

CERIAS Tech Report 2004-33

PRIVACY AND TECHNOLOGY: DEFINITION AND POLICY

by William A. Fraunhofer

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

PRIVACY AND TECHNOLOGY
DEFINITION AND POLICY

A Thesis

Submitted to the Faculty

of

Purdue University

by

William Arthur Fraunhofer

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Arts

August 2004

To my father, Valentine Frauenhofer, who instilled in me the desire to study what I had at hand and to learn about that which was not.

To my mother-in-law, Lyn Hassman, whose encouragement enabled this all.

ACKNOWLEDGMENTS

I wish to thank those who have supported me in this endeavor. Dave Wilson and James Hinde have been good friends and supporters for the two years at Purdue. The Faculty at Purdue and especially the Faculty and Staff of CERIAS are to be thanked for their efforts. I particularly wish to express appreciation to Professor Spafford, Professor Raskin, Professor Thompson and Marlene Walls.

I also need to thank my wife whose two year commitment to the program was at times stronger than mine. She managed the family and there is no expression of gratitude that I can make that would be adequate enough.

PREFACE

Amongst other things, the Supreme Court is famous for the observation that they do not know what obscenity is but that they can tell it when they see it. Privacy is in a similar bad state. Most people cannot define privacy, but they are familiar with it, especially when they lose it.

I add my insight to the issue by attempting to define privacy. Privacy is at stake because technology is constantly eroding what privacy we have left. Is this wrong or is it a natural state of affairs?

Looking at history, it is easy to see that especially power hungry despots, to invade the privacy of members of society, have often used technology of various forms. What is of great concern these days is the ready availability of snooping technology. In the United States there are stores specializing in tools to allow a woman spy on and catch a cheating husband. Obviously, these tools can be turned in other directions to break into the most secret elements of human life.

As we watch privacy erode we complain and some of us are moved to do something. A lack of definition inhibits us. How can we make regulations to stop something that we cannot even define? We cannot because we do not know where the boundaries are.

Using the definition I have created, I then derive some policy suggestions. This serves a two-fold purpose. First, I make some suggestions that might help the situation. Second, I use the policy to check my definition. While I am not an expert in policy I felt the exercise to be important.

Another check on the definition is based upon the global environment. For a definition to be maximally useful it should be exportable. I suffer from a common malady in this regard; I have a parochial view based upon the United States. I do not know of a cure but a way to relieve some of the symptoms is to adopt a global view and apply it to the best of my abilities.

TABLE OF CONTENTS

	Page
LIST OF TABLES.....	viii
LIST OF FIGURES.....	ix
ABSTRACT.....	x
CHAPTER 1 – HISTORICAL CONTEXT.....	1
Privacy as a Technological Development.....	2
Mosaic Law.....	3
Medieval Times.....	3
Industrial Times.....	4
Nineteenth Century.....	5
Twentieth Century.....	6
Summary.....	14
CHAPTER 2 – LEGAL HISTORICAL CONTEXT.....	17
American Watershed.....	18
Legislative Initiative.....	24
Summary.....	26
CHAPTER 3 – DEFINITION OF PRIVACY.....	28
Definition.....	29
Privacy and Technology.....	35
Ethical Considerations of Privacy.....	36
Expressive Privacy.....	37
Accessibility Privacy.....	40
Information as Property.....	43
Feminist Aspects.....	45
Summary.....	47
CHAPTER 4 – GLOBAL ISSUES.....	49
Europe.....	49
Australia.....	51
Asia.....	52
People's Republic of China.....	52
Japan.....	53
Republic of the Philippines.....	54
South America.....	54
Argentine Republic.....	55
Federative Republic of Brazil.....	55
United Mexican States.....	56
Africa.....	57

	Page
Summary.....	58
CHAPTER 5 – POLICY PROPOSAL.....	59
Stakeholders.....	59
Model.....	61
Government.....	64
Individuals.....	67
Company Responsibility.....	69
Cost-benefit Analysis.....	70
Summary.....	73
BIBLIOGRAPHY.....	74

LIST OF TABLES

Table	Page
TABLE 1 – Incremental Costs.....	72

LIST OF FIGURES

Figure	Page
FIGURE 1 – Timeline: Based on Chapter 1.....	16
FIGURE 2 – The Spectrum of Privacy.....	48

ABSTRACT

Frauenhofer, William Arthur M.A., Purdue University, August 2004, Privacy and Technology: Definition and Policy, Major Professor: Eugene H. Spafford

Many people believe that they have a right to privacy, but they also generally do not have a definition of privacy. Privacy can be divided into two categories: natural privacy and personal secrecy. Natural privacy is narrowly defined as that which is either discernible or inferable. Personal secrecy refers to attempts to limit the spread of discernible or inferable information. Based upon this distinction, I formulate some policies to help relieve this erosion of privacy. I also give a brief history of privacy and technology. Because privacy and technology issues are not limited to the United States I also provide a global perspective.

