminal Velocity,* 13 J. Marshall J. Computer & Info. L 453, 453 (1995).

giving rise to widespread indoor cultivation of marijuana.[339] Indoor cultivation is very lucrative since as many as four crops can be harvested annually.[340] However the whole process of cultivation generates thermal energy, which either escapes or is vented to the outside.[341] Such thermal energy can be detected by a thermal energy detection instrument, know as a 'Forward Looking Infrared Radar' (FLIR).[342] This instrument senses differences in surface temperatures and can record its findings on videotape.[343] Using FLIR generated visual images, law enforcement officials may assume that an individual is cultivating marijuana plants indoors.[344] These inferences, when combined with other evidence, may then lead the police to discover illegal gardening operations.[345] The question is whether an individual has a reasonable expectation of privacy under the Fourth Amendment that his home will not be subjected to search by Thermal Imaging. The landmark case of *Kyllo v. United States*[346] involved the use of thermal imaging. What happened in this case was that the law authorities suspected Kyllo of growing marijuana in his home triplex, the agents used a thermal imaging device to scan the triplex in order to determine if the amount of heat emanating from it was consistent with the high-intensity lamps typically used for indoor marijuana growth.[347] The scan showed that Kyllo's garage roof and a side wall were relatively hot compared to the rest of his home

[339] Mindy G. Wilson, *The Prewarrant Use of Thermal energy: Has this Technological Advance in the War Against Drugs Come at the Expense of Fourth Amendment Protections Against Unreasonable Searches?,* 83 Ky. L.J. 891, 892 (1995).
[340] *Id.*
[341] Mark J. Kwasowski, *Thermal Imaging Technology: Should Its Warrantless Use By Police Be Allowed In Residential Searches?,* 3 Tex. Wesleyan L. Rev. 393, 394 (1997).
[342] *Id.*
[343] *Id.*
[344] *Id.*
[345] *Id.*
[346] 121 S.Ct. 2038(2001).
[347] *Id.*

and substantially warmer than the neighboring units.[348] Based in part on the thermal imaging, a Federal Magistrate Judge issued a warrant to search Kyllo's home, where the agents found marijuana growing.[349] After Kyllo was indicted on a federal drug charge, he unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea.[350] The Ninth Circuit affirmed, upholding the thermal imaging on the ground that Kyllo had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home.[351] Even if he had, ruled the court, there was no objectively reasonable expectation of privacy because the thermal imager did not expose any intimate details of Kyllo's life, only amorphous hot spots on his home's exterior.[352]

But eventually the Supreme Court held that:

"Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a [F]ourth [A]mendment 'search', and is presumptively unreasonable without a search warrant." [353]

"It is only when an individual exposes what is personal to the public, that the personal item loses its Fourth Amendment privacy protection."[354] In other words, the police are free to observe what everyone else can observe.[355] But in the case of Kyllo, it was his

---

[348] *Id.*
[349] *Id.*
[350] *Id.*
[351] *Id.*
[352] *Id.*
[353] *Id.*
[354] Sherry F. Colb, *Is Use of Thermal Heat Imaging A "Search" Governed By The Fourth Amendment? How The Supreme Court Should resolve The Kyllo Case, available at* http://writ.news.findlaw.com/colb/20010228.html.
[355] *Id.*

intention to keep his activity away from the view of the public.[356] If the thermal imaging technology is used in a way, that it reveals marijuana plant cultivation only and nothing else, then, it may be appropriate to allow its use. The technology, however, can be misused i.e.-- it may be used to check if a person is present in his home, how many people are inside a house, and whether they are together or in separate rooms. This should not be allowed.[357]

G. Canivore and Echelon

The main reason for computer security is data privacy.[358] People protect their systems so that unwanted people can't see data they're not authorized to see.[359] The computer networks of the world are routinely used in the commission of serious criminal activities, including espionage, fraud and terrorist attacks.[360] Modern day organized crime and terrorists rely "upon telecommunications to plan and execute their criminal activities on a daily basis."[361]

Carnivore is a sealed box that the FBI installs at an Internet Service Provider (ISP).[362] The box filters packets, looking for emails of suspected criminals.[363] Once emails from

---

[356] *Id.*
[357] *Id.*
[358] Chris Parker, *Carnivore and Privacy: An Oxymoron?, available at* http://www.linuxsecurity.com/feature_stories/feature_story-63.html.
[359] *Id.*
[360] John Lewis, *Carnivore - The FBI's Surveillance System: Is It A Rampaging E-mailasaurus Rex Devouring your Constitutional Rights?*, 23 Whittier L. Rev. 317, 317 (2001).
[361] *Id.*
[362] Parker, *supra* note 353 at 167. An ISP is a company that provides end users (such as you and me and big companies) access to the Internet. Two large ISPs are Netcom On-Line Communication Services, Inc. (see http://www.netcom.com) and Performance Systems International, which is at http://www.psi.net. More information on ISP is *available at* http://www.oreilly.com/reference/dictionary/tsearch.cgi.
[363] *Id.*

suspects are found, they are saved for decryption and analysis.[364] The FBI claims that Carnivore is only meant for tapping the emails of suspected criminals.[365] Also built into Carnivore is a remote-access capability that allows FBI agents to check on the progress of the Carnivore system.[366] Authorities have used Carnivore-type tools more than 25 times in all types of criminal cases and in order to catch fugitives, drug dealers, extortionists and suspected foreign intelligence agents.[367] Carnivore is now called 'DCS-1000'.[368]

