Privacy in the Internet Environment

Terrence P. McGarty[1]
The Telmarc Group

Abstract

Privacy is a complex issue and the Internet takes this issue and compounds it in many ways. In this paper we take the issue of privacy, examine it in terms of current laws, US and European, and then examine the impact of the Internet on the broadly defined issue of privacy. This paper evaluates the various definitions of privacy and at the same time examines how the Internet presents both a threat to these "rights" and an opportunity to expand these rights and to sustain them in a global economy and environment of living.

Contents

[1] Dr. McGarty is also associated with the MIT ITC Consortium as a member of the Steering Committee of this Program at the Institute and is actively involved with the Institute in various elements of this program. This paper is a direct result of his efforts in that program.

INTRODUCTION

In the United States today, if an individual desires to fly between New York and Boston, then the individual must present their passport at the airport to secure passage. No other country in the world requires that its citizen, or even a foreigner, present "papers" for intra-country transport. The proposal is to do the same for trains. It is already done for auto rentals. At bridges and toll booths in most of the US today, silent monitoring devices which the citizens have paid for and installed in their autos monitor their movement along highways, measuring the speed through toll booths and even measuring the speed on the highway in a silent and unseen fashion. These changes were already in effect or in process before September 11, 2001 when the United States was deliberately and viciously attacked by Muslim forces. The commencement of the war on September 11, 2001, albeit not with Marshal law orders, gives the Government an additional leverage point to seek more control on private lives. But that control is in the context of security, questionable that it may be given the less than sterling performance of U.S. security forces.[2]

Companies such as General Electric are proposing "smart" appliances which would have IP addresses and in effect be elements of the Internet. GE could then monitor, on a real time basis, the opening and closing of refrigerators during TV commercials, could in conjunction with placing such "smart" appliances in conjunction with companies such as @Home, determine who is eating between commercials and how frequently this is done. This then can be correlated with a persons health records, and via a smart appliance in the auto installed by General Motors, the weight of the person may be determined each morning.

Microsoft and Intel has actually placed special codes in software and hardware respectively that allows for IP addressing and for the identification of any user at any time. The placement of "cookies" in anyone's computer allows the placer to monitor the behavior of that erstwhile customer whenever they so desire.

There are old principles of privacy that go beyond what we now, especially in the US, understand as privacy. The old principles are those of anonymity. That is the "right to be left alone". For many generations in the US one could refuse to identify oneself in any way unless arrested. The first exception to that was the set of laws passed in 1942 in California that made it a crime to fail to provide police identification if approached. This was an outgrowth of Pearl Harbor and the threat of the supposed, and quite real, Japanese invasion of the west coast. The law staid on the books for almost half a century.

Roe v. Wade entered and greatly expanded but also confused the privacy issue by following on Griswold which allowed for private actions, not just the ability to conceal my identity. There was in the eastern part of the US the assumed "right" of anonymity. One could take money, species or any other form, enter a transaction without identifying oneself and consummate the transaction in a totally anonymous fashion. One, in effect, had a "right to be left alone". The United States today, especially in the last seven years, has changed dramatically. The US government is seeking and effecting ways to monitor and have access to all of ones transactions, communications, especially on the Internet, and in many ways all of ones private life, despite Fourth Amendment protections, which have been broadly interpreted to effectively protect non-electronic analogs of what the Government is now invading. In fact, the US Government is proposing insuring that the "right to be left alone" in the Internet be eliminated, that it, and in many cases it alone, has the ongoing ability to penetrate each persons most hidden acts, be it email, Web searches, or electronic transactions. These are all being done in the name of national security.

[2] For example, Secretary of Transportation, refuses to apply Bayes analysis on potential threats since such use of a priori data would in his mind constitute racial profiling. Bayesian analysis has a long and successful history in various fields, most notably in intelligence, in fact it is the cornerstone of intelligence. Thus Mineta would potentially infringe on everyone rights rather than use the facts and target the threats. The issue is that the Constitution guards us via probable cause. If we let such probable cause be reduced to nothing by adhering to the principles of non-profiling, then we lessen all our rights.

This paper addresses three questions: (i) what is the definition of privacy, and (ii) what rights do we have to privacy and from whence are they derived, and (iii) what does privacy mean in an electronic world such as the internet environment and how do we relate what we know in the physical world to the electronic world? These are three simple but at the same time highly complex questions. The Supreme Court only recognizes sexual behavior to be governed by privacy rights. However, privacy is so broad a concept that Justice Brandeis in his famous paper with Weaver stated that it was the "right to be let alone". In other dimensions it is viewed as a more fundamental right of natural law, common law, constitutional law, tort law, and actual laws as may be promulgated by the Legislative bodies.

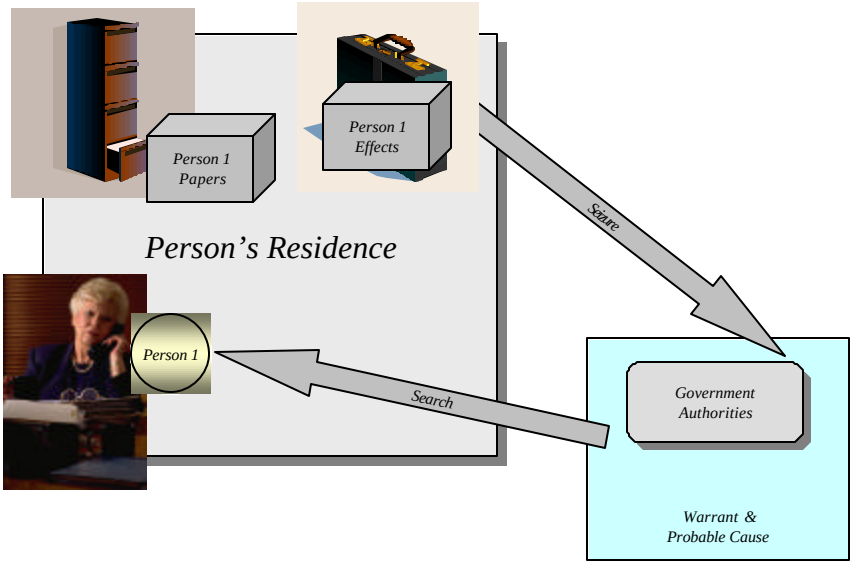
PRIVACY AND ITS LEGAL ELEMENTS

Privacy has several legal basis. Each basis has a different definition. We start with the three most common bases; Constitutional, Laws, and Torts. Constitutional basis is what has been granted by the US Constitution, generally the Bill of Rights. The Law or Legal basis is what has been expressly granted by laws passed. The Tort basis is generally what has been granted via litigation.

1.1 Constitutional

The Constitution grants certain rights, mostly via the Bill of Rights and the additional amendments to the Constitution. Consider the Fourth Amendment. The following figure shows what is generally accepted under the Fourth Amendment protections. Namely, in one's home, one is safe from "unreasonable searches and seizures", namely those done without a warrant, such warrant requiring probable cause of a crime, and this process is called due process. The Fourteenth Amendment extends this from the Federal Government to the State Governments.

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.



The Constitution does not say that the government cannot search and seize, it says that it must follow a process to do so. That process is carefully controlled and should not be abused. If we take the simple figure shown above, we have several elements; person, person's residence, person's papers, persons' effects. We then also have due process, which is probable cause and a warrant issued thereto. It is real simple. But it is not. If we review the Supreme Court cases, as shown in Appendix B we see that there are many ways to extend or delimit each of these concepts. For example, if I am in my house that is one thing, if I am on a street

corner at 3 in the morning looking at a jewelry store that may be quite another. There is also the issue of what constitutes a search and what constitutes a seizure.

Since we do not have a well defined set of terms in the world of tangibles, then how do we expect the world of intangibles to be well understood. The recent Supreme Court ruling on Verizon v. FCC on May 13, 2002 has the Court opining on such issues as TELRIC pricing, Ramsey efficiency, and interconnection and unbundling policy. Since most economists are captives of the incumbent monopolists, one wonders how nine individuals who are unlikely to place their own phone calls can reach any logical conclusion on such an issue. In fact this opinion is a clear example of what one may expect from the Court if it expands to the cyber domain, especially since so many interest are involved.

There are certain Constitutional rights that we have as American citizens, and also possibly as resident aliens, in the United States. The one most favorable to privacy is the Fourth Amendment to the Constitution as follows:

Article IV. : 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.

We can see how these have evolved in four areas.

Privacy

The following is a summary of key Opinions in this area:

Griswold v Connecticut 381 U.S. 479 1965[3]*:* Griswold was the Executive Director of Planned Parenthood in CT. CT had a law against selling or prescribing contraceptive devices. PP sued CT to be able to provide birth control methods to the CT citizens, and in this case specifically a husband and wife. The Court first granted that the married couple, part of Griswold et al, had standing to assert a constitutional right and second that the CT law violated the right of marital privacy which was covered by the penumbra of the Bill of Rights. Justice Douglas states*: "In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion."* and also *"The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…"*

Roe v Wade 410 U.S. 113 1973: Roe is the classic case. She was pregnant and brought a class action suit against the constitutionality of the Texas law which made abortions illegal. Justice Blackman rendered the opinion. Roe claimed that she had protection under the 1st, 4th, 5th, 9th, and 14th Amendments. The Court stated that the Texas act was unconstitutional The claimant used Griswold and the penumbra theory under the 14th Amendment.

Bowers v Hardwick 478 U.S. 186 1986: Justice White delivered the decision. Charged with violating the Georgia law of sodomy with another adult male in the bedroom of his home, respondent Hardwick (respondent) brought suit in Federal District Court, challenging the constitutionality of the statute insofar as it criminalized consensual sodomy. The court granted the defendants' motion to dismiss for failure to state a claim. The Court of Appeals reversed and remanded, holding that the Georgia statute violated respondent's

[3] Cantor describes the penumbra theory developed in Griswold as having an origin in law in Cicero and having a general origin in principle in Plato. See Cantor p. 22.

fundamental rights. The Supreme Court upheld the Georgia Court. The Court focused on the filed brief and stated that the States have rights to create laws.

Search

Boyd v U.S. 116 U.S. 616, 1886: This was a case resulting from a Customs search and subsequent demand by the law authorities for certain documents that The district attorney in New York ordered the defendant to produce invoices showing certain plate glass was imported illegally, against the 1874 Customs Act. The defendants complained about the constitutionality of the law. Ruling summarizes prior cases and laws. States 1789 statute for custom duty collection as stating that searches for Customs violations are permitted. Court used this reference since it was same Congress which passed Bill of Rights (original intent). Court goes o to stress the Colonial opposition to English writs of assistance which empowered English to have warrantless searches. The Court details John Adams opposition to this and further strengthens the original intent of the framers as opposing warrantless searches and seizures. Court refers again to 1789 Custom Act and restates acts restriction "cases and circumstances where they might be compelled to produce…by the ordinary rules of proceeding.." Court further states that "any compulsory discovery…or compelling the production of …books and papers…is contrary to the principles of a free government. It is abhorrent.." Court overthrew the ruling and remanded case.

Carroll v U.S. 267 U.S. 132, 1925: This case concerned the search of a vehicle without a warrant in an attempt by the police to discover liquor in violation of prohibition. The police suspected that the defendant was involved in some form of bootlegging, but the stop occurred some time after their initial suspicions, with no further evidence having been obtained in the interim. In the early days of the automobile the Court created an exception for searches of vehicles, holding in Carroll v. United States 55 that vehicles may be searched without warrants if the officer undertaking the search has probable cause to believe that the vehicle contains contraband. The Court explained that the mobility of vehicles would allow them to be quickly moved from the jurisdiction if time were taken to obtain a warrant. Thus the Court upheld the conviction and made a distinction based upon the auto as the element being searched.

U.S. v Di Re 332 U.S. 581, 1948: This case referred to a defendant possessing illegal gas rationing coupons. The police had prior knowledge that certain persons would be carrying and trafficking in illegal gas ration coupons. The defendant was stopped in a vehicle and one of the passengers held the coupons in plain view to the police officers. DiRe was taken out of the auto and frisked and the coupons were found on his person. The driver, Reed, was the suspect and the police had no knowledge of Di Re. The Court reviewed Carroll and stated that Carroll seemed to imply that warrantless searches were appropriate for an auto. The Court made a distinction here about Carroll allowing an auto search and the DiRe case of a search of the person. The Court states: We are not convinced that a person, by mere presence in a suspected car, looses immunities from search of his person to which he would otherwise be entitled." The conviction was overturned.

Terry v Ohio 392 U.S. 1, 1968: Police officer sees a group of men acting suspiciously. Based upon that observation he then stops and frisks them. He finds a weapon, upon which discovery they are arrested. The men object on Fourth Amendment grounds of an unlawful search and seizure. The observation lacks probable cause but the "stop and frisk" is not a seizure and a search under the Fourth Amendment. The Court views "stop and frisk" as separate from "search and seizure". The stops based upon police officers experience and the frisk is for the safety of officer and public and limited to the "discovery" of weapons. The Court justifies "stop and frisk" as follows*: "This scheme is justified in part upon the notion that a "stop" and a "frisk" amount to a mere "minor inconvenience and petty indignity…"* The Court stated: "*In our view the sounder course is to recognize that the Fourth Amendment governs all intrusions by agents of the public upon personal security, and to make the scope of the particular intrusion, in light of all the exigencies of the case, a central element in the analysis of reasonableness*." The conviction stood.

U.S. v Ross 456 U.S. 708, 1982: Justice Stevens delivered the Opinion. In this case a police officer obtained a tip stating that a certain person was selling narcotics. In fact the information stated that the individual had

just completed a sale. The informant detailed the perpetrator and his vehicle. The police did a check on possible perps and found the defendant. The fund the defendant and then the police took defendants keys and opened trunk. A bag was found in trunk and in the bag was cash and on the bag was narcotics. The Court of Appeals reversed the decision. The Appeals Court used Carroll to stated that the police could search trunk but not the bags. The Court restated the Opinion Carroll that a warrantless search of an automobile stopped by police officers who had probable cause was not unreasonable under the 4th Amendment. In fact the limitation is on "unreasonable" search and seizure. The Court also again reiterated the fact that the Founding Fathers themselves made a distinction of warrants for homes but warrantless for vessels, thus vehicles. The Court ruled that the police could do a warrantless search based upon the long standing fact that the Court had recognized the impracticality of securing a warrant in cases involving a vehicle. The Appeals Court decision was overturned and the search and its fruit permitted.