CHAPTER 1 – HISTORICAL CONTEXT

“In the beginning ...”,¹ and so the universe was created for all creatures. Eventually, man was formed but the biblical first man, Adam, was a solitary creature. He shared the earth with the animals and his deity. Given an omniscient deity, someone who knows every thought and act of man, is there privacy?

If we include a deity in the group of individuals who concern us in privacy, the universe turns into a single panopticon. Privacy would be a ridiculous concept and the entire discussion would be over.

Adam does not enjoy true privacy, in fact there is no privacy because the information cannot be withheld from someone nor is there anyone to avoid. It becomes an empty term in this situation.

Then, along comes Eve. Finally someone to hide from, someone Adam can share or withhold information from and someone who can do the same to Adam. Thus, with the creation of Eve, rights and duties amongst people come into existence.

Privacy can only exist if there is something to be held from another or if there is a place to seclude ourselves from others. It is a by-product of society.²

1 Bereshis (Genesis) 1:1, of the Judeo-Christian Bible.

2 I review progress and privacy in the European and American context only. The rest of the world was very active, but I have little information and really only intend this chapter to show that there has been some level of privacy that technology has eroded.

Early Christians needed to seclude themselves from their persecutors during the Roman era. By hiding themselves in the catacombs for services, they were able to keep their activities secret and therefore kept their lives. This was privacy, as it is colloquially known, against intrusion, based upon practical motivation.

Also, throughout time, military forces have kept their plans private. Consider the Trojan horse, an affair that would have been for naught and forgotten in history if the plan had not been kept private to the planners and executers.

My point so far has been that privacy has existed from the beginnings of society. As people began to interact with others in organized society, there was some form of privacy, and there was prying into the privacy of others. Curiosity seems to be a fundamental element of human existence.

Privacy as a Technological Development

Beginning with pre-history, societal groups, such as tribes and hunting parties developed. One may regard society as a technology. Society is created by humans to be used by humans for the furtherance of human goals. Even though other animals participate in societies, these groups are believed to be instinctual groupings, not the intellectual groupings that humans form.

Society as a technological device negatively impacts privacy by imposing requirements that its members interact. Essentially, society as a technology reduces the

privacy of individuals. However, society as a technology also created privacy. Privacy can be viewed as a technological development from this perspective.

Mosaic Law

Mosaic Law, derived from the five books of Moses and commonly referred to as the Old Testament, condemns many acts that would be considered invasions of privacy. Telling tales about someone, especially true tales, are condemned as “loshon hara” or the evil tongue [26]. The Shulchan Aruch, the codification of Mosaic Law, states that building a house so that one could look into someone else's bedroom is prohibited.

Among the ancient Hebrews, privacy was enhanced by the theocratic power and rules of the state. Violation of the law entailed not only the secular condemnation, but the truly held conviction was that the deity would also be displeased. This is a period that contributed to the common law interpretation of privacy and subsequent modern views.

Medieval Times

The middle Ages was a time of control by the Roman Catholic Church, and for part of this time there was a struggle between the religious and secular interests for power and the resulting compromises. To this day the Roman Catholic Church wields

some power in the face of strong nation states. It is the mix and compromise of this time that created the basis upon which modern privacy builds.

Papal authority allowed the church to investigate many aspects of private lives. The infamous Spanish Inquisition as well as inquisitions in other countries had the power to invade privacy as well as coerce information from people. Those who were forcibly converted lived in a state of continual fear of an investigator from the inquisition arresting them for some practice that was considered non-conformist.

Opposed to this were the relatively weak national governments. Truly, this was a time of fiefdoms, local control of an area by some lower level noble who wielded near total autonomy in the affairs of that region.

Privacy was not an affirmative state of affairs, but rather the vacuum created by secular and religious inability to interfere. Had modern technology been available, there would have probably been a great deal of monitoring and other invasions of privacy. The only question left would have been: "What is the hierarchy of who is monitored by whom?"

Industrial Times

As the medieval times moved into the religious reformation, a great deal of questioning about all sorts of dogma took place. Religious differences were the spark of this revolution, but scientific, philosophical, and economic differences began to be questioned.

Cities had been increasing in size and importance and these were the centers of this activity. Greater concentrations of people allowed the ideas to be refined and disseminated more readily.

Early technology had far reaching consequences. Consider the printing press. This invention was created to permit the making and selling of Bibles: an economic motive but one that obviously had far reaching consequences.