Carnivore is a major privacy risk. Even though it can be made active only by a court order and directed only towards a suspect's email, there is no way for it to not intercept email of innocent private citizens while it scans for evidence in a criminal investigation.[369] Because Carnivore uses key words and phrases, it is likely to pick up email to and from people who have nothing to do with a crime simply because their email contains certain words.[370] A recent article on CBSNews.com showed that the Carnivore is not a reliable way of catching criminals.[371] The article reported that the FBI had destroyed evidence gathered in an investigation involving Osama Bin Laden's Al Qaeda terror network after the FBI's Carnivore's system mistakenly captured information to which the agency was not entitled.[372] A March 2000 memo to agency headquarters in Washington stated that the FBI software had not only picked up targeted emails "but also picked up emails on non-covered targets."[373] "The FBI technical person was apparently

---

[364] *Id.*
[365] *Id.*
[366] *Id.*
[367] D. Ian Hopper CBS News, *Memo Reveals FBI E-mail Snafu* (Washington May 29, 2002) *available at* http://www.cbsnews.com/stories/2002/05/29/attack/main510393.html.
[368] *Id.*
[369] *See* www.about.com, *Privacy Eaten Away By Carnivore, available at* http://netsecurity.about.com/library/weekly/aa072500a.htm.
[370] *Id.*
[371] See s*upra* note 362.
[372] *Id.*
[373] *Id.*

so upset that he destroyed all the email take, including the take on the suspect," according to this memo.[374] This episode was made public through a Freedom of Information Act request filed by the electronic Privacy Information Center, which is a Washington advocacy group.[375] The material was not included in an original release but became public after a federal judge ordered the bureau to give out more documents.[376] The issue in this case was an investigation in Denver in which the FBI's Bin Laden unit was using the bureau's Carnivore system to conduct electronic surveillance of a suspect under a Foreign Intelligence Act warrant.[377] The suspect's name and other information identifying details were marked out of the letter.[378] The memo surfaced as the FBI was addressing concerns that it mishandled aspects of terrorism investigation prior to the September 11 attacks.[379] Those concerns also focused on a warning from the FBI's Phoenix office about Arab pilots training in the United States last July.[380] Privacy groups and some members of Congress have complained that Carnivore has the potential to collect more information than what is required.[381] "Here's confirmation of the fact that not only did it do that, but it resulted in a loss of legitimately acquired intelligence," said David Sobel, general counsel of the Electronic Privacy Information Center, the group that sued to get the documents.[382]

[374] *Id.*
[375] *Id.*
[376] *Id.*
[377] *Id.*
[378] *Id.*
[379] *Id.*
[380] *Id.*
[381] *Id.*
[382] *Id.*

ECHELON is a term associated with a global network of computers that automatically search through millions of intercepted messages for pre-programmed keywords or fax, telex and e-mail addresses.[383] Every word of every message in the frequencies and channels selected at a station is automatically searched.[384] The processors in the network are known as the ECHELON Dictionaries.[385] ECHELON connects all these computers and allows the individual stations to function as distributed elements an integrated system.[386]

ECHELON is a code word for an automated global interception and relay system operated by the intelligence agencies in five nations – the United States, the United Kingdom, Canada, Australia and New Zealand.[387] The original ECHELON dates back to 1971.[388] However, its capabilities and priorities have expanded greatly since its formation. According to recent reports, it is capable of intercepting and processing many types of transmissions throughout the globe.[389] In fact, it has been suggested that ECHELON may intercept as many as three billion communications every day, including phone calls, e-mail messages, Internet downloads, satellite transmissions, and so on.[390] How does ECHELON work?[391] Apparently it collects data in several ways. Reports suggest it has massive ground based radio antennae to intercept satellite transmissions.[392]

---

[383] FAS Intelligent Resource Program, *ECHELON, available at* http://www.fas.org/irp/program/process/echelon.htm.
[384] *Id.*
[385] *Id.*
[386] *Id.*
[387] Claw, Protecting the Bill Of Rights For The Next Generation, *Echelon, We're All At Risk, available at* http://www.libertyteeth.org/echelon.html.
[388] *Id.*
[389] *Id.*
[390] *Id.*
[391] *Id.*
[392] *Id.*

In addition, some sites reputedly are tasked with tapping surface traffic.[393] These antennae reportedly are in the United States, Italy, England, Turkey, New Zealand, Canada, Australia, and several other places.[394] It is also believed that ECHELON uses numerous satellites to catch "overflow" data from transmissions between cities.[395] These satellites then beam the information down to processing centers on the ground.[396] The main centers are in the United States (near Denver), England (Menwith Hill), Australia, and Germany.[397] It is also believed that ECHELON has even used special underwater devices, which tap into cables that carry phone calls across the seas.[398] According to published reports, American divers were able to install surveillance devices on to the underwater cables.[399] One of these taps was discovered in 1982, but other devices apparently continued to function undetected.[400]

There is evidence to show that Echelon significantly invades privacy. Although the evidence is circumstantial, there are alleged violations by the secret surveillance of political organizations such as Amnesty International.[401] Many nations have laws, that prevent invasions of privacy.[402] But it is rumored that ECHELON has engaged in a trick in order to avoid these legal restrictions. For example, it is rumored that nations would not use their own agents to spy on their own citizens, but assign the task to agents from other countries.[403] ECHELON is the ultimate in spy software.[404]

---

[393] *Id*.
[394] *Id.*
[395] *Id*.
[396] *Id*.
[397] *Id*.
[398] *Id*.
[399] *Id*.
[400] *Id*.
[401] *Id*.
[402] *Id*.
[403] *Id*.
[404] Lewis, s*upra* note 355 at 333.