Wyoming v. Houghton Wyo. 98-184, 1999: This recent case involves a routine traffic stop. At the stop the police officer notices a hypodermic syringe in plain view in the driver's pocket. The driver admitted to taking drugs. The police officer then searched the glove compartment. There he found drugs. The Court upheld the conviction by establishing that the police had probable cause. The cases used were Carroll and Ross as described above.

Wiretapping

Olmstead v U.S., 277 U.S. 438, 1928: Justice Taft delivered the decision. Olmstead was a leading conspirator in a bootlegging ring. He moved liquor from Canada to the US. The police put taps on the telephone lines of all the conspirators. The taps were placed outside of the homes and were done without warrants. The information gathered from the taps were used to convict. The Court stated: "The court held the Act of 1874 repugnant to the Fourth and Fifth Amendments. As to the Fourth Amendment, Justice Bradley said [277 U.S. 459] *"Concurring, Mr. Justice Miller and Chief Justice Waite said that they did not think the machinery used to get this evidence amounted to a search and seizure, but they agreed that the Fifth Amendment had been violated. But, in regard to the Fourth Amendment, it is contended that, whatever might have been alleged against the constitutionality of the acts of 1863 and 1867, that of 1874, under which the order in the present case was made, is free from constitutional objection because it does not authorize the search and seizure of books and papers, but only requires the defendant or claimant to produce them. That is so; but it declares that, if he does not produce them, the allegations which it is affirmed they will prove shall be taken as confessed. This is tantamount to compelling their production, for the prosecuting attorney will always be sure to state the evidence expected to be derived from them as strongly as the case will admit of. It is true that certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting, and, to this extent, the proceeding under the Act of 1874 is a mitigation of that which was authorized by the former acts; but it accomplishes the substantial object of those acts in forcing from a party evidence against himself. It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure.""* Olmstead v. United States, 32 one of the two premises underlying the holding that wiretapping was not covered by the Amendment was that there had been no actual physical invasion of the defendant's premises; where there had been an invasion, a technical trespass, electronic surveillance was deemed subject to Fourth Amendment restrictions.

Berger v New York 388 U.S. 41, 1967: Justice Clark delivered the Opinion. Berger was convicted in bribery of a government official. A bar owner had complained that officials from NY State Liquor Board had entered his bar and without cause seized his books. The bar owner said it was in reprisal for failing to pay bribe. On this basis an wire tap was authorized by NY court for 60 days on the office of official. Based on wiretap evidence the warrant was extended. Evidence was obtained on two other bars being shaken down. Defendant stated that this information was not legally obtained since the warrant was for evidence on the first case. Court ruled that this was un-constitutional. The warrant was too broad in scope.

Katz v U.S., 389 U.S. 347, 1967: Justice Stewart delivered the Opinion. The defendant was convicted for a violation of the wagering acts. The FBI recorded his calls without a warrant by attaching a recording device on the outside of a telephone booth. The defendant tried to pose the following two questions: *"A. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth. [389 U.S. 350] B. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution."* The Court rejected this posing. The Court stated: *"The Government stresses the fact that the telephone booth from which the petitioner 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. But what he sought to exclude when he entered the booth was not the intruding eye -- it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen…. To read the Constitution more narrowly is to ignore the vital role that* the *public telephone has come to play in private communication."* Further; *"What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*." Finally the Court states: "*Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored "the procedure of antecedent justification . . . that is central to the Fourth Amendment,"{ 24} a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case*.." The Fourth Amendment protects people, not places.

Civil Rights

NAACP v Alabama 357 U.S. 449, 1958: The case was about Alabama trying to force the NAACP to disclose its members list as a part of registering in Alabama. The Court said: "*This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said in American Communications Assn. v. Douds, supra, at 402: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order.* ***Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs****."*

The key to these Opinions is how do we transfer them from the physical worlds to the electronic world of the Internet and Data world. There is some insight in what we see in the wiretapping cases, this may extend to these new domains.

1.2 Laws

The laws on privacy are of recent construction and introduction. They are generally Federal but now there are many state laws in the same area. Mell states the following:

"Between 1966 and 1990, several federal statutes dealing with personal privacy were enacted by Congress. These statutes were the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, the Family Education Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Privacy Protection Act of 1980, the Paperwork Reduction Act of 1980, the Computer Matching and Privacy Protection Act of 1988,249 and the Video Privacy Act of 1994. While the Freedom of Information Act of 1994251 was enacted to provide access to files held by the government, the parameters of its disclosure provisions and its exemptions from disclosure have operated to provide privacy of sorts to the individual."

The statutes have had mixed results in defending the individual's privacy. While each of these statutes is diagrammed in the Appendix, a brief overview of their respective purposes is provided here.[4]

The Freedom of Information Act (FOIA) makes federal records available for inspection and copying by the public. Its ostensible policy is that citizens should be able to find out what their government is doing. FOIA has several exemptions, one being that information should not be disclosed when such action would constitute a clearly unwarranted invasion of privacy.

The Fair Credit Reporting Act (FCRA) was the first piece of federal privacy legislation designed to regulate the disclosure of information held by the private sector. FCRA was touted as offering three basic forms of privacy protection to the consumer. First, it limits disclosure of reports on individuals to companies with a legitimate business need for the information. Second, it requires that organizations which provide credit or investigative reports to third parties also make their records available to the subject of the report. Finally, it mandates procedures for the correction of errors in reports.

The Privacy Act (PA) was enacted to protect the confidentiality of individuals about whom a government agency held a file containing personal information. Like FCRA, it provides the individual with access to information stored about him and establishes procedures for the correction and amendment of these files. It also attempts to limit the government's ability to disclose the information to third parties.

The Privacy Protection Act (PPA) limits the procedures by which the government can gain access to the files held by newspaper agencies.

The Family Education Rights and Privacy Act (FERPA) limits the ability of schools and colleges to disclose student records to third parties. It also requires the school or college to provide the student access to such records and provides procedures for challenging the accuracy of and amending student records. This law has recently come under sever criticism in the light of student suicides, especially the one at MIT. The issue here is the old standard of in loco parentis and what role the University has in replacing the parents, acting for the parents, or in allowing the student freedom to do whatever they like independent of the parents.

The Right to Financial Privacy Act (RFPA) gives bank customers a limited expectation of privacy in their bank records by requiring that law enforcement officials follow certain procedures before any information can be disclosed. Recent Supreme Court cases have stipulated that checks are the banks property and not the individuals and that there is no expectation of privacy, express or implied, in one bank records.

Despite the apparent scope of coverage of these statutes, the actual protection afforded the individual's privacy varies greatly from one to the next. The number of statutes passed, each an attempt at protecting "privacy," partially explains society's failure to design a coherent policy regarding the aspects of personal information needing protection.

In addition, Mell has summarized the Privacy laws in terms of what their attributes are and in terms of comparing one to the other. These are contained in Appendix A. The US Privacy laws summarized are as follows:

[4] These are due to Mell and are contained in the paper referred to.

Act	*Interest Protected*
Privacy Act of 1974 (PA), 5 U.S.C. § 552a (1994)	Amends Freedom Of Information Act to: 1) give individual right to request access to records about him; 2) prevent agency disclosure of personal information to third parties without subject's consent. Information must 1) be relevant to the agency's use; and 2) must inform the individual whether collection is mandatory or voluntary.
Computer Matching and Privacy Protection Act of 1988 (CMPPA), 5 U.S.C. § 552a(o) (1994)	Amends Privacy Act to limit the collection of information from individuals. Provides guidelines for matching data about the same individual between agencies.
Paperwork Reduction Act (PRA), 44 U.S.C. §§ 3501-3520 (1988)	Limits collection of information from individuals, and saves government money. Relates to information collection requested of government agencies.
Privacy Protection Act of 1980 (PPA), 42 U.S.C. §§ 2000aa - 2000aa - 12 (1994)	Establishes procedures allowing police to obtain information from newspapers.
Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. §§ 3401-3422 (1994)	Regulates manner that government gains access to bank records about individuals.
Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g (1994)	Amends the Privacy Act and limits disclosure of student records to third parties. Records maintained by any educational institution receiving federal funds. Consent generally required before disclosure made to a third party. Denial of federal funding to the institution, but no individual cause of action.
Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. §§ 1681-1681t (1994)	Limits the disclosure of "consumer reports" or "investigative consumer reports" to third parties (i.e., "users") by "consumer reporting agencies" (CRAs).
Video Privacy Act (VPA), 18 U.S.C. § 2710 (1994)	Prevents "videotape service provider" from disclosing personally identifiable information concerning individual's tape selection to third parties.
Freedom of Information Act of 1966 (FOIA), 5 U.S.C. § 552 (1994)	Promotes open government by disclosing information relating to the workings of government. Only records indexed in a particular manner need be disclosed.

1.3 Torts

Tort law is a complex collection of precedents and processes. It is in many ways uniquely American. To a European it is a mess that reflects the litigious structure of the American legal system. In fact it is an almost unique way in which Americans directly and personally may “change” or “create” new laws, via the process of litigation and precedents. Americans have a republican representative form of government wherein the

Congress enacts laws and the President and the executive effect them in practice. The legal system in the United States, via the tort process, allows that each individual may in effect create their own laws, by filing suit, using precedents, and creating new precedents. The new precedents have the full force of law going forward. The process may be complex but it works and again in many ways empowers American citizens with the ability to make small but clearly perceptible changes in the laws and seek and obtain remedies not readily available to them under the law. The tort system fills the cracks of the written law.

In the area of privacy the tort of privacy was not to be found. Torts dealt with land, assault, or some physical interaction between two or more people. The classic start is considered to be the work of Cooley, his book on Torts, Torts, 2nd Edition, 1888. He established the concept by phrasing privacy as "the right to be let alone".[5]

The classic paper by Warren and Brandeis in 1890 established a more detailed framework for privacy, again along the lines of "being let alone".

Prosser has written in his book of Torts extensively concerning privacy. As we have discussed above, Tort protection is based on precedents in the law and not upon specific laws passed by Congress or the States. There is also the standard, used a reference, not precedent, the Restatement of Torts, which gives sum and substance to the torts as if they were laws, which they are not.

Prosser enumerates the following torts as applied to privacy:

Appropriation[6]: This is the appropriation for the defendants benefit of the plaintiff's name or likeness. This is typically the using of the plaintiffs image or likeness to the benefit of the defendant. Thus a person may sue on a tort basis of appropriation and prevent the defendant from using any picture or likeness.

Dobbs discusses how this relates to certain first Amendment rights but generally commercial speech is less protected and the issue of appropriation is related to commercial speech in general.[7] The issue of identity theft however is totally different. This is a criminal offense and is separate from the tort issue.

Unreasonable Intrusion[8]: As Prosser states "*…consist of intentional interference with another's interests in solitude or seclusion, either as to his person or to his private affairs or concerns..*" This typically is a result of someone rifling through another's belongings, trespassing on their property, but has been extended to listening to private conversations, peering in windows, and the like.

This may be a bit more difficult to prove.[9] A classic case was one where a physician brought a non-physician into a delivery room while a woman was giving birth. This tort is beyond trespass or Fourth Amendment rights (limited to the government only). The general rule is that an employer may have access to its employees records. However, certain states have established laws protecting those records. The issue here is that unreasonable intrusion is limited by the personal sphere, which itself may have limits. Clearly the home is a part of the sphere, the delivery room may be part, but the office may clearly not unless established otherwise by law.

---

[5] Prosser, p. 849.

[6] Prosser, p. 851.

[7] Dobbs, p. 1198.

[8] Prosser, p. 854.

[9] Dobbs, p. 1200.

Public Disclosure of Private Facts[10]: This is the telling of private facts about someone to another person or persons. There are essentially four elements; (i) the disclosure must be public, (ii) the facts must be private, (iii) the facts made public must be highly offensive to a reasonable person, and (iv) the public must not a legitimate interest in the information. As Prosser states, " the law is not for the protection of the hyper sensitive".[11]

This is no defamation. The truth of the facts is irrelevant under this claim. The issues are not necessarily at conflict with the First Amendment. Clearly if the information is wrongfully obtained it becomes tainted and cannot be used. In fact, even lawfully obtained public information, may, under this tort be actionable.[12]

False Light in the Public Eye[13]: This tort is the public placing of the plaintiff in a highly unfavorable and possible objectionable light. This may be the entering of the plaintiff into some contest as the ugliest duckling, or as the longest eared person, or some other unfavorable presentation. It may include the statement that the person has stated that he said some statement which is abhorrent.

This has four elements: (i) publication to a substantial group or the public, (ii) the information puts plaintiff in false light, (iii) the false light would be highly offensive to a reasonable person, and (iv) the defendant knew it to be false or acted with recklessness.[14] This may not be defamation, it may be false but may not reach the level of defamation. The Supreme Court has ruled from time to time on this issue of false light and libel. Libel has better standing but false light has remained in most jurisdictions.

In summary, the tort protections protect the individual from intrusions, from misrepresentations, from the telling of private facts, and from the taking of an identity or parts related thereto. The torts relate to the person, and indirectly to the persons property. They reemphasize the concept of the "right to be let alone".

1.4 Limitations

The laws have certain protections. These protections range from legal limitations placed by law upon the authorities, Constitutional protections granted in the Constitution such as due process, and tort protections that act to protect against non governmental entities. One should always remember that the Constitution protects us as citizens from the over reach of the Government, but in no way protects us from the over reach of other citizens. The latter is protected by laws and torts.

1.5 Due Process

Due Process means simply that the government cannot invade privacy or person, papers, or effects without probable cause and obtaining a warrant. There are certain exceptions, generally those relating to "inspections" for customs duties. The extent of this due process may vary. In the "*Terry*" search a warrant to "stop and frisk" is not necessary if the officer has reasonable suspicion regarding the person involved.

1.6 Substantive Due Process

[10] Prosser, p. 856.

[11] Prosser p. 857.

[12] Dobbs, p. 1205, see California Supreme Court ruling on Melvin v Reid.

[13] Prosser, 863.

[14] Dobbs, p. 1208.

Substantive due process is a heavy burden, it means that the matter at hand requires the government to go the extra mile. The private lives of people generally fit that category as discussed in *Griswold* or *Roe v Wade*.