Bibles represented the religious information upon which the Roman Catholic Church was founded. By controlling the availability of Bibles, the church could control the availability of this information and thereby restrict the commentary and criticism on the church.

Printing Bibles allowed more people to have a Bible which added to the formation of sects based upon it. This in turn reduced the power of the church and increased the power of the secular.

Further, printing allowed for the creation of other books and newspapers that spread information about non-religious issues. This further strengthened the secular government to the detriment of the religious.

Nineteenth Century

The nineteenth century is important to privacy. Governments were well established as the power to deal with, the United States had put some restrictions on the invasion of privacy in the Constitution, and other countries were generating various laws

and regulations to protect the privacy of citizens.

As the century progressed, there were more instances of people asserting their rights. Court cases started to be heard and decisions were made that limited the government's ability to intrude on the privacy of a citizen.

Indeed this is the century in which the famous article by Warren and Brandeis ([37] pg. 29)³ was published. That article, published by the Harvard Law Review using a printing press complained about the use of the printing press and camera to invade the privacy of private citizens and the broad dissemination of that information by newspapers.

This paper brought the matter of technological tools used to invade privacy into a public forum. Subsequent court cases then attempted to use the theory that was advanced to gain relief for some people. The results were mixed and will be discussed later.

Twentieth Century

Without question, technology has shown the greatest growth in the twentieth century. A variety of electronic and photonic communications media have come into existence: the computer, networking and internetworking, medical devices, and a mania for documenting and saving information. At the end of the century, we certainly see the evolution from industrial based society to an information society. Similar to the early

³ This is discussed in chapter 2.

industrial period, technology exceeded the ability of policy makers to control and regulate.

Privacy is faced with a large number of assaults. Databases record details about individuals to the point that future generations may know more about the day to day life of ancestors from this time than of even the most famous person of any previous generation.

Data flows through wires and light pipes without encryption, laying bare an information stew that is rich in information about people, people that the information identifies with incredible precision. Despite our ability to cloak such information, most people are blissfully ignorant of the potential problems that a few seconds of this data could cause.

Amitai Etzioni, in his book ([12]), discusses a number of these problems. Additionally, David Brin ([6]) and Simson Garfinkel ([15]) note the problem and discuss it, each offering his own solution.

We know of the problems, but they are not resolved. For one thing most people are just coming to grips with the information age and its implications. As the industrial revolution had its high priests, engineers and mechanics, who understood the workings of the new marvels, so too the information age has its high priests who understand the technology and its ramifications. Beyond the priestly class there is some understanding, but it is incomplete and in many cases incorrect.

Historically there was a growth of technology to solve other problems with an eventual adaptation to new requirements. The adaptation was slow, a matter of decades, and subtle.

Let us look at a timeline and then consider how it impacts people⁴. (This timeline is not necessarily correct in the details, but the relative positions of the activities conform to information in this chapter. Their temporal placement is also approximate.)

Starting with the 1920's and 1930's, there were some cases that were making their way through the court system⁵. Articles had been written and now people were starting to try to apply the theories in a practical manner.

Initially, the technology that represented the greatest threat to privacy was the telephone. People assumed that their conversations were inviolate, assuming a private line⁶. Criminals engaged in bootlegging, (it was the time of national prohibition) and gambling were early adopters of this technology, much to their detriment. By placing the details of their activities on a phone wire, they opened themselves up to others who might want to listen. Government employees who were part of the technologically knowledgeable availed themselves of this information.

While the naïve mobster was responsible for the leak of information, the government agents who devised a way to bend the technology to their needs took

4 See figure 1 at end of chapter.

5 cf. Chapter 2 for the legal history of privacy in the United States.

6 When I was much younger, my parents had a telephone installed in our house, but the only service available was party-line service (which I do not believe even exists anymore). With this wonderful service, we could lift the receiver and listen to the neighbors conversations. Of course, when my mother found out about this activity I was treated to my first lecture on privacy. The gist of that lecture was that it was not a good thing to do and anyway the other party could hear the click and know that I had lifted the receiver and get me in trouble.

advantage of them. Legal theorists talk about the “reasonable expectation of privacy” ([37] pg. 93). The mobsters had the expectation and the government did not believe it existed. Ultimately the courts agreed with the government and then eventually changed course in the opposite direction.

The expectation of privacy that existed in the mobster's mind was reasonable given the naïveté of the time and the lack of experience with the technology, but once the ability to listen in was demonstrated, the reasonableness dissolved. In effect a reasonable expectation demands that there be some awareness of the medium and its security weaknesses. Business could have been transacted by more secure media, e.g. the mail, albeit without the efficiency that the telephone afforded them.

Let us move now to the 1940's, a time of war and the need for national defense. Great strides forward in technology were taking place with the invention of RADAR, nuclear weapons and energy, computers, cryptography and cryptanalysis, and espionage.