CHAPTER 4

GLOBAL TRENDS IN PRIVACY PROTECTION.[405]

A. India.

The Indian Constitution recognizes an impressive array of Fundamental Rights, covering a wide range of civil, political, cultural, economic and social rights.[406] But the Constitution does not expressly recognize the right to privacy.[407] However Article 21 of the Constitution states: "No person shall be deprived of his life or personal liberty except according to procedure established by law."[408]

In 1964, the Supreme Court first recognized that there is a right of privacy implicit in Art. 21.[409] There are also other Indian laws that guarantee the right to privacy.[410] Unlawful attacks on the honor and reputation of a person can invite an action of tort or criminal law.[411] There are no general data protection laws in India.[412] Wiretapping is regulated under the Indian Telegraph Act of 1885, and on December 20, 1996, the Supreme Court of India ruled that: "[w]iretapping is a serious invasion of a persons privacy" and called for the government to update the century-old Indian Telegraph Act's clause on interception.[413] This suit was a public interest suit brought by

---

[405] Banisar and Davies, s*upra* note 1 at 53 (1999).
[406] Vijayashri Sripati, *Human Rights in India – Fifty years After Independence,* 26 Denv. J. Int'l L. & Pol'y 93, 98 (1997).
[407] The Constitution of India (1949).
[408] *Id*.
[409] Banisar and Davies, s*upra* note 1 at 53.
[410] *Id.*
[411] *Id*.
[412] *Id*.
[413] Rishab Aiyer Ghosh, *India's High Court Pulls Plug On Wiretapping*,(December 26, 1996) *available at* http://www.wired.com/news/topstories/0,1287,1128,00.html.

the People's Union for Civil Liberties.[414] The Court ruled that an order for wiretapping could be issued only by the Federal Home Secretary - the most senior official in India's equivalent to the US Department of Justice.[415] In "urgent" cases, this power can be delegated to slightly lower-level officials.[416] The Court said: "Wiretaps can be used only if no 'other reasonable means' are available."[417] However, in this case, the Supreme Court did not rule on what exactly is in the public interest and what justifies interception.[418] Wiretapping in India is used by the Intelligence Bureau (Central Bureau of Investigation),[419] which claims to be the longest-existing intelligence service in the world.[420]

However even after the modification of the act, there have been instances of illegal wiretapping by the Indian government.[421] According to prominent Non-Governmental Organizations (NGO's) in India, the mail of many NGO's in Delhi and other strife torn areas in India continue to be subjected to interception and censorship.[422] There are very comprehensive plans being made for a massive "citizens database" to be owned and operated by the state.[423] It is rumored that this exercise will climax in a scheme called 'NISHAN' (National Identification System Home Affairs Network) or the INDIA CARD, by which all citizens will have to carry identity cards containing all relevant information (including legal records) about them, identifying photographs and

---

[414] *Id.*
[415] *Id.*
[416] *Id.*
[417] *Id.*
[418] *Id.*
[419] The Central Bureau of Investigation (CBI) is the equivalent of the FBI.
[420] *Id.*
[421] Banisar and Davies, s*upra* note 1 at 54.
[422] *Id.*
[423] The Hindustan Times, September 17, 2000, *available at* http://www.hindustantimes.com/nonfram/170900/detFEA03.asp.

bio metric date (data about their body measurements, hand prints etc.).[424] This kind of card is unnecessary as in India there are already various forms of identification-- For example, a driver's license, a Ration card (this is issued by the government to buy groceries at a subsidized rate), a PAN (Permanent Account number) number given to all Indian citizens who pay taxes. The Union Minister of India, Mr. L.K. Advani is very keen on the implementation of INDIA CARD basically to check the influx of illegal immigrants.[425]

India is heading in the same direction as the west as people do end up giving more personal details than they would care to ordinarily when for credit cards and opening bank accounts.[426] NISHAN will merely put it all together — apparently for use by the State — but the prospect of this data falling into wrong hands will rightfully make anybody suspicious of this scheme.[427] If NISHAN is implemented, it will offer detailed information on every citizen and would mean that "Big Brother" has arrived in India.[428]

B. The United Kingdom.

During the last decade, law enforcement agencies in Great Britain have increasingly relied on Close Circuit Television (CCTV) surveillance to enhance public security.[429] According to some researchers, the camera surveillance systems in the UK are discouraging and thus preventing crime.[430] Public video surveillance in the UK began very unassumingly in 1986, on a single square mile industrial estate outside the English

---

[424] *Id.*
[425] *Id*. A large number of illegal immigrants into India are the Bangladeshi Muslims.
[426] *Id*.
[427] *Id*.
[428] *Id*
[429] Kevin Reis, *The Eavesdropping Society: Electronic Surveillance And Information Brokering*, 632A PLI/Pat 627, 631 (2001).

town of King's Lynn.[431] Three CCTV video surveillance cameras were used and their impact was immediate.[432] In the years before the cameras were installed, there had been 58 crimes recorded on the estate and in the two years following the installation, there were no crimes reported.[433] Subsequently, cities and towns across Great Britain began using this crime prevention measure.[434] By 1994, over three hundred jurisdictions in the country had installed some form of public video surveillance.[435] In 1995, the national government made available up to $3.1 million in matching grants for cities and towns to establish CCTV video surveillance programs.[436] There are currently nearly eight hundred local public video surveillance programs in operation in the UK and the British government provides $22 million annually in matching grants.[437]