SCHOOLS OF THOUGHT

This section deals with the several concepts of some key thinker in the area of privacy or the prohibition thereof. Brandeis is the first in the US who with his partner Warren wrote a detailed treatise in the Harvard Law Review on privacy and its meaning and basis in law.[15] Etzioni in contrast takes a communitarian view that we should have no privacy, it is a socialistic or communistic view, called Communitarianism, which propose national identity cards, openness of health records, and the general openness of all private items for the "good" of the state. Etzioni is not as extreme as one can get but he clearly represents the thought pattern of many left wing liberals in the United States. The most recent is the dictates of Ellison of Oracle who is a new proponed of national identity cards after the September 11, 2001 attack on the United States. Despite the fact that all of the attackers were foreign nationals, who had visas and passports, Ellison, for what may appear to be personal gain, wants to issue personal identity cards, using his company's, Oracle, database, to track people at all times.

1.7 Brandeis

Louis Brandeis was to become one of the most significant Supreme Court justices. He was a Harvard Law School Graduate, he practiced law in Boston, and was one of the most insightful crafters of Supreme Court Decisions.

In his paper with Warren his partner, he begins by saying:

"That the 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. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. *Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life--the right to be let alone, the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession-- intangible, as well as tangible."*

Brandeis then goes on to describe the specific "privacy" rights and the sources of those rights:

"In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent. This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung, a drama acted. … The right is lost only when the author himself communicates his production to the public--in other words, publishes it. It is entirely independent of the copyright laws, and their extension into the domain of art. The aim of those statutes is to secure to the author, composer, or artist the entire profits arising from publication; but the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all.… The statutory right is of no value, unless *there is a publication; the common-law right is lost* as soon as *there is a publication…What is the nature, the basis, of this right to prevent the publication of*

[15] Warren and Brandeis, *4 Harvard Law Review 193 (1890)*

manuscripts or works of art? It is stated to be the enforcement of a right of property; …A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry; the restraint extends also to a publication of the contents. What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself. …The copyright of a series of paintings or etchings would prevent a reproduction of the paintings as pictures; but it would not prevent a publication of a list or even a description of them. Yet in the famous case of Prince Albert v. Strange *the court held that the common-law rule prohibited not merely the reproduction of the etchings which the plaintiff and Queen Victoria had made for their own pleasure, but also "'the publishing … though not by copy or resemblance, …".*

Brandeis then goes on to describe the following precedents:

" Abernethy v. Hutchinson, *3 L. J. Ch. 209 (1825), where the plaintiff…sought to restrain the publication in the* Lancet *of unpublished lectures which he had delivered … Lord Eldon doubted whether there could be property in lectures which had not been reduced to writing, but granted the injunction on the ground of breach of confidence…*

… Prince Albert v. Strange*, 1 McN. & G. 25 (1849), Lord Cottenham…recognizing a right of property in the etchings which of itself would justify the issuance of the injunction, stated, after discussing the evidence, that he was bound to assume that the possession of the etchings by the defendant had "its foundation in a breach of trust, confidence, or contract," and that upon such ground also the plaintiff's title to the injunction was fully sustained.*

… Tuck v. Priester*, 19 Q. B. D. 639 (1887), the plaintiffs were owners of a picture, and employed the defendant to make a certain number of copies. He did so, and made also a number of other copies for himself, and offered them for sale … the plaintiffs registered their copyright in the picture, and then brought suit for an injunction and damages. The Lords Justices differed as to the application of the copyright acts to the case, but held unanimously that independently of those acts, the plaintiffs were entitled to an injunction and damages for breach of contract.*

… Pollard v. Photographic Co.*, 40 Ch. Div. 345 (1888), a photographer who had taken a lady's photograph under the ordinary circumstances was restrained from exhibiting it, and also from selling copies of it, on the ground that it was a breach of an implied term in the contract, and also that it was a breach of confidence… Justice North interjected in the argument of the plaintiff's counsel the inquiry: "Do you dispute that if the negative likeness were taken on the sly, the person who took it might exhibit copies?" and counsel for the plaintiff answered: "In that case there would be no trust or consideration to support a contract." Later, the defendant's counsel argued that "a person has no property in his own features; short of doing what is libelous or otherwise illegal, there is no restriction on the photographer's using his negative." But the court, while expressly finding a breach of contract and of trust sufficient to justify its interposition, still seems to have felt the necessity of resting the decision also upon a right of property, in order to bring it within the line of those cases which were relied upon as precedents."*

Brandeis concludes with the following:

"First. The right to privacy does not prohibit any publication of matter which is of public or general interest….

Second. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel….

Third. The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage….

Fourth. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.

Fifth. The truth of the matter published does not afford a defense….

Sixth. The absence of "malice" in the publisher does not afford a defense….

The remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely:

An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.

An injunction, in perhaps a very limited class of cases."

Brandeis thus initially established the tort type protection that has been discussed herein. Specifically, the discussion by Prosser and the Restatement of Torts discussed by Prosser may be for shadowed by the recommendation by Brandeis.

However, Brandeis deflects inwardly, on the individual and a right to be let alone. It is the reclusive version of privacy. He most likely would never have imagined the role of the Etzioni school of thought, wherein the proposal is to embed micro chips to monitor each human!

1.8 Posner

Richard Posner, a prolific Federal Court Judge and faculty member at the University of Chicago, approaches privacy in a purely economic fashion. As he states:

"… the interest I am calling "the face we present to the world". Economics, with a bit of simple game theory… and some help from philosophy, can help us thread this maze, uncover the laws unity, think concretely, about problems often obscured by the "sonorous" talk of "privacy", and incidentally provide a bridge…"[16]

Posner is clearly a jurist who views almost all legal issues in an economic context. All interactions or actions are transactions, the decision to make and compete an action based on some economic measure or value. For example, I decide to rob a bank because in my mind I make money from doing so and the weighted probability of getting caught and the cost to me of doing so is significantly less than what I will get robbing the bank. It is not clear that all thieves think in terms of von Neuman game theorists, in fact I can think of very few people who can or even less who do.

To Posner, there is first and almost only and economic rule a play, a rule in many ways dependent on privacy as a property and with an economic or transactional value applied.

To better understand property and privacy one must consider why Richard Pipes, of Harvard, in his treatise on Property, makes the following statement regarding privacy:

"The whole concept of privacy derives from the knowledge that we can withdraw, partly or wholly, into our own space; the ability to isolate oneself is an important aspect of property rights. Where property

[16] Posner, Overcoming Law, p. 531.

does not exist, privacy is not respected…which helps explain why the Russian language-the language of a people who through most of their history have no private property in the means of production-has no word for privacy…"

Pipes is a Soviet and Russian scholar, a Pole, who had escaped the Soviet domination of Poland and Central Europe. He clearly understands the issues of privacy as derivative from but as superior to property. Pipes is one who has seen the flow of German Nazi troops and the counter flow of Russian Soviet forces back and forth across Poland. He understands the essential belief in the sanctity of the individual and in his work clearly and unambiguously states this.

Posner considers privacy as an element of an economic exchange. Part of that assumption is that privacy has value comparable to property. Pipes takes that even further and states a duality between property and privacy, in fact Pipes can be said to state that privacy is the natural extension to property.

Posner starts his discussion on Privacy in his book, *The Economics of Justice* ("EOJ"), as follows;

"Provisionally, privacy means the withholding or concealment of information, particularly personal information…"

Posner then states:

"It is no answer that people have the "right to be let alone" for few people want to be let alone"

Clearly that statement is at best self serving, since aloneness is not necessarily the same in all cases. I may want as a social animal to interact with people but at the same time I may want to retain the privacy or secrecy of my hobbies or collections.

Posner states regarding privacy as concealment. He argues that people frequently go around selling themselves but conceal items that may not allow them to be presented in the best light. Posner then goes on to say that in buying things, we should have the right to know anything material to the sale about the person selling the product. Thus for example, one may assume Posner demands that the seller of a Pizza if he has AIDS should reveal that to all buyers, or at least the buyer should have the right to ask and the seller the duty to respond truthfully. This is generally not the case.

He talks generally about the concepts of privacy as; (i) secrecy, (ii) seclusion, and (iii) autonomy. Specifically these are defined as:

Secrecy: Secrecy is a form of concealment. Posner states that he feels that what people do today is seek to keep personal information secret for personal gain.[17] In a sense the desire for secrecy is to control others perceptions of one's self.[18] This means to create an alternative persona. This concept of privacy in the Posnerian world is one we shall see again in the Internet world. The ability to create a persona, to mold by withholding and to mold by mis-stating, a new and unique personality. The Internet personas are based on controlling information, but positively and negatively.

Seclusion: In a sense this is a withdrawal from the cares of public life. Posner refers to gregarious seclusion, specifically when someone wants to be let alone to do something of more import, not a desire to separate themselves from society.[19]

[17] Posner, EOJ, p. 271.

[18] Posner, EOJ, p. 233.

[19] See Posner, EOJ, p 269. He has extensive discussion on these concepts.

Autonomy: Posner defines this as the "being allowed to do what one wants without interference". He further states that it is inappropriate to define privacy as the same thing.

The three types or characterizations of privacy from Posner seem very compelling. As he states in EOJ, the interpretation of Brandeis and the subsequent attempts by the Supreme Court to establish a right of privacy where none exists is to limit privacy to secrecy and seclusion and it should be expanded to be free from governmental interference.[20] This expansive interpretation would seem to be within the Brandeis format but Brandeis in writing his paper was responding to an invasive attack by the press, not government. Would Brandeis have responded in a similar fashion in today's world. Thus, in a Posnerian world, the autonomy construct is the broadest and most far reaching.

1.9 Etzioni

Etzioni is a communitarian. He states that:

"Communitarianism holds hat a good society seeks a carefully crafted balance between individual rights and social responsibilities, between liberty and the common good…"[21]

He further notes in the introduction of his book:

"my first call is to demonstrate that immoderate champions of privacy have not merely engaged in rhetorical excesses but that these excesses had significant and detrimental effects."

Etzioni further goes on to state:

"while we use voluntarily more …ID cards…they are inadequate…all people be required to identify themselves when asked to do so by public authority.."

He totally rejects the Fourth Amendment, he takes a neo-Nazi neo-Stalinist view that some benign public authority has the right to demand from the public, for no good reason, that they totally abandon all their constitutional rights.

Etzioni goes on to "re-examine" the privacy arguments. He criticized Warren and Brandeis, then criticized Griswold on the basis that although contraception may be good the right recognized under Griswold may lead to " the unbounded nature of the position embraced.."[22]

Etzioni goes on to suggest eliminating privacy as we now know it for such areas as national ID cards, implanting biometric identifiers in humans, expanding the Megan's law disclosures, increasing government control over encryption, disclosing who has AIDs, and other such areas. Etzioni would see the release of all medical records record if he sees them for the public good.

In many ways Etzioni is not an aberration but a clear example of what certain major and influential groups want, namely government access and control over not only information but the individual. The ID cards are a single first step, but the biometric plants are horrifying.

[20] Posner, EOJ, p. 315.

[21] Etzioni, p. 5.

[22] Etzioni, p. 193.

1.10 DeCew

DeCew has developed a concept of narrow and broad views of privacy. These views, based upon her work and others, is an ideal stepping off point for the development of privacy issues. She begins by establishing two elements of her reasoning: (i) the developments eschew privacy as a right, the discussions use rights terminology, but the establishment of privacy as a right is not a basis of her discussions, (ii) she makes no endorsements of the cases or decisions discussed. The reasons for these disclaimers at the outset are better understood as she develops the privacy concepts as regards to the feminist movement.

DeCew established privacy in two domains; Narrow View and the Broad Concept. We develop each as follows:

Narrow View: DeCew uses reference to two writers to map out some landscape for this narrow view. The first is Parent and his view that privacy is the protection of private knowledge.[23] This is the school of "secrecy" or "concealment" where an individual has the alleged right to keep from others what they desire. However, this view of privacy as secrecy is very narrow, it puts the burden on a narrow set of things which can be kept secret and puts the burden on the individual to keep them as secret. The second school is that of Henkin and the concept of privacy as autonomy.[24] Frankly Henkin perceives autonomy as separate from privacy. For Henkin autonomy is freedom from governmental regulation. Henkin believes that autonomy, not privacy, is the basis for the cases like Griswold. Privacy for Henkin is more narrow encompassing the tort based claims which are invasion from other persons. Thus, according to DeCew, the narrow view of privacy is concealment or secrecy and possibly the protection of invasion from others.

Broad Concept: The Broad Concept is more far reaching. DeCew defines three aspects and each, she states, has an affiliated set of claims.[25] These three aspects are:

1. *Informational Privacy:* This is the expectation that information about oneself is to be kept from public view. This is a right of secrecy.

2. *Accessibility Privacy:* This type of privacy allows one to keep from interfering with ones private actions. In effect it is a right of seclusion.

3. *Expressive Privacy:* This is the right to express ones self. In effect this is a form of self-expression.

DeCew's three elements, secrecy, seclusion, and self expression, are a broad view of the concept of privacy. However, the issue of anonymity is not within this domain. In fact it is an extension of the three elements as espoused by DeCew.

Expanding on DeCew, Mell states a theory of privacy via these definitions:

"Several privacy definitions recognize the individual's right to control personal information. In this article, privacy is the legally recognized power of an individual (group, association or class) to both 1) regulate the extent to which another individual (group, class, association or government) may access, obtain, make use of or disclose a persona concerning him, or concerning those for whom he is personally responsible; and 2) monitor and correct the accuracy of the persona compiled concerning him or those for whom he is personally responsible. This definition incorporates the five rights and demonstrates the situations in which the individual might want to control disclosure of personal information."

[23] DeCew p. 28.

[24] DeCew p. 35

[25] DeCew, p.75.

Mell further continues along the lines of property rights:

"The recognition of a property right in the individual about whom the persona is collected does not detract from the interest any collector or compiler of databases may have in the same persona. It does mean, however, that any information-collector's interest would be "subject" to that of the individual in some important respects. A basic premise of the law creating this property right should be that the identity of the holder or the information (government or private) industry would not determine the nature and extent of protection provided the individual. This is consistent with the current balancing of interests required both constitutionally and by existing regulatory statutes.

The property analogy is not without its difficulties for the electronic persona. Historically, the protection of any property was based on the presumption that the object to be protected had a consistent configuration regardless of the holder's identity. In contrast, the electronic persona is characterized by its mutability. Created and continually manipulated by parties other than the individual, the electronic persona may be the compilation of any variety of pieces of personal information. The key to recognizing a property interest in the electronic persona must be based in the identifiably of the persona to a specific individual. Once that link has been established, the persona "belongs" to the individual about whom it "speaks" without regard to the source or content of the specific pieces of information constituting it. Thus the electronic persona could be defined as a collection of at least three pieces of personal information concerning the individual (or those for whom he is responsible) that identifies the individual(s): for example, name, social security number, selective service number, finger print, etc.