Someone who steals the military secrets of a country in time of war is a traitor, a criminal most heinous and loathsome for our side and a hero for the other. Also, during a time of war the populace feels a sense of urgency to win and is willing to forgo rights to achieve victory provided that the rights return later⁷.

Unfortunately, the government traded on the wartime feelings by creating the “cold war” and the feeling of imminent attack that it brought to continue the need for

⁷ Giving up the rights is easy; getting them back can be troublesome. But as long as there is a reasonable expectation that the rights will be restored at the end of the war, we will yield some. I cite as an example the rationing and blackouts that the civilian populace accepted. Normal activity was restored at the end of the war allowing people to buy without ration coupons and to be free from having to shutter or curtain their windows at night.

a greater ability to violate the rights of citizens. J. Edgar Hoover used the Federal Bureau of Investigation as a private blackmail agency to continue his power. Senator Joe McCarthy claimed to know of communists in government and used that to pry into the lives of anyone who was suspected of communist sympathy.

The 1940's and 1950's were a black time for privacy from the government. Many justifications for violations came forward. But at the end of the 1950's a small change happened that began the reversal of that trend. Dwight Eisenhower nominated the ex-governor of California to fill the position of Chief Justice of the Supreme Court. Earl Warren was considered a conservative but when he took the helm of the court he began a liberalizing era in the United States.

Under the Warren court Miranda warnings became required⁸, publicly supported counsel had to be provided for certain crimes and judicial intervention became a more regular occurrence. ([5] and [16])⁹

As the 1960's rolled along, civil rights for blacks and eventually the opposition to the war in Viet Nam heightened the awareness of individual rights and privacy. The culmination of the anti-war protest was probably the riots in Chicago during the 1968 Democratic convention. This represented the bifurcation of the anti-war movement into the violent, revolutionary fork and the civil disobedient, legal rights

8 These are the warnings to arrested suspects advising them that they have the right to counsel, the right not to incriminate themselves, and other rights.

9 Berger [5] has an good discussion of some of the negative ramifications of these policies. Also, Gunther [16] contains the actual cases, their chronological order, and a discussion.

oriented fork. Because there was no real support for the violent fork, it eventually died out.([4] and [8])¹⁰

The civil disobedient fork continued into the mainstream of American culture where its after effects can still be felt. To this day there are activists employing the same tactics to achieve their goals. Probably the most effective use of these tactics was in the environmental movement.

One of the tactics was the gathering of names and lists of names to contact for help or to send newsletters. These lists needed to be sorted in a variety of ways depending upon the need at hand and lists could be shared by one group to help another group.

The most effective way to manage large lists is to use a computer database. With the coming of the 1970's computers were becoming more common and less expensive.

Often the history of something in the technological age follows a pattern.¹¹ The innovation, let us call it the movement to wear only burlap (burlappers), starts with a small group. It organizes, promotes activities and attempts to get its members to keep thinking about the matter through newsletters and meetings and begins to become stronger. At some point some action gels the group, perhaps an attempt to raise the cost of burlap. This point is then seized upon to allow the group to grow. Prior to this point

10 Hannah Arendt's book [4] "On Revolution" is an excellent discussion of this. Also, cf. Karl VonClausewitz's opus [8] "On War" for further information on how to successfully wage a war and some interesting insight on how this war was not waged correctly.

11 This was one of the lessons that I learned in a course taught by the Management School faculty at Purdue. (Technology Strategy) Case studies of technological innovation has resulted in an abstract pattern that most technological breakthroughs follow.

the group must be prepared to seize the moment. Computer databases permit a group to avail itself of the opportunity efficiently.

As noted above the 1970's saw the introduction of inexpensive computers and more powerful software. This allowed creation of lists of names that could be handled quickly and put into an order that was required for any situation. Mass mailings could be targeted to the particular segment that was impacted, perhaps in our example above the rainforest lovers could have the burlappers list and create a mass mailing explaining the horrible ravaging of the rainforest by those who were selling upscale mahogany burlap clothes.

People accepted that those groups that they supported needed the information but the government was not to be trusted and therefore should be given as little information as possible.

Around the late 1960's time frame, credit cards started to appear. Credit lenders like to know the likelihood that the person they grant credit to will repay it in the future. With the impersonalized nature of society, our greater mobility and the widespread acceptance of credit, some standardized way of identifying a person and getting an impartial history became critical.

During the New Deal of the 1930's the social security system was created and with it came the social security number. This number is critical for its eventual use as a standardized identifier. By the 1970's, this number was needed for taxes and its use in identifying a person and associating it with a credit history created the infrastructure that was critical for the credit card companies.