According to the English civil libertarians, there is no control in the UK over the commercial use of public video images recorded by CCTV.[438] Because the United Kingdom has more video surveillance per capita than any other country in the world, it is very easy to find footage from parking garages, housing developments, department stores and offices that may have commercial value.[439] Cameras may record women undressing in department store changing rooms, or husband and wives engaging in domestic squabbles.[440]

---

[430] *Id.* at 641.
[431] *Id* at 642.
[432] *Id*.
[433] *Id*.
[434] *Id*.
[435] *Id*.
[436] *Id*.
[437] *Id* at 643.
[438] *Id* at 645.
[439] *Id*.
[440] *Id*.

The United Kingdom does not have a Bill of Rights that protects individuals from government intrusions on privacy.[441] Individuals have limited recourse against local government agencies that provide revealing tapes to commercial producers.[442] While invasion-of-privacy lawsuits can be filed against the producers, they often protect themselves by making the footage sufficiently fuzzy to prevent clear identification of individuals.[443]

The UK is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) along with the European Convention for the Protection of Human Rights and Fundamental Freedoms.[444] In addition to these commitments, the UK is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[445]

C. Australia.

Neither the Australian Federal Constitution nor the Constitution of the six States contains any express provisions relating to privacy.[446] After the terrorist attacks on America on September 11, 2001, the Australian Parliament passed the Cybercrime Bill

[441] *Id.* at 646.
[442] *Id.*
[443] *Id.*
[444] David Banisar, *Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, available at* http://www.privacyinternational.org/survey/.
[445] *Id.*
[446] Banisar and Davies, s*upra* note 1 at 17.

2001 and a series of bills to expand electronic surveillance powers and increase penalties for espionage.[447] The principal federal statute is the Privacy Act of 1988.[448]

In December 2000, the *Privacy Amendment (Private Sector) Act 2000* (the Amendment Act) was passed by federal Parliament.[449] This amends the Privacy Act, which, until now, has mainly covered public sector agencies.[450] The National Privacy Principles (NPPs) in the Privacy Act set out how private sector organizations should collect, use, keep secure and disclose personal information.[451] The principles give individuals a right to know what information an organization holds about them and a right to correct that information if it is wrong.[452]

D. Germany.

The German government has approved a surveillance regulation that is intended to make it easier for authorities to eavesdrop on communications via fixed-line and mobile phone, e-mail, fax, and SMS (short message service).[453] This move put Berlin in line with other Western governments rushing to enact similar rules since the September 11 terrorist attacks in the United States.[454] The new rule, passed by the Cabinet requires

---

[447] Pete Young, *Australia reviews antiterrorist e-surveillance laws: "When is hacking into a network a police matter and when is it a national defense problem"?, available at* http://www.idg.net.nz/webhome.nsf/PrintDoc/7B971DF0C8D3E8C7CC256ADA000E7618!opendocument Australia's recent legislative efforts include: Cybercrime Bill 2001 - Passed by Parliament on September 27, which allows the jailing of computer hackers for up to 10 years. Telecommunications Interception Legislation Amendment Bill 2001 - introduced in the final days of the 39th Parliament, it proposes to expand police powers to tap phones, the Internet and email and finally The Criminal Code Espionage Bill - which will lift maximum jail terms for espionage to 25 years from seven.
[448] *See* Privacy Act, 1988 (Austl.).
[449] *See* <http://www.privacy.gov.au/publications/pia.doc>
[450] *Id.*
[451] *Id.*
[452] *Id.*
[453] Rick Perera, IDG News Service, Berlin Bureau, *Germany Joins World Wide Surveillance Trend,* ITworld.com 10/25/01, *available at* http://www.itworld.com/Tech/2987/IDG011025surveill/.
[454] *Id.*

network providers to install and maintain equipment and procedures to give access to their customers' electronic traffic when authorities have a legal surveillance order.[455]

The technical requirements are limited to providers of “public telecommunication systems,” which include fixed-line and mobile phone operators and providers of e-mail accounts, but not ISPs (Internet service providers).[456] However, "operators of the means of transmission that provide immediate user access to the Internet," such as DSL (digital subscriber line) connections, are also required to install the eavesdropping technology.[457] In Germany, the largest such operator is ‘Deutsche Telekom AG’, which is the former incumbent telecom provider, which is still majority-owned by the state.[458]

The proposals for surveillance regulations were set by the Government officials before September 11, but faced heavy criticism from the IT and telecom industry, which complained of the high cost of installing the required equipment.[459] However, industry representatives agreed to a compromise version of the regulations with the government officials.[460]

Not all industry concerns were addressed in the new version, said the IT industry association BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) in a statement, "but the regulation now presents an acceptable compromise between the legitimate interests of the state in surveillance of telecommunication and the Internet, on one side, and the technical and economic possibilities for the realization in practice on the other side."[461] BITKOM was particularly

---

[455] *Id*
[456] *Id*.
[457] *Id*.
[458] *Id*.
[459] *Id*.
[460] *Id*.
[461] *Id*.

relieved that the compromise version does away with plans for the wholesale surveillance of service providers, and instead focuses on user network connections, which the group said lightens the load for smaller network providers and ISPs.[462] But the privacy advocates were not easily pacified. Twelve human rights groups warned of the danger of a "surveillance state," citing the country's experiences with totalitarianism under the Nazi regime and East German communism.[463]