The common-law view was that an owner could never be deprived of his ownership rights without either consent or compensation. This theory is the basis of the current protection of identity as persona under the intellectual property doctrines of the right to publicity, misappropriation and copyright. Each of these doctrines is premised on the protection of various indicia of a specific person's identity from its commercial exploitation or use by a third party."

1.11 Tribe

Tribe is a professor at Harvard Law and is a noted liberal constitutional scholar. Tribes, in his book on constitutional law, details privacy into several areas where government allegedly interferes. The approach is to categorize dimensions of privacy in several areas and then to summarize the nature of the Courts rulings in each. As with most of the Court rulings, the challenge would be to establish a logical framework of what would be expected in variants from the special cases generally placed before the Court.

Tribe's areas are as follows[26]:

Mandatory Incantation and Liberty of Conscience:

The classic case is Wooley v Maynard where a Jehovah's Witness objected to the New Hampshire motto of "Live Free or Die".[27] The issue is can the Government take a position to infringe on the privacy of the individual by making the individual cooperate with the Government in a way in which the individual and their "space" are interfered with.

[26] See Tribe, Chapter 15.

[27] The New Hampshire case is of interest due to several factors. The motto was actually created in the French Revolution and then used almost simultaneously in New Hampshire. New Hampshire also had a Governor, Meldrin Thompson, who asked to Federal government to have the State National Guard equipped with Nuclear weapons to protect the US frontier from attacks from the Soviets from the north. New Hampshire has a unique reputation in that regard.

Compulsory Education and Freedom of Inquiry

The classic cases are *Meyer v Nebraska* and *Pierce v Society of Sisters*. They reaffirm the parents rights to raise their children, limited rights of teachers, and provide certain rights to local school boards. More recently in *Board of Education v Pico*, the Court allowed the keeping of certain books in libraries for the education of students.

Screening the Sources of Consciousness

In *Stanly v Georgia*, during a legal search, the authorities discovered pornographic files. The individual was convicted of possession of pornography, albeit in their him. The Court reversed stating that mere possession was not a crime even if the selling, transport or exporting was. This is the establishment of the fact that inner most thoughts are protected, even if the actions taken by these latter may not.

Coercive Conditioning

In one case, for example, *Kaimowitz v Department of Mental Health*, the Court reaffirmed the fact that a patient cannot be involuntarily made to participate in psychological experiments.

Prevention of Bodily Intrusion

Such items as compelled vaccinations, blood tests, bodily cavity exams, have limitations. In *Rochin v California* the Court held that forcible pumping of the stomach is a flagrant violation of fourteenth amendment due process.

Decisions about Birth

This is the *Griswold v Connecticut* and *Roe v Wade* decisions. The most intimate and personal control of birth control and birth are personal decisions that the government is prohibited from intervening.

Decisions about Death and Dying

This relates to death with dignity and the right to die. Such cases as *Brophy v New England Sinai Hospital* permit the removal of feeding tubes.

Choice of Life Plan and Risk Taking

The ability of a person to take personal risks, such a riding without a seat belt or without a helmet on a motorcycle, have certain standing. However in *People v Kohrig* there were limitations placed which allowed the state to control this to some degree. Again, New Hampshire has no seat belt law and no helmet law for motor cycles and the Federal government must let that stand.

Vocation

In *Schware v Board of Bar Examiners of New Mexico*, the Court held that the state could not deprive the plaintiff of being admitted top the Bar without due process on a record which the Bar could not rationally find as unfit.

Travel

In *Shapiro v Thompson* the Court stated that the right to travel was “not a mere conditional liberty…subject to regulation…but an unconditional personal right”.

Appearance

In *Kelley v Johnson* the Court upheld the right of the state to set standards for appearance of police officers. In *Katz v U.S.* the Court stated that the fourth amendment *protects people not places*.

Reputation and Records

In *U.S. v Miller* the Court stated that an individual has no protection of privacy when it relates to his checks.

In the Tribe areas of privacy, they relate to how we deal and are dealt with regarding personal choices, decisions, and actions. The relate to how we deal with and of ourselves and what protections we have under the Constitution to retain the penumbra of privacy. The question then becomes, how does one take the Tribian elements, and apply then to the Internet and Data world.

Another question regarding the Tribian elements, is can one construct a syntax from which this extension to other domains is possible. Are there elements that we can use a mathematical schema and understand the logical framework, establish a grammar and syntax which allows one to ascertain consistency and extensibility.

Clearly, under the law and the use of both the Constitution and the Court's precedents, we seek to establish a consistent architectural framework to establish the extensibility, to propose privacy analogs that have a clear and well defined nexus to the world as we find ourselves in.

INTERNET AND ELECTRONIC PRIVACY

As we have developed, privacy can be viewed in various contexts. Posner reflects on privacy as being in three different modes; secrecy, seclusion, and autonomy [28]. As secrecy it is a concealment of certain personal facts, as seclusion it is hiding, and as autonomy it is to be able to do our own thing, whatever that means, assuming it is legal.

As Brandeis stated in Warren and Brandeis:

*"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right **"to be let alone."** Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration."*

The above statement commences with the statement concerning recent inventions. In the Internet world, the recent inventions are overwhelming. For example, one may think if IP appliances, refrigerators with IP addresses which monitor their performance as well as those possibly of the owner. Is it possible to track

[28] Posner is of the economic school of law. He views almost all legal issues in the context of some financial or economic transaction. Cantor divides the legal theorists into seven schools, leaving Posner in what he calls the Law and Economics school. The other schools are: Justice and Liberty wherein he uses Maitland as the primary speaker, Marxist wherein he places Horwitz of Harvard, Feminist wherein he places Foucault, Psychoanalytic where is placed Lacan, Structuralism and Levi-Strauss, and Deconstructionist with Derrida.

what goes in and out of a refrigerator, even to the level of calories. The next step is implanting IC chips in humans, the extension of the smart card to the individual and track their for consumption, sex lives, and stress levels. So the statement by Brandeis that "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual…"* go to the heart of the Internet world and the issues of privacy.

The secrecy issue is keeping ones thoughts, ideas, concepts, and actions secret. This is the secrecy or privacy of the person. However, Posner then goes onto the issue of secrecy in communication. Namely the secrecy between people. Here facts are disclosed by the keeper to an recipient. However, if the two parties enter into an agreement to not share the information, item, fact, whatever, then the extension of privacy as secrecy may be extended beyond just one person. Clearly there is a great deal of justification of privacy as secrecy. To the extreme, the Fifth Amendment prevents self incrimination. The state has no right to force an individual to disclose anything that may be self incriminatory. In fact, the definition may be in the mind of the beholder. However, the government does have the right to have one disclose information that may be necessary to the prosecution of a case as is done in the case of a material witness to a crime. In fact, one may be incarcerated as a material witness, in apparent defiance of habeas corpus by a judge if one does not comply. Journalists are frequently jailed for refusing to provided sources. In that case however they have revealed the fact that they have information. For a non journalists material witness incarceration may be effected without any stated probable cause and without due process, despite the Constitution.

Privacy as seclusion if the ultimate of being let alone. It is a concept that Posner has developed at length.[29] Secrecy is that I do not want to tell you anything seclusion is that I do not want to be bothered by anyone. Seclusion is a desire not to be bothered by others, secrecy is a desire to conceal from others. Seclusion is a passive concept whereas secrecy is an active concept.

Autonomy, according to Posner, as a privacy concept is the freedom to do what one wants without interference.

The next question is can we extend this concept of privacy to more than one person, namely to a group. In addition in *NAACP v Alabama* the Court stated:

"It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as the forms of governmental action in the cases above were thought likely to produce upon the particular constitutional rights there involved. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said in American Communications Assn. v. Douds, supra, at 402: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."

This ruling allows for freedom of association in a form of privacy as a group. Thus if a group, why not a married couple. The US Supreme Court in *Griswold* stated as follows:

"In NAACP v. Alabama, 357 U.S. 449, 462 , we protected the "freedom to associate and privacy in one's associations," noting that freedom of association was a peripheral First Amendment right. Disclosure of membership lists of a constitutionally valid association, we held, was invalid "as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of

[29] Posner, EoJ, p. 269.

association." …. In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. ….."

Justice Douglas introduced the concept of the penumbra or shadow of protection of a privacy right. Admittedly this right was applied to the use of birth control but it was stated clearly. This then states that we have certain privacy rights as two people, at least two people having sex. This has yet to be extended to two people doing anything else.

As we have previously discussed, another view of privacy is in the context of property of the persona and the torts associated with the misappropriation of that property. Prosser, as discussed, has characterized four categories of tort relief under the heading of privacy:

1. appropriation of name or likeness;

2. intrusion upon an individual's seclusion, solitude or private affairs;

3. public disclosure of private or embarrassing facts; and,

4. publicity that places a person in a false light in the public eye.

These are common law "rights" that have been recognized in various forms of case law. We must ask however how and where they can be applied in an electronic world.

Consider a set of simple examples.

Case 1: I am walking down the street in New York. It is 8 PM and I am alone, dressed in a conventional manner, I an clean cut, and am conducting myself in a civil fashion. Does the police have a right to ask me for identity or if asked do I have a right to deny them such proof of identity. In New York, if questioned, and if there is no probable cause, namely there is no identified felon or potential felon for whom the police officer has been informed is a person to be "on the look out for" then the request has no merit and I have the right to deny the request, namely I have a right to be left alone and keep my anonymity. In California that is not the case. The California statue requires presenting identification. This is a result of the World War II problems with the risk of Japanese spies. It was a result of a clear and present danger. The question can then be posed, why not in New York fearing German spies, or is California wrong in having such a law. Do I have a right to be left alone in this context.

Case 2: A husband is at home with their spouse and engage in sexual activity. The activity involves the use of birth control methods. The state has declared the usage of these devices illegal. What right if any does this couple have?

Case 3: I am at home and I decide to use my telephone. I place a call to a friend and discuss how I really hat a certain situation and the persons involved. I make no defamatory statements. I have no predisposition to cause any harm, I have no criminal record, and neither does my friend. Does the government have a right to tap my phone lines under any law. If so, can they do it without getting a search warrant?

Case 4: I want to buy a new car. The car costs $25,000 and I want to pay for it in cash. I have the money in my bank account. I go to the bank, get the money in $100 bills and go to the car dealer. I pay for the car. Both the bank and the car dealer then file reports with the Federal government. Have they violated my right of privacy?

Case 5: I am a moderate Republican but I work in a city job in a very liberal Democratic city government. I decide that I want to send a contribution in for the new Republican candidate for President. I send in a check for $1,000. My wife and I make the contribution and we both send two checks, each for $500. A month goes by and my boss, a Democratic Party appointee calls me in and shows me the Republican donor sheets he

has received for the state. My name is there. He states that he does not like having Republicans in a sensitive political job. Has he violated my privacy rights.

Case 6: A patient has terminal cancer and is a user of morphine a controlled Class 1 narcotic. The patient purchases the drug from the local druggist with a prescription from their physician. The state orders all pharmacists to provide the names of all users of Class 1 controlled substances. What rights does the patient have regarding their medical records at the pharmacist?

Case 7: I am at home and use my computer to store all my business records. I was on the Board of a company which has gone bankrupt and the government is now investigating the company for criminal charges. I left the Board well before any of the claimed actions. A compute repair person comes into my house to fix my computer to work with a DSL modem. They also are the child of a shareholders who lost all their money. In the process they take all my records off of my computer. They then turn them over to the FBI. What rights, if any, to I have to protect those records?

These all relate to "privacy" in a broad context. At one extreme is personal sexual behavior, use of birth control or the desire to have an abortion, and at the other extreme the search and seizure of items from my person, such as information, data, records, identity, and such. They involve physical contact, telecommunications contact, and data contact. They do not all fit under the same set of laws in the context of U.S. legal systems however. In fact "privacy" under U.S. Supreme Court judgments relates almost exclusively to sexual maters, abortion and birth control, and say little if anything about the person qua individual.

1.12 Persona in the Internet and the Electronic World

The term persona is to be used to describe the individual as regards to the Internet and their life thereon as well as a persona of the individual in the electronic hyperspace facilitated by the Internet. We bifurcate the medium upon which this persona is created into two parts; (i) the public Internet as best exemplified by the proliferation of web sites, search engines, and email, and, (ii) the less than public electronic world of databases and information storage media owned generally more privately, and upon which are imprinted our day to day actions and reactions. We divide this world into these two elements and call them appropriately "Petri dishes".

The Internet Petri Dish: This environment for creation is the Internet as we know it, a world of web sites and email, a world in which the individual or a third party may create a persona.

The Electronic Data Petri Dish: This world is the world of third party databases, government or private databases, which contain our lives, and in turn reflect our persona. For example, it may be our health care provider, combined with EZ Pass (a highway electronic toll system), combined with Visa credit card, combined with the telephone company, combined with INS passport control, all creating a view of who we are. The persona we grow on this Petri dish is to some degree under our control but to a great degree at the control of others. We can be identified as someone who is ill each February, who calls their mother every day, spends a lot for restaurants in central Manhattan, goes away to war locations, and travels frequently to Washington, DC. What does that profile or persona mean and to whom does it have meaning. In many ways this is a much more powerful persona, it may say things about us that we may never really know, and do not want known. No single fact may be telling, but the correlation of these facts is overpowering. The simple example is what credit card companies do to protect their cards, relative to spending patterns, could one expand this to the total person, effectively electronically psychoanalyzing the person or more importantly the persona.

There has been the view that this persona is what the person creates but I will argue herein that there are many ways that this persona may develop. A digital persona is a mapping of the individual which may not be one to one with their actual identity. The Internet may allow the individual to create personas, many of

them in fact, and to live in the electronic cyber world as may personas, as many cyber-persons. I may create a persona, some other person may create a persona, or the Internet as an "organic" entity may create the persona.

Let us consider these three persona creation mechanisms:

Self Created Persona: This persona is what we create for and of ourselves on the Internet. We may create multiple such personas. It is our web page, it is what we say in chat rooms, it is how we choose to interact with others and how we want to identify ourselves. It is in many ways the extension in a much more complex domain what was done in CB radio. We can say whatever we want, we can create images, withhold information, or whatever we choose. We can, as stated, create multiple persona.