Within the credit history repositories resides one of the main breaches in the protective wall of privacy. When someone gets a job, when someone borrows money, when someone gets a utility service to the apartment he rents or the house he bought, when someone has a financial event in his life, all this is recorded by one of the main repositories. They store it in their computer databases, indexed by each individual's social security number. And it is saved for seven years¹².

Computers and databases enabled this collection of data, data communications facilitates it. Presently, credit information can be obtained online in under a minute¹³. It can also be reported incorrectly in the same time. Correcting the information can take months, during which time a person's financial life is turmoil.¹⁴

Analogously, Simson Garfinkel ([15]) talks about medical information that is collected about all of us without any access for correction. Any information reported from this database is as fallible as the financial information, but it is now hidden from our review.¹⁵

12 I worked in the credit reporting industry for a few years and know this information from an insiders perspective as well as from the perspective of several writers including Amitai Etzioni, Solove and Rotenberg, Simson Garfinkel and others too numerous to mention.

13 I actually designed a system that was supposed to perform the task of getting a request, querying three credit reporting bureaus, merging the information and returning the results within 15 seconds. The first implementation actually took 30 seconds, but we knew it could go faster.

14 Again from experience. We had a tester on the project that had gotten a phone call from a customer whose credit file consisted of the customer's information mixed with our tester's information. It took about 3 months to get the problem corrected. In the case of one repository, it took 2 months to get them to recognize the problem.

15 This information can be devastating as in the case of my father. He had been running around in the yard when a physician for the life insurance company came to give him a physical. The doctor said there was a heart problem and the insurance was denied. This information got back to the MIB database and he was not able to get any insurance despite a cardiologists report that there was no problem based upon an ECG and not just stethoscopic examination. He was in his 50's at the time and just got a bypass in his 80's, his first cardiac problem.

As computers got much less expensive, they became more pervasive in our society. Now, anyone can gather information, make it available to the public, and not provide recourse to correct the information unless required by law.([35])¹⁶

Then in the 1990's, information exploded. Internet access changed from a geek toy to a mainstream technology primarily because of the World Wide Web. To cope with this proliferation of information, search engines came into being allowing more efficient searches of the data.

Personal information that someone does not wish to be known represents an invasion of privacy, but so does spreading information about someone that is not correct. Both of these modes of privacy invasion are facilitated by using the web. Carefully crafted web pages can appear reliable, will show up higher on the search engine results, and can promote a vindictive agenda against someone.¹⁷

Summary

I have demonstrated that the privacy of individuals in a society has gone from a peak when societies were primitive to a nadir in current times. I have also shown how technology has been an instrumental element in this reduction.

There are several reasons that we need to understand the history of privacy.

16 The Fair Credit Reporting Act of 1970 requires that a process be in place to correct disputed information and note the dispute on the report. Most other reporting databases do not have similar regulations to which they must conform.

17 Perhaps the most egregious example of this is the scam that was run against a computer hardware supplier. A press release was submitted to a news site that reported, falsely, the CEO was leaving the company. While done for financial gain, it is still a terrible lie about the CEO and an invasion of his privacy.