The privacy activists stated: "The balance between legally guaranteed citizen freedoms and the state's rights of encroachment must not -- as at present -- be abolished in the interest of abstract state security."[464] These activists include the Humanist Union, the German Association for Data Protection, and the hackers' group Chaos Computer Club.[465] They were addressing not only the eavesdropping rule, but also other proposed security measures including fingerprinting, the release of student records to police, and increased surveillance of foreigners.[466]

E. China.

There are limited rights to privacy in the Chinese Constitution, which are subject to broad exemptions for protecting state security.[467] China has a long-standing policy that keeps a close track of its citizens.[468] According to expert W.J.F Jenner, " The Chinese States by the fourth century BC at latest were often remarkably successful in keeping records of their whole populations so that they could be taxed and conscripted. The state

[462] *Id.*
[463] *Id.*
[464] *Id.*
[465] *Id.*
[466] *Id.*
[467] Banisar and Davies, s*upra* note 1 at 31.
[468] *Id.*

had the surname, personal name, age and home place of every subject and was also able to ensure that nobody could move far from home without proper authorization."[469] In September 2001, the Chinese police set up a computer system along the Chinese railway network that allows officers to compare the faces of suspicious passers-by to an electronic database of mugshots.[470] This was done ahead of a week-long holiday that began in October during which an estimated 64 million people were expected to be travelling across China.[471] Now when passengers come into and depart from Beijing Station, they have to pass through numerous checkpoints.[472] Anyone who acts or looks suspicious is taken to a computer terminal linked to a network of wanted law breakers.[473] At least four such terminals were installed in the plaza in front of Beijing Station.[474] Suspects are lined up and compared to photographs and other information on thousands of wanted criminals from around China.[475]

Since 1984, all Chinese citizens over the age of 16 have been required to carry identification cards issued by the ministry of Public Security.[476] Identification cards include name, sex, nationality, date of birth, address and term of validity, of which there are three: between the ages of 16 and 25, it is 10 years, between the ages of 25-45, it is 20 years and for those aged 45 and over it is permanent.[477] In carrying out their duties, public security organs have the right to ask citizens to show their identity cards.[478]

---

[469] *Id* at 32.
[470] Agence France-Presse, *Technology: Computerized dragnet helping police catch suspected felons in China*, The Nando Times September 28, 2001. *available at* http://www.nando.net/technology/story/110713p-1237406c.html.
[471] *Id*.
[472] *Id.*
[473] *Id.*
[474] *Id*.
[475] *Id.*
[476] Banisar and Davies, s*upra* note 1 at 33.
[477] *Id*.
[478] *Id*.

By mid-2003 all of Hong Kong's 6.8 million residents will be offered digital identity cards for use in secure online transactions when the authorities introduce a new "smart" national identity card.[479] This card will replace the existing national identity cards held by all Hong Kong residents for immigration and foreign travel purposes.[480] The new chip card is controversial because it will contain other applications in addition to identity details, raising privacy concerns.[481] The card has embedded computer chips that hold names, pictures and birth dates as well as a digital template of both thumbprints.[482]

F. France.

While ECHELON has gained widespread notoriety, there is evidence that European countries are also carrying out international surveillance.[483] France reportedly has developed its own "Frenchelon" which is a worldwide network of spy satellites and listening stations that systematically eavesdrop on communications in the United States and elsewhere.[484] Monitoring stations are said to exist in French Guiana, in the city of Domme in the Dordogne region of southwestern France, in New Caledonia, and in the United Arab Emirates.[485]

---

[479] Adam Creed, *Hong Kong Identity Cards to Include Digital Ids*, Newsbytes Hong Kong China 27 Dec 2001. *available at* http://www.newsbytes.com/news/01/173233.html.
[480] *Id.*
[481] *Id.*
[482] See http://www.wired.com/news/technology/0,1282,50961,00.html.
[483] Kenneth Neil Cukier, *Communications Week International*, "Frenchelon": France's Alleged Global Surveillance Network And its Implications on International Intelligence Cooperation.
available at http://home.arcor.de/kraven/miniwahr/frenchechelon.html.
Author Kenneth Neil Cukier is a senior editor and Paris correspondent for Communications Week International, covering the technology, economics and public policy of the Internet. His articles on cryptography have been entered into U.S. Congressional testimony and used by a Presidential Commission studying export issues. From 1992 to 1996 he worked at The International Herald Tribune in Paris.
[484] *Id.*
[485] *Id.*

The information collected is reportedly used for both political and commercial ends.[486] Additionally, some people speculate that the French project may mark the first step in a pan-European effort to counterbalance the U.S.'s global spying capabilities.[487] The French project is said to be run under the Direction Généralé de la Sécurité Extérieure, an organization similar to the United States Central Intelligence Agency, and commercial information it generates is sent directly to the presidents of large French companies as well as government officials.[488] The existence of French global surveillance, first publicized in June 1998 by Jean Guisnel of the French newsweekly Le Point, has not been officially confirmed or denied by the French government.[489] The lack of a denial has caused observers to speculate that such a program may exist.[490]

Unlike the ECHELON project, which has been publicly documented by the U.K. based human rights organization, Omega Foundation, in a report for the European Parliament's Scientific and Technological Options Assessment (STOA) unit in January 1998, there is no official evidence that France or any other European nation practices systematic surveillance of international civilian communications.[491]