Other Created Persona: Others can create a persona of us. They can steal our identity, they can become us in ways in which we may never know. This may be identity theft.

Organic Created Persona: This is the creation of a persona independent of us or a third party, it is the creation of a persona by the accumulation of the interactions we have on the Internet, very much like to creations we have in the Electronic Data Petri dish world discussed above.

The broadening of persona in both Petri dishes is that of a Digital Persona. Mell describes the persona as follows[30]:

"The term "persona," derived from the Greek term for the mask worn by theatrical performers, is generally used to describe the various ways by which a person can be identified by personal information about him. The term is also used with reference to the right of publicity to describe the bundle of commercial values embodied in the identity of a person. The right of publicity comprises a person's right to own, protect and commercially exploit his own name, likeness and persona."

Mell goes on to state:

"The electronic persona is then autonomous, commoditized into the physical world, directing from the electronic wilderness the actions and transactions in which we are involved. It can survive our deaths, exist totally without our awareness and be unresponsive to sudden changes in our society and lifestyles. To the user of this information, who will seldom meet the individual face-to-face, the electronic persona becomes the "real person." The outsider will see and use the persona to make decisions about the individual's life. In effect, the individual becomes secondary to the accuracy of the persona. No one or two pieces of information can tell the entire story of the individual's life. Nor do the separate pieces of information necessarily identify the individual directly. At some point, however, the combinations of personal information can form seemingly complete "images" of the individual. At that critical moment, an electronic persona is born and its reality overtakes our own."

1.13 Creating the Digital Persona

Life on the Internet requires that individuals be able to identify themselves while still retaining privacy and confidentiality. All the components are in place for the marketplace to evolve a uniquely elegant and powerful solution to these identity and privacy needs on the Internet.

An individual will not have a single identity on the Internet. Instead, he or she will have multiple identities for use in different situations, a concept we call the "Digital Persona." The Digital Persona emerges from and combines other personal identifiers. At birth, humans are named. Soon afterwards, they are assigned social

[30] See Mell

security numbers. Later, people acquire drivers' licenses, passports, credit cards and other identifying records. They have school and job affiliations, home addresses, telephone numbers and email addresses. The Digital Persona is a collection of such digital identities, stored on a network directory and made selectively available by the user, much as a person now physically takes out various cards from his or her wallet in different situations.

Mell makes the following statement regarding this persona:

"The electronic persona is stored and manipulated in the database environment. It cannot be categorized as stock or material suitable for either traditional copyright or patent protection. The several layers of interests competing for its use make the electronic persona sui generis as property. Collected and stored in both government and private databases, the electronic persona is a valuable resource or property. Each database represents a bundle of competing rights in its use. The interests of the government, the public and commercial entities continually conflict with one another as they flow through commerce. The government needs to access personal information to determine eligibility for benefits or violations of lawful regulation. The public has a right to access this information to assist it in understanding the nature and scope of governmental activity. Commercial interests include the economic interest of a data collector, compiler or user in personal information about an individual. These three interests must achieve a balance, but none should be presumed superior to the others. Ultimately, the private nature of the information should allow the subject to control disclosure of the information to third parties."

Mell is using the persona created externally in databases as an example. She develops this construct and the exogenous persona which we frequently have no control over and frequently have no knowledge of. The Internet persona has characteristic which are similar. It is a person we may crate or also a person created without our participation.

One can view self generated persona on the Internet in at least four distinct levels:

1. "Lurker" – a listen-only identity that can exist undetected in some communities;

2. "Present" – an anonymous identity that can listen and send but whose identity is unknown;

3. "Self-Identified" – an identity which is entirely defined by the user;

4. "Certified Identity" – an identity some of whose aspects are not user-controlled, but are certified by another entity (such as a government agency, a company or a bank)

Mechanisms to build these identities are partially available today on the Internet. Chat rooms have the ability to have "viewers" who watch but do not participate (Lurkers). Anonymous re-mailers enable people to participate while hiding their identities ("Present"). Chat rooms and online communities often have identities that are limited to specific uses and completely defined by the user (with properties like age and sex left up to the user.) When companies give employees email they in effect certify that the person is affiliated with that company. Cookies in browsers often contain a mixture of self-reported information and information certified by a provider. Certification Authorities exist to authenticate characteristics of identity, such as age, location or ability to pay, that are necessary to engage in certain activities or complete certain transactions.

These collections of identities will be stored in well known places accessible to users on the Internet. Users will be able to manage all components of their Digital Persona except for those that require certification, which will be controlled by the certifying entities.

The Digital Persona can become a central focus for privacy protection on the Internet as well as private data systems. Through it, the individual keeps control over his or her identities and can choose to disclose information to other parties on an as-needed basis. The user can choose to send only a reference to the

needed information and can use encryption or other authentication tools to make sure that the other party is who or what it represents it is. The user can give general instructions to his or her Digital Persona about what information to release for which activities under what safeguards, or he or she can individually approve each use of data or each transaction.

Organizations doing business on the Internet should clearly state their privacy policies on their Websites and have a legal obligation to follow them. With such information about Website privacy policies, users can instruct their Digital Persona to "negotiate" with Websites about release of personal data. The P3P technology under development by the World Wide Web Consortium (see details in 2.8.2) appears one such promising approach to facilitating the flow of necessary identifying information while still protecting individual privacy as defined by the user.

More generally, software technology is becoming available to manage the tradeoffs between anonymity, privacy and accountability at each level of identity within the Digital Persona; that is, software that can:

1. Enable users to control and manage their Digital Persona;

2. Support negotiations between consenting parties regarding the exchange of information;

3. Document exchanges of information or transactions; and, if needed,

4. Collect evidence to show violations of privacy agreements.

The necessary tradeoffs are best resolved directly between affected parties, and within the context of particular situations. Firms and other organizations that have published their privacy policies will have commercial as well as legal incentives to comply with them. Bad reputation travels fast. We believe that technical tools and non-governmental arrangements will provide essential privacy protection in most cases.

Government presence is needed, however, to assure an appropriate legal framework for private transactions on the Internet, and to take action if voluntary efforts to protect privacy fail. Much of the framework for privacy protection on the Internet carries over from traditional commerce and is well articulated in the "Electronic Bill of Rights" presented in the *First Annual Report of the U. S. Government Working Group on Electronic Commerce*:

1. The right to choose whether one's personal information is disclosed

2. The right to know how, when and how much of that information is being used

3. The right to see that information themselves

4. The right to know if information is accurate and correct it if it is not.

E-commerce requires a level of trust between buyers and sellers, including a secure payment mechanism that is appropriate for a particular transaction. Different kinds of transactions will use different forms of payment and levels of authentication:

1. Secure credit card payments for many consumer transactions;

2. Third party escrows for certain transactions between individuals (e.g., auctions);

3. Certification Authorities for high-value or other important transactions.

Technology is commercially available to support each level, and each has a different cost structure. Each level also requires processes for buyer protection, transaction enforceability and dispute resolution, which

rely primarily on existing legal frameworks. International coordination is needed, but additional government intervention to support e-commerce security and payment mechanisms doesn't seem necessary at this time.

From the seller's viewpoint, e-commerce security should be thought of in terms of risk management. Issues such as fraud, buyer authentication, and recourse for non-payment arise in e-commerce just as in other commercial transactions. Ways to manage e-commerce risk appear to be evolving satisfactorily within the private sector, although many issues remain (such as the lack of an adequate experience base on which to determine appropriate premiums for purchased or self-insurance). In particular, the technology generally appears adequate and available to support risk management for e-commerce.

Markets rely on information about buyers, sellers, and products, and participants in market transactions have for much of this century relied on both direct assertions (e.g., advertising) and third-party references (e.g., credit bureaus, D&B, Consumer Reports). However, these brokers of reference data are being joined by private, direct sources of claims that circulate without the safeguards of traditional systems. The ability to efficiently and reliably establish or withdraw trust for commercial transactions may be disrupted.

New claims may take a variety of forms. For example, firms may circulate "private blacklists" based on unspecified or otherwise unverified claims about creditors. While the law grants firms and individuals certain rights in their dealings with credit bureaus and other traditional providers of such data, the private blacklist may have no specified recourse for review, challenge, or correction. Similarly, individuals can circulate economically damaging claims about institutions that a corporation may find difficult to fight (e.g., McDonalds). Spoofing can also pollute the commercial environment by undermining trust, which, in the absence of reference schemes, can then be generalized to other legitimate actors in the market space (cf. the "Dysson" scam).

Recourse may be slow or unavailable. Without guaranteed protections through commercial law, recourse may be sought through claims of defamation, libel, etc. This avenue is slow, expensive, and of limited value in international commerce. Since it is also by definition ex post facto, it may rightly be claimed to be inadequate to the problem, since the new information generated never expunges the previous information. The circulation of conflicting claims and even persistently discredited information (e.g., urban legends) can result in marketplace relations characterized by tentativeness, protracted and/or multiple negotiation, and inefficient, costly diligence efforts.

There may be alternative methods of addressing the problem. One issue is the establishment of trusted third party arbitrators of commercial information. This may be the traditional firms or new mediators. Acceptance of third party arbitrators should be subject to private sector agreement.

A second matter is the migration from traditional information asymmetries that characterize especially business-consumer relationships (the data companies can get about consumers is much more systematically collected and reported over longer periods than that available to consumers about businesses) to an environment in which more symmetrical information relationships can be established. Efforts to extend and expand the types of consumer information associated with Zagat© type guides are much easier and dynamic on the net, and the openness of such systems (the desirability of a large 'N') can act as a safeguard against individual vigilante actions.

There may also be mechanisms and markets for generalizing and publishing the trust-related data created by individual consumer decisions. For example, Amazon.com now includes a feature that allows consumers interested in a book to see what others interested in that work also bought. By moving away from self-reporting to reports based on behavior and then aggregating the data, this feature allows individuals to distribute decision-making about the extension of preferences.

Such features could be raised one level so that similar distributed decision-making could be a guide to initiating relationships with firms instead of products. An individual that had negotiated a commercial relationship with a firm to his/her individual satisfaction could learn what other people who had made similar

trust decisions with that firm to see what other firms they had extended relationships to. If it were sufficiently dynamic, such a mechanism could allow people to make threshold decisions about new commercial relationships based on growing or falling numbers of analogous relationships.

DEFINITION OF ELECTRONIC PRIVACY

1.14 Definitions

Definitions of "private" and of “privacy” are often sought. Many of those who have studied privacy know what it is when they see it but have difficulty defining it. The difficulty is based upon the fact that when defined it delimits. The Fourth Amendment process is a clear example. It defines a set of rights, but on a case by case basis, the meaning of those rights are clarified. For example, let us assume we accept the following definition as a starting point:

“when information is given by A about A to B, B may use it for no other purpose without A's consent. If B wants to use it in another way, B must give A the option of not being included - whether by specific opt-in or opt-out strategies or by general policy.”

Many privacy approaches assume that control of privacy and information disclosure can be accomplished simply by supplying users with information about the privacy policies of a site being accessed. These mechanisms may not be workable in practice. In particular, the notion that users will be able to explicitly choose to exchange privacy for access to goods, information, or other benefits may not work well when a broad range of alternatives does not exist. Just as, if there are few suppliers of a physical good, users often have little choice of price or quality, there may often be no practical way to both obtain goods or information and preserve privacy.

One particular type of information disclosure involves identification of the identity of the originator of a message. Notions of privacy imply that there should be a right of anonymity, and anonymity may be particularly important for some types of political speech. But any such right must be balanced with the right to not interact with anonymous parties. Example: if spammers were uniquely identifiable as such, TCP transactions downloading SPAM could abort early, definitively ending SPAM as an issue.

Many recent trends also seem to mitigate against intelligent user choices about privacy and information disclosure. For example, recent versions of popular browsers make it harder to make informed choices about acceptance of information-disclosing “cookies” than some of their predecessors and some rule-based cookie-control programs have disappeared from the marketplace.

There are also privacy concerns about infrastructure-related databases. For example, records of domain name registrations and address allocations have traditionally been public in order to permit users of other domains or spaces to track down problems and get assistance with resolving them. But, in recent years, those databases have been captured and utilized for targeted marketing purposes and that practice has led to strong suggestions that the data not be public.

On the surface the privacy issue seems to be a relatively straightforward clear-cut issue. Individuals and organizations have the right to privacy, where: *Privacy implies the ability for an individual or organization to have control over their personal information. This includes access to and control over what information is disclosed, when, to whom, and how it is used.*

But upon closer investigation, this issue is far more complex. Privacy is a two-edged sword in that loss of privacy offers the potential for good and bad. Customers are concerned with their loss of privacy. They are concerned that when their personal information is collected, it can fall into the wrong hands or just be misused, resulting in one or more of the following undesired situations, in increasing order of concern.

1. Annoying and unwanted sales pitches and cross sells

2. Personal embarrassment, damage of one's reputation, and in the case of corporations, the loss of trade secrets.

3. The denial of some desired end result; e.g. eligibility for health coverage, request for loan, application for employment.

4. Perpetrating some criminal activity, such as child porn, theft, fraud, account or identity take-over.

5. On the other hand, customers are motivated to provide their personal information for a number of reasons, including:

6. To obtain better more customized/personalized products and services

7. To obtain both specific information of value (e.g. personalized news); or in anticipation of gaining some unspecified benefit (e.g. unanticipated bargains, offers, analyses)

8. To obtain a desired product/service or end-result (e.g. commitment of a loan, acceptance of health claim, etc.)

9. In return for incentives such as money, loyalty points, frequent flyer miles

In some cases, the customer will initiate a request for a specific personalized service. For example, a customer might ask the service to alert him whenever it receives news articles on particular specified subject(s) of interest, and will fill out a personal information and preference form provided by the service provider for the requested service. The customer provides requested personal information with the understanding that the information will only be used in support of the requested service.

In other cases, the customer may be willing to provide information, where the service provider is given more latitude in the use made of this information in anticipation of unspecified benefits and/or in return for incentives. For example, based upon an analysis of customer-supplied information about their current mortgage and financial health, a mortgage company offers the customer attractive refinance options for her consideration. Prior to the offer the customer had not requested nor anticipated the need or desire to refinance. In another example, a bookstore knows that its customer enjoys Danielle Steele novels, so sends him a book review of a new author whose novel has gotten rave reviews and is likened to a Danielle Steele novel. Again the customer never requested this information but is glad to receive it. In both these examples, by using personal information the company offers the customer services and products that the customer perceives as value. The downside of giving a service provider this sort of latitude is that the service provider's use of the information might lead to offers and services that the customer finds at best a waste of time and not particularly useful. Worse, the use of the information might result in a serious invasion of the customer's privacy.