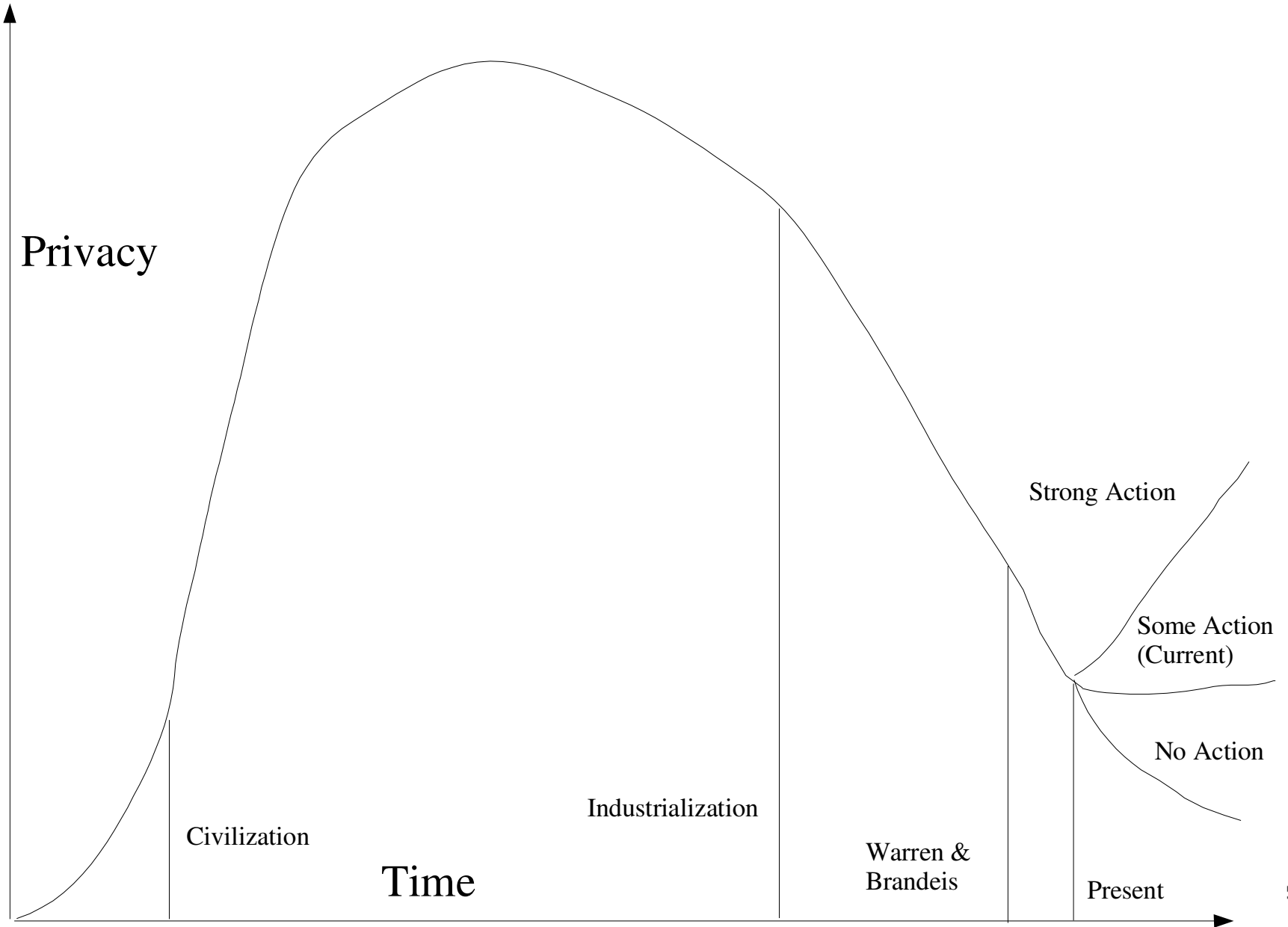
First, history shows us that privacy has existed since the beginning. Modern commentators complain about the intrusion and reduction of privacy, but it is important to show that it actually existed to show it being reduced. We also must understand the extent to which that reduction is taking place.

Secondly, historical accounts allow us to understand how the trend has occurred and what events have facilitated the trend. The old business adage is that someone cannot manage what cannot be measured. Similarly, someone cannot track and understand a trend unless he can put some measures to it, even inexact measures. What is crucial to understand here is the rate at which the trend has changed.

Lastly, there is a phenomenon that limits the ability of people to intuitively comprehend activities that occur too slowly. When something has occurred over the period of centuries, only reflective contemplation of the information will allow us to properly understand the activity. By recounting the history of privacy, even in a schematic form as I have done, there is now a basis for contemplation and analysis.

I continue from here with an analysis of the legal history and then present the results of my reflection on the history by creating a definition of privacy and finally present some recommendations for future action and direction.

Figure 1 – Timeline:
Based on Chapter 1



CHAPTER 2 – LEGAL HISTORICAL CONTEXT

We have considered the historical background leading up to the present. Part of the historical development has been legal development.

Legal reasoning has almost solely shaped the current structure of privacy in the United States. Numerous complaints, court cases, opinions, law journal articles and a few books on the subject have resulted. In this chapter, a historical perspective of the law as it pertains to privacy and particularly information privacy is presented. It is only a brief sketch and in no way do is it intended to be exhaustive: for that the books mentioned in the bibliography should be read.

While most people generally credit the Harvard Law Review article of Samuel Warren and Louis Brandeis ([37] pg. 29) as the starting point for an acknowledgment of the right of privacy, in actuality there had already been some history preceding this.

In England, there was a famous case in which a Member of Parliament, Wilkes, had written some critical and possibly seditious articles about the government. ([27] pg. 27) At some point, it became obnoxious enough for the government to act. His home, his offices and the homes of several colleagues were searched and a general warrant was issued for the arrest of the publisher, writer and distributor of the particularly offensive edition. Eventually, Wilkes was released because the government cannot arrest

a sitting Member of Parliament. The court also warned the government that the action of searching the private papers of an individual was not tolerable.

American Watershed

Samuel D. Warren, Jr. was a wealthy Bostonian whose parties were reported in the newspaper's society column. Mr. Warren, a wealthy businessman and attorney decided that the reporting was excessive, so he collaborated with a former schoolmate, Louis D. Brandeis¹⁸, to write and publish an article about privacy and the law. Published in 1890 in the Harvard Law Review, this article became the cornerstone of privacy law in the United States.