However, a French official familiar with the France's system stated privately that such a program indeed exists, but at a "vastly smaller scale" than ECHELON.[492] The person claimed that ECHELON intercepts around 3 million messages per minute, while the French system intercepts roughly 2 million messages per month.[493]

---

[486] *Id.*
[487] *Id.*
[488] *Id.*
[489] *Id.*
[490] *Id.*
[491] *Id.*
[492] *Id.*
[493] *Id.*

CHAPTER 5

FUTURE PRIVACY ISSUES

Privacy is a very complex and vexing issue.[494] Solutions to the problem of privacy would be very easy to imagine but difficult to implement.[495] As between many privacy issues the privacy issue dealing with biometrics is especially alarming.[496] The biometric industry is booming and soon there will be a widespread adoption of biometric systems.[497] If for example, one form of biometric systems such as fingerprinting were adopted, the various databases containing the digitized versions of the prints could be combined.[498] While such a system is most likely to be developed by the commercial sector for use in financial transactions, the government would be likely to want to take advantage of these massive databases for other purposes, especially if a country were to enter a time of social unrest and instability.[499] The widespread implementation of video surveillance is harmful for several reasons.[500] We are growing more accustomed to video cameras watching our every movement.[501] We will soon reach a time when these cameras will be considered part of the furniture and will loose track of our civil and fundamental rights.[502]

---

[494] Willis H. Ware, *Contemporary Privacy Issues, available at* http://www.southernct.edu/organizations/rccs/resources/research/comp_and_priv/ware/future_priv.html#future.
[495] *Id.*
[496] Beth Givens, Director, Privacy Rights Clearinghouse, *A Review of Current Privacy Issues, available at* http://www.privacyrights.org/ar/Privacy-IssuesList.htm.
[497] *Id.*
[498] *Id.*
[499] *Id.*
[500] *Id.*
[501] *Id.*
[502] *Id.*

In the new world of electronic commerce, an emphasis is being placed on the establishment of mechanisms for authenticating the identity of an individual who wishes to engage in a transaction.[503] In order for electronic commerce to move beyond simple online credit card purchases, and into more complex transactions involving contracts or financing, some form of 'digital signature' mechanism is a certain development.[504] While such a signature would make new commercial transactions possible, it also raises significant privacy concerns, because if safeguards were not built into such a system, it would create permanent electronic tracks.[505]

The next emerging privacy issue would be the "smart card" proposals.[506] In assuming consumers will continue to sacrifice privacy for convenience, the creation of a single card or number, that combines commercial and government transactions requiring authentication, is a likely possibility.[507] There is increasingly rapid growth in wireless technologies.[508] Digital cell-phones are becoming smaller, cheaper and have more sophisticated features.[509] They can send and receive email messages, surf the internet and so on. The vision of many corporations and Internet start-ups is to be able to deliver location specific advertising to these cell phone devices.[510] So, if you're traveling through the city on a freeway, you might receive a message telling you that just off the next exit is a restaurant that serves your favorite food.[511] Or as you walk past Starbucks, you'll be

---

[503] The Honorable Bob Barr, *A Tyrant's Toolbox: Technology And Privacy In America,* 26 J. Legis. 71, 80 (2000).
[504] *Id.*
[505] *Id.*
[506] *Id.*
[507] *Id.*
[508] Givens, s*upra* note 489.
[509] *Id.*
[510] *Id.*
[511] *Id.*

flashed a message offering you a special on double lattes.[512] Cell phones must now be able to pinpoint the user's location to the nearest 100 feet for emergency assistance purposes.[513] If you are in a traffic accident, emergency vehicles can find you easily to administer assistance.[514] Unfortunately the cost of these conveniences and personal safety measures is personal privacy.[515] Our cell phones will continue to remain location-tracking devices.[516]

[512] *Id.*
[513] *Id.*
[514] *Id.*
[515] *Id.*
[516] *Id.*

CHAPTER 6

REMEDIES

The Privacy Act of 1974[517] attempted to strike a fragile balance between the government's need to gather and to use personal information and the individual's competing need to maintain control over such personal information.[518] In furtherance of these competing goals, the Privacy Act requires every federal agency maintaining a record on an individual within a system of records to: (1) permit the individual to control the use and dissemination of information contained in the record; (2) permit the individual to review, to correct, or to amend information contained in the record; (3) regulate and restrict the collection, maintenance, use, and dissemination of information in the record; and (4) be subject to civil suit for specified violations of the Privacy Act.[519] Collectively, these safeguards are designed to protect individual privacy, while preserving the government's ability to gather and to use personal information.[520]

The Privacy Act of 1974 attempts to strike a balance between the government's need to gather and to use personal information and the individual's need to exercise control over that information.[521] The balance, however, has never been achieved.[522] Instead, the

[517] Privacy Act of 1974, 5 U.S.C. § 552a(a)(1) (1988).
[518] Todd Robert Coles, *Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption*, 40 Am. U. L. Rev. 957, 965 (1991).
[519] *Id* at 966.
[520] *Id.*
[521] *Id* at 1001.
[522] *Id.*

Privacy Act has favored the government's desire for information at the expense of individual privacy.[523]

The best way to protect privacy is to give individuals the tools to do it themselves.[524] There should be a watch over the government's tendency to sacrifice people's privacy for other goals and perform government wide reviews of new federal programs for privacy violations before they're launched.[525] If the Government is implementing certain surveillance technologies, there should be notification of such surveillance to the citizens.[526]