Over time the customer will learn whether it can trust a company to use personal information wisely and to provide value, rather than a nuisance or worse to the customer. This sort of trust is engendered and cultivated through:

1. The service provider's brand and reputation

2. The customer's experience and relationship with the service provider

3. Referrals and testimony by third parties

4. Guarantees and means of recourse

5. Existing laws, contracts and regulations

6. Self auditing

In any event we see that in the customer's eyes all service providers are not equal with respect to their trustworthiness in protecting customer information. The importance of and need for additional law and regulation is unclear and varies with the service provider. The need for additional regulation is likely to be influenced by whether or not there is a ready availability of service providers and third parties with proven reputations and track records who are willing to offer services with adequate privacy protections.

The regulatory environment is currently quite mixed and uncertain. There currently are advocates and arguments both favoring and arguing against special privacy legislation for on-line commerce. The European Union passed a privacy directive that went into effect this year. It requires that consumers "get disclosure statements" on how personal information will be used and the option of preventing companies from sharing information about them. Further, any company doing business in the European Union is prohibited from sending information to countries that do not meet a threshold of protection. The U.S. is one of the nations that do not meet the European standard.

The new European directive requires that companies tell people when they collect information about them and disclose how it will be used. In addition, customers must provide informed consent before any company can legally use that data. This would be an "opt-in." policy, rather than an "opt-out" policy where the customer is informed of the intent to collect data and the purpose to which the data is used, but the data is collected unless the customer objects and expressly instructs the company not to. The U.S. is so far favoring a voluntary industry self-audit and policing approach, and is more disposed to an opt-out policy.

The European directive law also requires companies to give people access to information about themselves. This is not always practical. For example, a company purchases or collects data for a specific purpose (e.g. a direct mail solicitation) and does not retain the data. Because of this American officials say they disagree with giving people unconditional access to information about themselves, saying access should be allowed only if it is reasonable or practical to do so.

Under European law, each member nation is required to implement the directive by enacting its own law. Six nations have drafted or passed such laws so far. It is not clear that all European nations will actually pass regulation and/or institute such a policy. In the short term government and industry officials predict that nothing much will happen. Most countries have yet to implement their own laws to carry out the directive. And several countries, including Germany, have had tough laws in place for years, and companies have found ways to deal with the requirement. For example, in 1995 Citibank was challenged in Germany, but successfully demonstrated to the German government officials there how its system protected data in the United States, and it has since operated without conflicts.

Given that sufficient services are available with adequate privacy assurances, and no really grievous well-publicized privacy violations occur, the need for and nature of additional privacy regulation for Internet, over and above the already existing laws and regulations in the consumer protection area, are likely to remain cloudy and uncertain.

1.15 Privacy in a Electronic Transaction Environment

The previous discussion generally argues that the customer is already in control over what information should be provided to what company and for what purposes. There are already various consumer protection laws on the books, such as the Fair Credit Reporting Act, which forces banks to let consumers know they may "opt out" of information sharing, which includes both the internal use of the data for cross-marketing and selling the data to third parties. Additionally, the customer can be educated to be cautious in giving out

private information to any but well-known and trusted service providers who voluntarily provide ample warning to the customer, what they intend to collect and for what purpose. But there are some special issues and concerns in the on-line world.

Some information can be collected without the customer's direct knowledge. In some cases, data can be collected without the customer's knowledge. Information can be captured without requiring the user to explicitly provide it. For example, a user's navigation clicks can be stored by the client as "cookies" or as hidden fields in URLs and forms, accessible by the service provider. Information collected from the user as part of the service session can be collected and stored by the server, or it can be stored as part of a secure socket layer (SSL) session index (if the HTTP session is cryptographically protected). For example, a web server can measure, records and stores a customer's actions while visiting their web site and from transactions they process. Information concerning the customer can also be captured from properties contained in customer email addresses and Internet service descriptions. This is a concern because it is being obtained without informed customer consent (either implied, opt-out, or specific, opt-in).

A related privacy concern deals with infrastructure-related databases. For example, records of domain name registrations and address allocations have traditionally been public in order to permit users of other domains or spaces to track down problems and get assistance with resolving them. But, in recent years, those databases have been captured and utilized for targeted marketing purposes and that practice has led to strong suggestions that the data not be public.

The ability of a service provider to collect this type of information should be common knowledge but customers are often unaware of this capability. The consciousness and concern of the public regarding these indirect means of information capture is increasing. Responsible on-line service providers are beginning to alert their customers when this data is being collected, and how the collected information will be used. Technology solutions are being developed that would give the customer greater control, including blocking, over the collection of this sort of information. In fact technology plays an important role in privacy protection over the Internet.

The acceptance and practical implementation of most privacy approaches is still unknown. Most of the privacy approaches rely on technology solutions. For example, encryption is required to prevent unauthorized third parties from eavesdropping and intercepting the exchanged private information. Authentication technologies are needed to make sure that the transacting parties are who they claim to be and that the information provided is authentic and has not been tampered with by eavesdropping third parties. Implementing encryption and authentication over the Internet has its own set of issues ranging from issues of interoperability, cost, performance, scalability and legal and regulatory restrictions that are discussed elsewhere in this document.

Additional technology solutions have also been proposed to assist in the implementation of privacy protections. One of the most well known is the Platform for Privacy Preferences (P3P), proposed by W3C. P3P is a technology that makes possible a kind of automated assistance in the screening of information requests and control over the delivery of requested information, including a negotiation of privacy terms between the individual and the service provider the information. It operates sort of like a digital analogue to caller id and blocking of caller id, where the requesting party wishes to know who is phoning, but this information can only be provided if the calling party does not block the request.

P3P increases the explicitness with which privacy policies are expressed, allowing the user and the service provider to specify and match for each data item, the terms of usage (e.g. how the information will be used, for what purpose and who the information will be shared with). This includes information not explicitly supplied by the user, but collected indirectly, as just discussed in the previous paragraph.

In principle this technology sounds quite promising. It protects the user while minimizing manual intervention. These mechanisms may however not be workable in practice. For example, the user may find the technology too complex and/or not acceptable. Specifying ones privacy preferences down to each data

element may prove too daunting to the user. It could require the user to either set as many as 80 or more parameters, or rely on a program that can map/infer these parameters from a smaller set of simpler higher level privacy preferences, or through learning customer preferences by observing customer behavior. Alternately, the system can simply work with default settings that can be over-ridden by the user. Further complicating this technology is that the user preferences may involve too many variations. In fact, the user may change his/her mind and preferences frequently. And of course for P3P to work, it needs to be implemented on top of good privacy and authentication infrastructure which have implementation issues of their own that are discussed in subsequent sections.

Customer provided information is unreliable and varied. Further adding to the confusion surrounding customer supplied information is the underlying complexity surrounding any individual identity. We all are in actuality many different individuals with different roles and attributes. For example, a person can simultaneously be a father/mother, husband/wife, corporate officer, consumer, advisor, patient, and member of a number of different lifestyle organizations (e.g. Gay and Lesbian, Black American, College alumni). We tend to often keep these different identities separate and in very different compartments of our lives. These various identities and roles can lead to very different information being provided and inferred by a service provider depending upon the context in which the data is collected. The customer may wish to supply different information, for different persona, service providers, and circumstances.

The customer may even choose to provide the service provider with inaccurate or incomplete information. This may be deliberate; e.g. as a means of ensuring privacy is not violated, to ensure eligibility for some service, or for sheer delight in making mischief. It also might be inadvertent; e.g. in error. So it is likely that the disclosure of information involves more than deciding which information items to release under what conditions of privacy. It also concerns which version of the information items is provided, the context under which the information is provided, and the need of the service provider to check the accuracy and authenticity of the information provided.

The customer can't always appreciate all the different ways bits of information can be combined and used? The user, or their surrogate program, may not truly appreciate the actual information value contained in a piece of information when combined with other data items and make poor privacy preference selections that they will be unhappy with. For example, although an individual data item by itself might not appear to pose a privacy concern, when combined/associated with other similarly seeming harmless bits of information, often collected at another time and circumstance, may provide insights whose disclosure in the wrong hands would be of great concern. For example, a customer might be concerned if the money and purchases made on two different credit cards from two different companies were combined. It might reveal a shaker financial history than either set of data taken alone would show.

The issue of the use of agents, proxies and brokers on behalf of the consumer adds complexity to the privacy issue, especially when they are software robots. P3P, which was just discussed above, allows both user privacy preferences and service provider privacy principles to be placed in a form that is suitable for unambiguous interpretation by software agent programs. Software agents are likely to be used by many other applications in addition to P3P. These se agents raise a whole set of additional issues. For example, can a software agent be trusted? Authenticated? How does one bestow and verify that the agent has clearly recognizable authorizations? Who is liable if the agent makes a mistake or violates the user's privacy.

There are some instances where customer permission might/should not be required. Collecting information about one's customers might be needed by the service provider in order for them to manage fraud and resolve disputes. In this case the collected personal information allows the service provider to detect unusual practices and anomalies that can help to spot attempted fraud, and to challenge and authenticate transacting parties to verify that a transaction is legitimate and has the consent of all involved parties. It can also be used to identify, catch, and prosecute criminals. Other examples might be government reporting requirements for criminal prosecution, for collection of taxes, census and statistics-taking and other purposes. But the customer can be made aware of the collection of this information and the use of this information can be restricted to just the stated purposes.

There are cases where the customer but can be pressured into providing information. A firm accepting some risk or liability on behalf of its customer has the right to request information needed to help it manage and price its risk. For example, a financial firm that grants a customer a loan, providing money on credit, is assuming a risk that the customer might default. The financial firm has the right to request information that would give it some confidence that the customer has the capacity and will to repay the loan. That seems a fair exchange – sensitive personal information for a needed product – e.g. a loan. But what if the firm also plans to sell the information to other third parties for a profit? The customer may not want their data used for any purpose other than that required for processing the loan, credit or other related service, but needs the offered service (e.g. loan) so badly that it is forced to accept the firms terms and to allow them to resell the data. Should a consumer be protected against this pressure? The notion that users will be able to explicitly choose to exchange privacy for access to goods, information, or other benefits may not work well when a broad range of alternatives does not exist. Just as, if there are few suppliers of a physical good, users often have little choice of price or quality, there may often be no practical way to both obtain goods or information and preserve privacy.

Privacy concerns varies greatly by the nature of the transaction/interchange. Concerns over privacy and the need for authentication of the information provided vary greatly by the nature of the transaction. Examples include:

1. A friend to share information with – social/personal
2. A merchant to purchase something from – commercial, difference between high value and low value transactions
3. Chat room conversation – informal, social/personal
4. Entering into a business relationship – commercial
5. Applying for a loan – commercial
6. Communicating with your doctor – commercial

Of course the unreliability of the user information supplied can serve to protect personal privacy, particularly in social situations where the information provided cannot be as easily cross-checked and validated by any but an authorized commercial service provider.

This diversity of information-exchange needs and multiple roles played by any one individual suggests that a universal national identification is probably not a good idea. It will not satisfy all the various needs information exchange and for identification, and could destroy a means for an individual to ensure their privacy through selective dissemination of unreliable and varied information.

1.16 Anonymity versus privacy

One particular type of information disclosure involves the identity of the originator of a message. Notions of privacy suggest to some that there should be a right of anonymity, and anonymity may be particularly important for some types of political speech. But any such right must be balanced with the right to not interact with anonymous parties. For example: if spammers were uniquely identifiable as such, TCP transactions downloading SPAM could abort early, definitively ending SPAM as an issue. Additionally implementing reliable business transactions with the ability to resolve disputes and meet government regulations (such as taxation and money laundering reporting) often conflict with the desire for anonymity.

Historically, in the English and American Common Law principles, there is an inherent right to Anonymity, namely, one may take a fungible currency, such as gold, or even "dollars" and enter into a transaction with another party without either party needing to know the identity of the other party. There is recourse if the party sells defective goods, if there is a fraud perpetrated, or if some other crime or *Tort* results. However, neither party is generally required to reveal to the other their identity at any time prior to, during, or even after the transaction. If we accept the over one thousand years of precedent regarding anonymity, then we may ask how does it apply to the Internet. Specifically we may ask:

1. Can we create an environment wherein the "identity" we create can be kept private and secure and that we may enter into any form of communications and transaction on an anonymous basis?

2. Can we create a secure form of "money" which allows us to purchase and get involved in value based transactions without the need for identifying ourselves and again retaining our anonymity?

3. Can we apply all laws that ensure protection, as we have done for the course of the Common Law, and do so in an electronic anonymous environment?

It should be remembered that the United States was generally one of the few countries where identity papers were never carried during the twentieth century, with the exception of California, an artifact of fear of the Japanese during World War II. However, again as the world is opening up, other countries no longer require the possession of the infamous identity "papers", whereas the United States is now the only country that demands "papers", namely passports or the like, for inter-state transport by air. Identity and the governments "right" to access it and its concomitant other elements, has evolved in a rapid fashion in the US without and delimitation under the law. The issue is will the lack of anonymity in the Internet facilitate and accelerate this process of a lost right?

Fromkin has stated four types of computer or Internet anonymity"

"Before discussing remailers in any detail, it is useful to distinguish between four types of communication in which the sender's physical (or "real") identity is at least partly hidden: (1) traceable anonymity, (2) untraceable anonymity, (3) untraceable pseudonymity, and (4) traceable pseudonymity. The objective of these categories is to disentangle concepts that are otherwise conflated: whether and how an author identifies herself as opposed to whether and how the real identity of the author can be determined by others."

Fromkin further states:

"Anonymity has often had a good press in the United States. Perhaps the most famous political tract in this country's history, the Federalist Papers, were written pseudonymously. In 1958, The Supreme Court upheld the right of members of the NAACP to refuse to disclose their membership lists to a racist and surely vengeful state government,[31] a decision that I imagine almost every lawyer in the US would endorse today. Simultaneously, however, the United States has nurtured a deep-seated fear of conspirators and conspiracy,[32] with the McCarthyite witch-hunts of the 1950's being only one of the more lurid examples. Anonymous communication is of course a superb tool for the conspirator.

The US Constitution does not guarantee a right to be anonymous in so many words. The First Amendment's guarantees of free speech and freedom of assembly have, however, been understood for many years to provide protections for at least some, and possibly a great deal, anonymous speech and secret association."