Building on Judge Cooley's "... right to be left alone ...", the expansion of the definition of property to include intangible possessions, and the U. S. Constitution's amendments' regulation of governmental invasion of privacy, this paper attempts to build a foundation for privacy from non-governmental entities. In conclusion they state:

"... The common law has always recognized a man's house as his castle, impregnable, often even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?" ([38] pg. 38)

18 Louis D. Brandeis was to later become a justice of the United States Supreme Court.

In effect this article argues that government is prohibited from invading the privacy of a home and life, and that restriction needs to be extended to private individuals. Furthermore, it is argued, this right must be enforceable in court the same as the right is enforceable against governmental intrusion.

From this well thought out article there proceeded several decades of inaction despite Brandeis's appointment to the Supreme Court bench.

Many theories have been proposed, but I think that there are two that are probably the most likely: a privacy suit requires the plaintiff seeking damages for the loss of privacy to bare more of her private world to the court, and ultimately the public as a whole, to prove the loss, and simply because a law review article proposes a new theory, it is not binding and might not even be acceptable to judges on the bench.

An excellent example of both these is the case of *Roberson v. Rochester Folding Box Co.* in which Ms. Roberson was required to testify about the shock and humiliation that she suffered when she learned about the use of her photo.¹⁹ In this case, the majority of the court specifically rejected the Warren-Brandeis theory of privacy on the grounds that it invited too many lawsuits and “... doing violence to settled principles of law by which the profession and the public have long been guided ...”([38] pg. 53)

Interpretivism is the inertial restraint on adoption of new laws by judiciary instead of legislature. It observes that Constitutional mandate that the legislative power reside in Congress²⁰, and that judicial power resides in the courts²¹. It further holds that

19 171 N.Y. 538, 64 N.E. 442 (1902). This case involved a woman whose photo was used to sell flour. The photo was used without either her permission or knowledge.

20 US Constitution Art. I sect. I

21 US Constitution Art III, sect. I

because the delineation is well marked there should be no circumstance in which one branch performs the duties of the other branch except where explicitly permitted²².

In this case, interpretivism carried the day and forced the legislature to do its job. *Pavesich v. New England Life Ins. Co.* ([38] pg. 55)²³ resulted in the right to privacy being upheld. Though this is a move in the direction of upholding Warren-Brandeis, it never directly referred to the article but based its action upon other reasoning.

There is a problem with using legal decisions as a basis of the proper definition of the right to privacy. Courts have a particular jurisdiction over which they have sway but the boundary is tightly defined and one inch outside that physical boundary puts a person into another jurisdiction with different rulings.

Eventually the rulings get reviewed by higher courts with larger boundaries but the same problem applies. If the Supreme Court reviews and rules on the matter, it now applies to the entire country. But the 'if' is a large question. There is nothing binding the court to review a case and even though it reviews the case it may defer in making a ruling and even if it rules, the ruling might be overturned by a later court hearing another case. A Supreme Court ruling is relatively definitive and binding.

Consider the wiretapping case of *Olmstead*. ([35] pg. 281)²⁴ This is an interesting case for a number of reasons: it was heard by the Supreme Court, Justice

22 The Senate sits as a judicial body to decide whether to convict a president pursuant to a bill of impeachment. This is explicitly permitted in Art. I, Sect. 3. Interestingly enough, when the President is being impeached, the Chief Justice of the Supreme Court presides, which is the only time that all three branches of government are forced to act together on the same piece of work: legislature on prosecution and jury, judiciary deciding procedure, and executive on defense.

23 122 Ga. 190, 50 S.E. 68 (1905). *Pavesich's* photo was used without either his knowledge or permission. (Similar to *Roberson*)

24 277 US 438 (1928) Brandeis's classic dissent in the privacy arena.

Brandeis was on the court, it involved a wiretap that invaded the privacy of the defendant, and the Brandeis opinion came down on the minority side. Government agents used technology to listen in to Olmstead's telephone conversations and then used the information to try Olmstead for criminal activities he was engaged in. No warrant was issued and the Supreme Court decided that none was needed.

Justice Brandeis wrote a great dissent, joined in part by Justice Oliver Wendell Holmes, but the law did not follow Brandeis until a decision 39 years later. ([38] pg. 87)²⁵

At that time the court reversed itself, too late for Olmstead and a fallow period for privacy.

As time progressed, understanding of the technologies involved in an invasion of privacy increased within the judiciary. (An old adage states that the wheels of justice grind exceedingly slowly but they grind exceedingly finely.) With this understanding comes the greater willingness to oversee the use of technology.