Laws are needed that require improved computer security.[527] In 1970 Congress passed the Fair Credit Reporting Act, which gave Americans the previously denied right to see their own credit reports and demand the removal of erroneous information.[528] Elliot Richardson, who at the time was President Nixon's Secretary of Health, Education and Welfare, created a commission in 1972 to study the impact of computers on privacy.[529] The most important contribution of the Richardson report was a bill of rights for the computer age, which was called the 'Code of Fair Information Practices'.[530] "The code is based on five principles:

1. There must be no personal-data record-keeping system whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

---

[523] *Id.*
[524] Barr, s*upra* note 496 at 83.
[525] Simson Garfinkel, *Privacy And The New Technology, What They Know Can Hurt You, available at* http://past.thenation.com/cgi-bin/framizer.cgi?url=http://past.thenation.com/issue/000228/0228garfinkel.shtml (February 28, 2000).
[526] Barr, s*upra* note 496.
[527] Garfinkel, s*upra* note 518.
[528] *Id.*
[529] *Id.*

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Privacy is one of our most cherished freedoms, and today it is being suppressed by technology. The shape of our future will depend on how we deal with the present issues. I think the main remedies for privacy violations would how we control or regulate this threat to our freedom as we face it today."[531]

[530] *Id.*
[531] *Id*

CHAPTER 7

CONCLUSION

It is true that with the advancement in technology our society has become very interconnected and interdependent, making it difficult to have absolute privacy. But every society should also have its limits. Police technology invading our privacy rights would also have a detrimental effect on the mental health of a person.[532] It would increase the amount of stress in our lives, and we would be less free to disclose personal information in interpersonal relationships.[533] Computer profiling in the case of the Financial Crimes Enforcement Network[534] could raise equal protection issues.[535] FinCen searches use variables such as race, religion, gender and national origin.[536] The system might identify people as suspects on the basis of their names or surnames or national origin.[537]

But a major issue, which would justify the government in resorting to these measures, would be to combat the problem of terrorism. Terrorism had been employed for centuries as a means of forcing change through heightened diplomatic pressure and politically consequential violence without having to bear any responsibility.[538] Terrorism creates fear and thus undermines the confidence of society.[539] Essentially terrorism has three effects: An immediate effect of killing or injuring those who are deemed a

---

[532] *Id*.
[533] *Id*.
[534] *See* chapter 3 (A).
[535] *Id* at 420.
[536] *Id.*
[537] *Id*.
[538] Seth R. Merl, *Internet Communication Standards For the 21st Century: International Terrorism Must Force the U.S. To Adopt "Carnivore" and New Electronic Surveillance Standards,* 27 Brook. J. Int'L. 245, 248 (2001).

prohibited target; an intermediate effect of intimidating the larger population therefore influencing their political behavior; and an aggregate effect of undermining overall public order.[540] With the recent terrorist attacks on the United States and around the world, the government is justified in enforcing new measures in order to ensure our safety. In my country, India, terrorism has been a problem for years and if I had a choice to chose between my privacy on one hand and my safety on the other, without hesitation, I would choose the latter. But at the same time there has to be a balance struck somewhere in the middle.[541] We need to protect our privacy and also support law enforcement by utilizing new technologies specifically designed to keep our countries safe from thieves, criminals and terrorists.[542]

Ever since I became interested in the issue of privacy, I always remember the novel '1984' written by George Orwell.[543] In his novel, Orwell envisioned that by the year 1984, a totalitarian government would rule the world. In his novel, he described a society where there were cameras in people's homes and in their work places. The surveillance was so powerful to the extent that the government controlled people's thoughts. People were constricted in their acts and could not lead a normal healthy life. There was a famous caption that was used repeatedly throughout the novel: "BIG BROTHER IS WATCHING YOU". Big Brother signifies the government. The totalitarian world envisioned by Orwell never became a reality, but in essence he is trying to let people know that they should be aware of what is going on around them. We have

---

[539] *Id.*
[540] *Id.*
[541] See Lewis, s*upra* note 169.
[542] *Id.*
[543] George Orwell, 1984 (1948).

certain fundamental rights, which are very precious to us, and I think these rights should never be taken away.

BIBLIOGRAPHY

1. David Banisar and Simon Davies. Global Trends in Privacy Protection: An International Survey of Data Protection, and Surveillance Laws and Developments. 18 J. Marshall J. Computer & Info. L. 1,1 (1999).

2. Kent Walker. Where Everybody Knows Your Name: A Pragmatic Look At The Costs Of Privacy And The Benefits Of Information Exchange. 2000 Stan. Tech. L. Rev.2, 3 (2000).

3. Carol M. Bast. What's bugging you? Inconsistencies And Irrationalities Of The law Of Eavesdropping. 47 DePaul L. Rev. 837, 881 (1998).

4. William C. Hefferman. Privacy Rights. 29 Suffolk U. L. Rev. 737, 746 (1995).

5. Moore v. New York Elevated R.R. Co. 130 N.Y. 523, 29 N.E. 997 (1892).

6. Griswold v. Connecticut. 381U.S. 479 (1965).

7. Roe v. Wade. 410 U.S. 113 (1973).

8. Whalen v. Roe. 429 U.S. 589 (1977).

9. Bowers v. Hardwick. 478 U.S. 186 (1986).

10. Michael Froomkin. The Metaphor is the Key, Cryptography, The Clipper Chip, And the Constitution. 143 U. pa. L. Rev. 709, 712 (1995).