[31] NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).

[32] I discuss the US hypersensitivity to conspiracy in A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709, 850-62 (1995).

Anonymity is in extremis the "right to be let alone". Generally we agree to that right if one is in their home. Generally we agree to that right if one is in ones auto or out by them selves. Generally we agree to that right between husband and wife or between people engaged in a sex act, unless otherwise banned by the state such as Bowers. How then do we extend that to transactions. That is the first step in the anonymity debate, can I use cash to buy something that I want no to know that I am buying.

Let us assume I want to buy a pornographic file. Let us assume it is legal to do so. Let us assume I do so with cash at a local store. Then do I have a right, say under the tort of "Public Disclosure of Private Facts" to prevent someone from telling third parties of this. Does the Government or a neighbor have the right to obtain the information and disseminate it in a public manner?

RIGHTS, LIBERTIES, AND FREEDOMS

The legal structure that we operate in the United States is a complex amalgam of laws, culture, and people. Notwithstanding the laws, and especially the Constitution, we see that the Supreme Court has the ultimate authority to "invent" expansions and "invent" contractions on our freedoms. Privacy is one of those areas. The classic example is Roe v. Wade, wherein the Court allowed abortion under the rubric of a right of privacy. At the other extreme, the Court has been closing down the rights of privacy that we would normally seek under the guise of delimiting the search and seizure limitations.

The issue hereunder is the following:

What do we mean by privacy? This is a definitional problem and in the case of the law it may be addressed in one of two ways. First we can create a law to protect privacy, in which case we can define it and thus delimit it. Second, we can address a case process wherein we seek a court to rule on some case.

The issues of rights, liberties and freedoms is a set of discussions in the theory of laws. Cantor has presented an interesting structural description of the types of schools of legal studies and we find this useful to review so as best understand where the issue of privacy may find a home and where it may be attacked. The Cantor categories are as follows:

1. ***Justice and Liberty:*** Cantor states that this school is founded on the approach of Maitland. It states that there is an interaction between legal ideas and societal contexts. It is a school that attempts to integrate many features of a culture into the law, and that views the law a vehicle for social and societal change.

2. ***Marxist:*** This is the classic Marxist approach which states that the law and the legal system is just a tool of industrialists to maximize their profits.

3. ***Feminist (Foucault):*** The law is a tool for oppression, it serves holders of power, and it has been a general tenet of the feminist school which views laws as oppressive tools of the male dominant society to keep women in their place. DeCew discusses this school of privacy especially Katherine McKinnon's approach to legal studies. The a priori view creates a ad hoc propiter hoc form of argument, which makes it very difficult to understand and develop the issue of privacy.

4. ***Psychoanalytic (Lacanian):*** Law is considered a psychosexual control and dominance mechanism.

5. ***Structuralist (Levi-Strauss) :*** Mind and society combine to elicit the law. This is reminiscent of the Society of the Mind, by Marvin Minsky, one of the fathers of Artificial Intelligence at MIT. The theory is that the mind and society interact, that society can be better served by the understanding of the almost algorithmic interactions and that the optimization of these interactions is an improved embodiment of the law.

6. ***Deconstructionist :*** This is classic Derrida. The Derrida school of deconstructionist though must place you in the mind of both the authored and the reader, each having differing planes of reference. The "original intent" doctrinal approach to the Constitution is somewhat a Derrida approach, what did the founding fathers mean. Unfortunately, even there, the simple battle between Federalists and Anti-Federalists is best reflected in the conversation tempus proximis, not necessarily in the "self serving" writing of those attending.

7. ***Economics :*** This is the Chicago Schools as described best by Posner. The discussion on Posnerian theory is that every interaction is at heart an economic transaction. The state should understand that and the state is or is not a party to that transaction. The law is a reflection of what the state has as an interest in the transaction, and it reflects through a quasi economic metric how it values that transaction.

These seven "schools" as described by Cantor are a useful construct to develop an better understanding on how best to reflect upon privacy. W\Canto does not include the Etzioni type Communitarianism, but one may place that in the Justice and Liberty school of modernism, wherein what is good for all applies. I would argue that Rawls belongs in that school as well.

1.17 Definitions

DeCew states the following:[33]

"Two points should be kept in mind. First, … I shall not place special interest on privacy as a right, as opposed to a claim or interest. A "claim" is often described as an argument that someone deserves something. A "right" is then a justified claim; justified by laws or judicial decisions if it is a legal right, by moral principles if it is a moral right."

Judge Thomas C. Cooley in 1880 in his treatise on *Tort*s stated that privacy is the "right to be left alone".[34] Warren and Brandeis in 1890 further expanded upon this and explained privacy in a far reaching manner.

DeCew further paraphrases Catharine MacKinnon in characterizing two general types of privacy:[35]

"…privacy has developed to protect both (i) an individual interest in avoiding disclosure of personal matters, as well as limiting government intrusion on a regulation of these matters, and (ii) an interest in independence in making certain kinds of important decisions regarding body, home, and lifestyle."

This simply stated means the we have a set of two privacy rights; the right to conceal and the right to act. The right to conceal we shall call the right of anonymity and the right to act we shall call the right to choose.

1.18 Rights

Rights are those elements provided by or under the law, whatever law may be controlling, by which we as individuals, or collectively as a people may act without fear of the government or any other controlling force seeking to intervene on our actions in any way. Thus, we have, under the U.S. Constitution, some defined rights of free speech. It is not as free as we may think it to be, but it is free to a great extent.

---

33 DeCew, p. 27.

Keeton & Prosser, p. 851.

[34] Keeton & Prosser, p. 849.

[35] DeCew, p. 82.

In Blackstone's Commentaries on the law, he establishes the fundamental rights of Englishmen[36]:

1. Personal security:

2. Personal liberty:

3. Private property:

Finnis develops in some detail the Hoheld ideas of rights.[37] They can be summarized as follows:

Definition: Let P_n and P_m be persons n and m respectively. A person may be either natural or legal.

Definition: Let $F_{n,m}$ be any act from P_n to P_m.

Definition: P_n has a claim-right *than Pm should $F_{n,m}$, if and only is Pm has a* duty *to P_n to perform act $F_{m,n}$. $F_{n,m}$ and $F_{m,n}$ are* reciprocal *acts.*

For the time being this definition of a claim-right assumes a definition of a duty and a definition of reciprocal. We shall defer the discussion on these until latter.

Definition: P_m has a liberty *relative to P_n to perform an act $F_{m,n}$, if an only if P_n has* no-claim-right *that P_m must perform act $F_{n,m}$.*

Definition: P_n has a power *relative to P_m to perform act $F_{n,m}$, if an only if P_m has a* liability *to have his legal position changed by P_n executing $F_{n,m}$.*

Definition: P_m has an immunity *relative to P_n performing act $F_{n,m}$, if and only if P_n has no power, a* disability*, to change P_ms legal position by performing act $F_{n,m}$.*

Thus claim-right, liberty, power, and immunity are defined in terms of duty, no-claim-right, liability, and disability. Albeit somewhat circular, these constructs can be used to establish a certain framework for the establishment of what rights does one expect for example for privacy.

1.19 Rights of Man

The Rights of Man, established at the beginning of the French Revolution, were an alternative to the Bill of Rights as established in the US Constitution. The key elements relating to privacy are as follows:

2. The aim of all political association is the preservation of the natural and imperceptible rights of man. These rights are liberty, property, security, and resistance to oppression.

4. Liberty consists in the freedom to do everything which injures no one else; hence the exercise of the natural rights of each man has no limits except those which assure to the other members of the society the enjoyment of the same rights. These limits can only be determined by law.

[36] See Posner, EoJ, p. 15.

[37] Finnis, p. 199.

5. Law can only prohibit such actions as are hurtful to society. Nothing may be prevented which is not forbidden by law, and no one may be forced to do anything not provided for by law.

6. Law is the expression of the general will. Every citizen has a right to participate personally, or through his representative, in its foundation. It must be the same for all, whether it protects or punishes. All citizens, being equal in the eyes of the law, are equally eligible to all dignities and to all public positions and occupations, according to their abilities, and without distinction except that of their virtues and talents.

7. No person shall be accused, arrested, or imprisoned except in the cases and according to the forms prescribed by law. Any one soliciting, transmitting, executing, or causing to be executed, any arbitrary order, shall be punished. But any citizen summoned or arrested in virtue of the law shall submit without delay, as resistance constitutes an offense.

9. As all persons are held innocent until they shall have been declared guilty, if arrest shall be deemed indispensable, all harshness not essential to the securing of the prisoner's person shall be severely repressed by law.

10. No one shall be disquieted on account of his opinions, including his religious views, provided their manifestation does not disturb the public order established by law.

11. The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by law.

17. Since property is an inviolable and sacred right, no one shall be deprived thereof except where public necessity, legally determined, shall clearly demand it, and then only on condition that the owner shall have been previously and equitably indemnified.

1.20 Bill of Rights

Consider the following elements of the Bill of Rights. Each may have some element of a privacy right established:

Article I. : Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Clearly this allows for the privacy of thought and religious expression. It also may be extended by the assembly clause to extend privacy from the individual person to the group. The expression

Article II. : A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

One view of this is the privacy right to possession and protection of the person. This has not been deemed an approach by the Court but in the sense of the right of “the people” both collectively and individually is the essence of the right of privacy as both individual and group.

Article III. : No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Article IV. : 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.

Article V. : No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Article VI. : In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

Article VII. : In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.

Article VIII. : Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

Article IX. :The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

1.21 Natural Law

Natural law is an old concept that basically means that there exists a set of principles, methods to evaluate those principles, and the ability to generate laws from the principles and methods. Consider what Finnis presents as the basis for natural law.[38] Namely that:

(i) There exists a set of ***basic principles (BS)*** reflective of a basic and generally agreed set of human goods to be sought or realized,

(ii) There exists a set of ***methods and procedures (M&P)*** that allow for the distinguishing of "sound" from "unsound" and allow anyone to distinguish what is "reasonable" and what is "unreasonable",

(iii) That the combination of BS and the M&P allow for the establishment of general moral standards, GMS.

Latter Finnis states[39]:

"Natural law – the set of principles of practical reasonableness in ordering human life and human community – is only analogically law…"

In contrast, Aquinas, in Question 94 derives natural law from Divine Law.[40] The issue in Aquinas is that there is a hierarchy of these laws, Divine, Natural, and Human. He takes a great deal of time developing the

[38] Finnis, p. 23.

[39] Finnis, p. 280.

essential linkage of the natural law being what we a culture of humans use as the basis for Human law which is derivative from the ruler. The concept is that natural law precedes human law, human law exists only because divine law recognizes the king.

1.22 Common Law

As Eisenberg states, the common law has two major types of propositions; doctrinal and social.[41] Common law is that collection of legal rules which are the concatenation of what has gone before. In the areas of torts and contracts common law principles dominate. Specifically Eisenberg states[42]:

"What then does the common law consist of? It consists of the rules that would be generated at the present moment by application of the institutional principles of adjudication. I call this the generative conception of common law…"

CONCLUSIONS

Privacy is an evolving concept. It has been developed within the regimes of Constitutional law, Tort law, US Law, and the broad basis of natural and common law. It has been viewed as the right to be left alone, a property right, an economic right, and most recently as a right to control ones reproductive capabilities and actions. In the electronic world it has been viewed since September 11, 2001, as less of a right and more of a liability since most government agencies want unfettered access to individual's thoughts, ideas, proclivities, and intended actions. At what point does the governments powers end and the citizens rights begin. The issue here is "government powers" and "citizen rights". Not necessarily or even at all the rights of enemies or foreigners. Not the rights of the government since the government has powers given to it by the people as stated in the constitution. But the issue is what rights do American citizens, and by extension other respective citizens have.

The area of privacy protection over the Internet is complex involving many conflicting requirements, unresolved issues and unknowns. These issues include making the proper trade-off between the needs of society vs. the rights of the individual, and between the benefits of personalization vs. abuse of privacy. For example, there are conflicts between the need for information in support of criminal prosecution (e.g. money laundering, fraud control, tax evasion) versus concerns for individual privacy protection. There are many unknowns regarding the likely acceptance and effectiveness of associated privacy solutions.

Can they be practically implemented? Is the best approach self-policing or regulation, user opt-in or opt-out? Will they be acceptable from an economic and practical implementation? Are they acceptable from a cost, convenience, performance, and ease of use viewpoint? Will they truly prove effective in helping to enforce privacy policy and providing the desired privacy protections? Will they result in acceptable risk exposure? Can they accommodate international and cultural differences? In light of these unresolved issues and unanswered questions, a hands-off, wait-and-see policy is recommended for the time being with respect to any special legislation. We should let the multiple solutions and market forces work themselves out.

What might be helpful is a program directed at educating users with respect to privacy cautions and the tools they have available today to alleviate these concerns.

---

[40] Aquinas, p. 54.

[41] See Eisenberg, p. 1.

[42] Eisenberg, p. 154.