11. Ruth Gavison. Privacy and the Limits of Law. 89 Yale L.J. 421, 433 (1980).

12. Irwin R. Kramer. The Birth Of Privacy Law: A Century Since Warren and Brandeis. 39 Cath. U. L. Rev. 703, 703 (1990).

13. Christopher S. Milligan. Facial Recognition Technology, Video Surveillance, and Privacy. 9 S. Cal. Interdisciplinary L.J. 295, 312 (1999).

14. Gerald K. Freund. Look Up In The Sky, It's a Bird, It'd a Plane...It's Reasonableness. 20 Sw. U.L. Rev.195, 198 (1991).

15. Stephen P. Jones. Reasonable Expectations of Privacy: Searches, Seizures, And The Concept Of The Fourth Amendment Standing. 27 U. Mem. L. Rev. 907, 908 (1997).

16. Melvin Gutterman. A Formulation Of The Value and Means Models Of The Fourth Amendment In The Age Of Technologically Enhanced Surveillance. 39 Syracuse L. Rev. 647, 649 (1988).

17. Richard S. Julie. High-Tech surveillance Tools And The Fourth Amendment: Reasonable Expectations of Privacy In The Technological Age. 37 Am. Crim. L. Rev. 127, 128 (2000).

18. Olmstead v. United States. 277 U.S. 438, 48 S.Ct. 564 (1928).

19. Madeline A. Herdrich. California v. Greenwood: The Thrashing Of Privacy. 38 Am. U. L. Rev. 993, 1001 (1989).

20. United States v. Chadwick. 433 U.S. 1, 97 S.Ct. 2476 (1977).

21. United States v. Gerend. 662 F.Supp.1218,1218 (D.Conn. 1987).

22. United States v. Anderson 8598 F.2d 1171, 1177 (1988).

23. Rawlings v. Kentucky 448 U.S. 98, 106 (1980).

24. Rakas v. Illinois, 43 U.S. 128, 152 (1978).

25. California v. Hodari. 499 U.S. 621 (1991).

26. Arizona v. Hicks, 480 U.S. 321, 328 (1987).

27. Florida v. Riley. 488 U.S. 445 (1989).

28. Steven A. Bercu. Towards Universal Surveillance In An Information Age Economy: Can Police Handle Treasury's New Police Technology?. 34 Jurimetrics J. 383, 383, 384 (1994).

29. Joel Feinberg. Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?. 58 Notre Dame L. Rev. 445, 453 (1983).

30. Robert Puterski. The Global Positioning System—Just Another Tool?. 6 N.Y.U. Envtl. L.J.93, 94 (1997).

31. Richard C. Balough. Global Positioning System and the Internet: A Combination With Privacy Risks. 15-OCT CBA Rec. 28, 28 (2001).

32. Dorothy J. Glancy. Privacy and Intelligent Transportation Technology. 11 Santa Clara Computer & High Tech. L.J. 151, 153 (1995).

33. Charlene L. Lu. Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy With the Need for Effective Law Enforcement. 17 Hastings Comm/Ent L.J. 529, 532 (1995).

34. Michael Froomkin.The Death of Privacy?. 52 Stan. L. Rev. 1461, 1479 (2000).

35. Kurt Wimmer. Privacy and Mobile Telecommunications. 19_SUM Comm.Law. 20, 20(2001).

36. Matthew Mickle Werdegar. Lost? The Government knows where you are: Cellular Telephone Call Location Technology and the Expectation of Privacy. 10 Stan. L. & Pol'y rev. 103,103 (1998).

37. Amy M. Intille. Video Surveillance and Privacy: Implications for Wearable Computing. 32 Suffolk U. L. Rev. 729, 751 (1999).

38. Andrew Jay Mcclurg. Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places. 73 N.C. L. Rev. 989, 1022 (1995).

39. Bob Barr. A Tyrant's Toolbox: Technology and Privacy in America. 26 J. Legis. 71, 72 (2000).

40. Daniel J. Polatsek. Thermal Imaging and the Fourth Amendment: Pushing the Katz Test Towards Terminal Velocity. 13 J. Marshall J. Computer & Info. L 453, 453 (1995).

41. Mindy G. Wilson. The Prewarrant Use of Thermal energy: Has this Technological Advance in the War Against Drugs Come at the Expense of Fourth Amendment Protections Against Unreasonable Searches?. 83 Ky. L.J. 891, 892 (1995).

42. Mark J. Kwasowski. Thermal Imaging Technology: Should Its Warrantless Use By Police Be Allowed In Residential Searches?. 3 Tex. Wesleyan L. Rev. 393, 394 (1997).

43. John Lewis. Carnivore - The FBI's Surveillance System: Is It A Rampaging E-mailasaurus Rex Devouring your Constitutional Rights?. 23 Whittier L. Rev. 317, 317 (2001).

44. Vijayashri Sripati. Human Rights in India – Fifty years After Independence. 26 Denv. J. Int'l L. & Pol'y 93, 98 (1997).

45. Kevin Reis. The Eavesdropping Society: Electronic Surveillance And Information Brokering. 632A PLI/Pat 627, 631 (2001).

46. Todd Robert Coles. Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption. 40 Am. U. L. Rev. 957, 965 (1991).

47. Seth R. Merl. Internet Communication Standards For the 21st Century: International Terrorism Must Force the U.S. To Adopt "Carnivore" and New Electronic Surveillance Standards. 27 Brook. J. Int'L. 245, 248 (2001).

48. George Orwell, 1984 (1948).