REFERENCES

Aquinas, Thomas	Treatise on Law, Summa Theoligia, Questiones 90-97, Regnery (Washington) 1996.
Boyd v. US	116 U.S. 616 (1886)
Cantor, N.F.	Imagining the Law, Harper (NY, NY) 1997.
Cooley, T.C.	Law of *Tort*s, Little Brown & Co. (Boston, MA) 1888.
Cunningham, R.A., et al	The Law of Property, West Publishing (St Paul, MN) 1993.
DeCew, Judith W.	In Pursuit of Privacy, Cornell Univ Press (Ithaca, NY) , 1997
DeCew, Judith, W.	In Pursuit of Privacy, Cornell University Press (Ithaca, NY) 1997.
Dobbs, Dan B.	The Law of Torts, West Group (St Paul, MN) 2000.
Eisenberg, Melvin A.	The Nature of the Common Law, Harvard (Cambridge), 1988.
Etzioni, Amitai	The Limits of Freedom, Basic (New York) 1999
Finnis, J.	Natural Law and Natural Rights, Oxford (Oxford) 1980.
Finnis, John	Natural Law and Natural Rights, Oxford Press (Oxford), 1980
Froomkin , A. Michael	Anonymity and Its Enmities, Associate Professor of Law, University of Miami School of Law, http://acr.law.miami.edu.
Glancy, Dorothy	Privacy and the Other Miss M, Northern Illinois University Law Review, Summer, 1990, Symposium on the Right to Privacy: After One Hundred Years, 10 N. Ill. U. L. Rev. 401
Griswold v. Connecticut	381 U.S. 479 (1965)
Habermas, J.	Between Facts and Norms, MIT Press (Cambridge, MA), 1996.
Hayek, F.A.	The Road to Serfdom, University of Chicago Press (Chicago, IL), 1994.
Holmes, O.W.	The Common Law, Back Bay Books (Boston), 1963.
Keeton, W.P.	Prosser and Keeton of *Tort*s, West Publishing (St Paul, MN) 1984.
Mell, Patricia	Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, University of California, Berkley, Technology Law Journal, Vol. 11, Issue 1, Spring, 1996.
Mill, John S.	On Liberty, Penguin (London) 1974.
Olmstead v. US	277 U.S. 438 (1928)
Pipes, Richard	Property and Freedom, Knopf (New York) 1999

Posner, R.A.	The Problems of Jurisprudence, Harvard University Press (Cambridge, MA) 1990.
Posner, R.A.	Law and Literature, Harvard University Press (Cambridge, MA) 1998.
Posner, R.A.	The Problematics of Moral and Legal Theory, Harvard University Press (Cambridge, MA) 1999.
Posner, R.A.	Economic Analysis of Law, Little, Brown & Co (Boston, MA) 1992.
Posner, R.A.	The Economics of Justice, Harvard University Press (Cambridge, MA) 1983.
Posner, R.A.	Overcoming Law, Harvard University Press (Cambridge, MA) 1995.
Pound, R.	The Spirit of the Common Law, Marshall Jones Co (Boston, MA), 1921.
Rawls, J.	A Theory of Justice, Harvard University Press (Cambridge, MA), 1971.
Rawls, J.	Political Liberalism, Columbia University Press (New York), 1996.
Roe v. Wade	410 U.S. 113 (1973)
Schoeman, Ferdinand D.	Privacy and Social Freedom, Cambridge Univ Press (Cambridge) 1992
Schumpeter, J.A.	Capitalism, Socialism, and Democracy, Harper & Bros (New York), 1942.
Schumpeter, Joseph A.	Capitalism, Socialism, and Democracy, Harper (New York), 1975.
Standler, Ronald, B.	Privacy Law in the USA, http://www.rbs2.com, May, 1998.
Stone, G.R. et al	Constitutional Law, Little, Brown & Co (Boston, MA) 1991.
Tribe, L.H.	American Constitutional Law, Foundation Press (Mineola, NY) 1988.
Tribe, L.H., M.C. Dorf	On Reading the Constitution, Harvard University Press (Cambridge, MA) 1991.
U.S. Department of State	Country Reports on Human Rights, Privacy, 1997.
Whalen v. Roe	423 U.S. 1313 (1975)

APPENDIX B: KEY SUPREME COURT RULINGS

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
NAACP v Alabama 357 U.S. 449 1958	1958	Civil Rights	The case was about Alabama trying to force the NAACP to disclose its members list as a part of registering in Alabama. The Court said: "*This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. When referring to the varied forms of governmental action which might interfere with freedom of assembly, it said in American Communications Assn. v. Douds, supra, at 402: "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature." Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order.* ***Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs****."*	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Griswold v Connecticut 381 U.S. 479 1965	1965	Privacy	Griswold was the Executive Director of Planned Parenthood in CT. CT had a law against selling or prescribing contraceptive devices. PP sued CT to be able to provide birth control methods to the CT citizens, and in this case specifically a husband and wife. The Court first granted that the married couple, part of Griswold et al, had standing to assert a constitutional right and second that the CT law violated the right of marital privacy which was covered by the penumbra of the Bill of Rights. Justice Douglas delivered the opinion. The logic for Douglas for establishing standing was based upon CT having arrested and convicted the defendants, albeit for a $100 fine. Douglas states*: "In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion."* and also *"The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."* Thus for the first time a "right to privacy".	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Roe v Wade 410 U.S. 113 1973	1973	Privacy	Roe is the classic case. She was pregnant and brought a class action suit against the constitutionality of the Texas law which made abortions illegal. Justice Blackman rendered the opinion. Roe claimed that she had protection under the 1st, 4th, 5th, 9th, and 14th Amendments. The Court stated that the Texas act was unconstitutional The claimant used Griswold and the penumbra theory under the 14th Amendment. The Court went through the history of abortion laws demonstrating that they were of recent history. The classic statement is that the Hippocratic oath expressly prohibits abortion, and that almost all physicians in the US take that oat at their graduation from medical school, but the Court states "the Oath originated in a group representing only a small segment of Greek opinion.." The Opinion then states: "The Constitution does not explicitly mention any right of privacy. In a line of decisions…the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution." This then became the basis of the Opinion.	
Whalen v Roe 423 U.S. 1313 1975	1975	Privacy		
U.S. v Miller 425 U.S. 435 1976	1976	Privacy		

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Bowers v Hardwick 478 U.S. 186 1986	1986	Privacy	Justice White delivered the decision. Charged with violating the Georgia law of sodomy with another adult male in the bedroom of his home, respondent Hardwick (respondent) brought suit in Federal District Court, challenging the constitutionality of the statute insofar as it criminalized consensual sodomy. The court granted the defendants' motion to dismiss for failure to state a claim. The Court of Appeals reversed and remanded, holding that the Georgia statute violated respondent's fundamental rights. The Supreme Court held: The Georgia statute is constitutional. (a) The Constitution does not confer a fundamental right upon homosexuals to engage in sodomy. (b) Against a background in which many States have criminalized sodomy and still do, to claim that a right to engage in such conduct is "deeply rooted in this Nation's history and tradition" or "implicit in the concept of ordered liberty" is, at best, facetious. (c) There should be great resistance to expand the reach of the Due Process Clauses to cover new fundamental rights.	
Boyd v U.S. 116 U.S. 616 1886	1886	Search	This was a case resulting from a Customs search and subsequent demand by the law authorities for certain documents that The district attorney in New York ordered the defendant to produce invoices showing certain plate glass was imported illegally, against the 1874 Customs Act. The defendants complained about the constitutionality of the law. Ruling summarizes prior cases and laws. States 1789 statute for custom duty collection as stating that searches for Customs violations are permitted. Court used this reference since it was same Congress which passed Bill of Rights (original intent). Court goes o to stress the Colonial opposition to English writs of assistance which empowered English to have warrantless searches. The Court details John Adams opposition to this and further strengthens the original intent of the framers as opposing warrantless searches and seizures. Court refers again to 1789 Custom Act and restates acts restriction "cases and circumstances where they might be compelled to produce…by the ordinary rules of proceeding.." Court further states that "any compulsory discovery…or compelling the production of …books and papers…is contrary to the principles of a free government. It is abhorrent.." Court overthrew the ruling and remanded case.	First case that clearly lays out the limitations of search and seizure without warrants. It clearly states the "intent" of the framers of the Constitution to make it unlawful and more importantly abhorrent to demand the delivery of "papers" to the government. It does not change the Customs right to search.

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Carroll v U.S. 267 U.S. 132 1925	1925	Search	This case concerned the search of a vehicle without a warrant in an attempt by the police to discover liquor in violation of prohibition. The police suspected that the defendant was involved in some form of bootlegging, but the stop occurred some time after their initial suspicions, with no further evidence having been obtained in the interim. In the early days of the automobile the Court created an exception for searches of vehicles, holding in Carroll v. United States 55 that vehicles may be searched without warrants if the officer undertaking the search has probable cause to believe that the vehicle contains contraband. The Court explained that the mobility of vehicles would allow them to be quickly moved from the jurisdiction if time were taken to obtain a warrant. Thus the Court upheld the conviction and made a distinction based upon the auto as the element being searched.	This starts to begin the process of delimiting the areas of protection. The literal interpretation is that the auto is not secure and that it is akin to placing your property in plain view, even if it is not. This may mean that we could expect that Boyd could protect the computer in ones home but that a "packet" moving over a network may go un-protected via Carroll.
U.S. v Di Re 332 U.S. 581 1948	1948	Search	This case referred to a defendant possessing illegal gas rationing coupons. The police had prior knowledge that certain persons would be carrying and trafficking in illegal gas ration coupons. The defendant was stopped in a vehicle and one of the passengers held the coupons in plain view to the police officers. DiRe was taken out of the auto and frisked and the coupons were found on his person. The driver, Reed, was the suspect and the police had no knowledge of Di Re. The Court reviewed Carroll and stated that Carroll seemed to imply that warrantless searches were appropriate for an auto. The Court made a distinction here about Carroll allowing an auto search and the DiRe case of a search of the person. The Court states: We are not convinced that a person, by mere presence in a suspected car, looses immunities from search of his person to which he would otherwise be entitled." The conviction was overturned.	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Terry v Ohio 392 U.S. 1 1968	1968	Search	Police officer sees a group of men acting suspiciously. Based upon that observation he then stops and frisks them. He finds a weapon, upon which discovery they are arrested. The men object on Fourth Amendment grounds of an unlawful search and seizure. The observation lacks probable cause but the "stop and frisk" is not a seizure and a search under the Fourth Amendment. The Court views "stop and frisk" as separate from "search and seizure". The stops based upon police officers experience and the frisk is for the safety of officer and public and limited to the "discovery" of weapons. The Court justifies "stop and frisk" as follows*: "This scheme is justified in part upon the notion that a "stop" and a "frisk" amount to a mere "minor inconvenience and petty indignity,"* The Court stated: "*In our view the sounder course is to recognize that the Fourth Amendment governs all intrusions by agents of the public upon personal security, and to make the scope of the particular intrusion, in light of all the exigencies of the case, a central element in the analysis of reasonableness*." The conviction stood.	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
U.S. v Ross 456 U.S. 708 1982	1982	Search	Justice Stevens delivered the Opinion. In this case a police officer obtained a tip stating that a certain person was selling narcotics. In fact the information stated that the individual had just completed a sale. The informant detailed the perpetrator and his vehicle. The police did a check on possible perps and found the defendant. The fund the defendant and then the police took defendants keys and opened trunk. A bag was found in trunk and in the bag was cash and on the bag was narcotics. The Court of Appeals reversed the decision. The Appeals Court used Carroll to stated that the police could search trunk but not the bags. The Court restated the Opinion Carroll that a warrantless search of an automobile stopped by police officers who had probable cause was not unreasonable under the 4th Amendment. In fact the limitation is on "unreasonable" search and seizure. The Court also again reiterated the fact that the Founding Fathers themselves made a distinction of warrants for homes but warrantless for vessels, thus vehicles. The Court ruled that the police could do a warrantless search based upon the long standing fact that the Court had recognized the impracticality of securing a warrant in cases involving a vehicle. The Appeals Court decision was overturned and the search and its fruit permitted.	
Wyoming v. Houghton Wyo. 98-184 1999	1999	Search	This recent case involves a routine traffic stop. At the stop the police officer notices a hypodermic syringe in plain view in the driver's pocket. The driver admitted to taking drugs. The police officer then searched the glove compartment. There he found drugs. The Court upheld the conviction by establishing that the police had probable cause. The cases used were Carroll and Ross as described above.	
Lochner v People of the State of New York 198 U.S. 45 1905	1905	Substantive Due Process		

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Muller v State of Oregon 208 U.S. 412 1908	1908	Substantive Due Process		

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Olmstead v U.S. 277 U.S. 438 1928	1928	Wiretap	Justice Taft delivered the decision. Olmstead was a leading conspirator in a bootlegging ring. He moved liquor from Canada to the US. The police put taps on the telephone lines of all the conspirators. The taps were placed outside of the homes and were done without warrants. The information gathered from the taps were used to convict. The Court stated: "The court held the Act of 1874 repugnant to the Fourth and Fifth Amendments. As to the Fourth Amendment, Justice *Bradley said (page 621): [277 U.S. 459]* *"Concurring, Mr. Justice Miller and Chief Justice Waite said that they did not think the machinery used to get this evidence amounted to a search and seizure, but they agreed that the Fifth Amendment had been violated.* *But, in regard to the Fourth Amendment, it is contended that, whatever might have been alleged against the constitutionality of the acts of 1863 and 1867, that of 1874, under which the order in the present case was made, is free from constitutional objection because it does not authorize the search and seizure of books and papers, but only requires the defendant or claimant to produce them. That is so; but it declares that, if he does not produce them, the allegations which it is affirmed they will prove shall be taken as confessed. This is tantamount to compelling their production, for the prosecuting attorney will always be sure to state the evidence expected to be derived from them as strongly as the case will admit of. It is true that certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting, and, to this extent, the proceeding under the Act of 1874 is a mitigation of that which was authorized by the former acts; but it accomplishes the substantial object of those acts in forcing from a party evidence against himself. It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure.""* Olmstead v. United States, 32 one of the two premises underlying the holding that wiretapping was not covered by the Amendment was that there had been no actual physical invasion of the defendant's premises; where there had been an invasion, a technical trespass, electronic surveillance was deemed subject to Fourth Amendment restrictions.	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Berger v New York 388 U.S. 41 1967	1967	Wiretap	Justice Clark delivered the Opinion. Berger was convicted in bribery of a government official. A bar owner had complained that officials from NY State Liquor Board had entered his bar and without cause seized his books. The bar owner said it was in reprisal for failing to pay bribe. On this basis an wire tap was authorized by NY court for 60 days on the office of official. Based on wiretap evidence the warrant was extended. Evidence was obtained on two other bars being shaken down. Defendant stated that this information was not legally obtained since the warrant was for evidence on the first case. Court ruled that this was un-constitutional. The warrant was too broad in scope.	

Supreme or State Court Ruling	*Year*	*Area*	*Principles of Ruling*	*Application to Privacy*
Katz v U.S. 389 U.S. 347 1967	1967	Wiretap	Justice Stewart delivered the Opinion. The defendant was convicted for a violation of the wagering acts. The FBI recorded his calls without a warrant by attaching a recording device on the outside of a telephone booth. The defendant tried to pose the following two questions: *"A. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth. [389 U.S. 350]* *B. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution."* The Court rejected this posing. The Court stated: *"The Government stresses the fact that the telephone booth from which the petitioner 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. But what he sought to exclude when he entered the booth was not the intruding eye -- it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen…. To read the Constitution more narrowly is to ignore the vital role that* the *public telephone has come to play in private communication."* Further; *"What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*." Finally the Court states: "*Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored "the procedure of antecedent justification . . . that is central to the Fourth Amendment,"{ 24} a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case*." The Fourth Amendment protects people, not places.	