Justice Brandeis foreshadowed this change in his dissent when he said, "... Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." ([35] pg. 283-284)²⁶ Smith brings out that this quote echoes a Harvard Law Review article that Brandeis wrote. ([24] pg. 148) In that article Brandeis mentions

25 388 US 41 (1967) *Berger v. New York*

26 *Olmstead v. United States*, 277 US 438

the use of television which indicates that the justice kept abreast of the technological changes that were taking place²⁷.

It should be noted that the right of privacy was not being invented in this arena, but its enforcement against individuals was a new concept. There were laws against a governmental intrusion, despite what the *Olmstead* ruling seemed to indicate.

If *Olmstead* was bad law, there were reasoned grounds in support of it. Looking at Chief Justice Taft's decision, we see that the key for the majority was not the privacy, but rather the question concerning the seizure of property. Listening was not deemed a seizure because nothing was taken; the information was still conveyed without loss from one party to the other. "The language of the [fourth] amendment cannot be extended and expanded to include telephone wires ..." ([35] pg. 282) Nothing was seized, no search conducted. All that occurred was the overhearing of an electronically conveyed message.

Information and the way that government gathers it continued to evolve. Decisions eventually lead the way to an overturning of *Olmstead*.

In 1967, another case wound its way to the Supreme Court to try the theory that telephone conversations were not protected by the fourth amendment. ([38] pg. 87)²⁸. A New York law was overturned and information from wiretaps was now considered private.

27 The time was 1928 and television was very much in its infancy. To not only know about the technology but to also see how it could be used in violation of privacy required either a great grasp of the potential of the technology or a lucky happenstance that mentioning it would be deemed appropriate in future years. At this time Brandeis was 71 years old.

28 *Berger v. New York*, 388 US 41 (1967).

To this point we have examined a number of court cases that have defined and redefined the right of privacy in the face of technological intrusions. Along this path, two good and opposing articles appeared to add to the argument and a third article made an attempt to point the way to the future of privacy in relation to technology.

Dean William Prosser²⁹ starts with a synopsis of the Warren-Brandeis article and then proceeds to define four torts that have emerged from the case law to that point. ([38] pg. 58)

He notes that every state except four, at the time of his writing, had accepted the right of privacy and the states rejecting it had rejected it as being an act of interpretivism and therefore requiring legislative remediation. From this article came the definitions of invasion of privacy in the “Restatement (second) of Torts”. ([38] pg. 60-61)³⁰

Prosser drew a legal definition of invasion of privacy from the normative base of legal decisions that existed to that point. But it took Edward Bloustein³¹ to broaden the definition to include the protection of “personal liberty” and “human dignity.” ([38] pg. 60) Rather than echo the current thinking, he abstracted it to a new level.

Following from these articles, the Supreme Court decided *Griswold*³² and states; “... the right of privacy which presses for recognition here is a legitimate one.”

29 Dean of Boalt Hall Law School of the University of California, Berkley, writing in 1960.

30 Restatement (second) of Torts, Sections 652b, c, d, e.

31 President of Rutgers University.

32 *Griswold v. Connecticut*, 381 US 479 (1965). The case involves a dispute between the state and Planned Parenthood concerning the legality of disseminating birth control information that was then escalated to a Constitutional question about the right of privacy.

([38] pg. 61) A strong statement affirming what had only previously been hinted. This truly was the event that opened the gate.

Legislative Initiative

Not all law follows from the courts. The legislature is constituted to pass laws for the common good. Subsequent to this case some laws were forthcoming.

The Electronic Communications Privacy Act of 1986 (ECPA) ([35] pg. 324)³³ provides regulation of wiretapping and associated activities. A tap that captures the information as it is transmitted has the strongest requirements regarding warrants and judicial oversight while a pen register that merely captures the addressing information requires no warrant.

ECPA addresses the communication of information, but the information itself also must be regulated to prevent undesirable disclosures. While Titles I and II regulate all communications over a communications channel, (wire, radio, satellite or light), other legislation regulates certain information that would be damaging if it were released. HIPAA ([35] pg. 210)³⁴ of 1996 and FCRA ([35] pg. 519)³⁵ of 1970 are two

33 ECPA consists of three titles. Title I is codified as 18 USC §§2510-2522 and addresses communications as they travel over the wire, (it is also referred to as the “Wiretap Act”), Title II is codified as 18 USC §§2701-2711 and addresses the data of a communication as it is stored either at an endpoint or a waypoint, and Title III is codified as 18 USC §§3121-3127 and addresses “Pen Registers” and trace and trap devices, (the definitions here were modified by the US Patriot Act and broadened to not only include devices that capture a telephone number, but any addressing or routing information.)

34 Health Insurance Portability and Accountability Act of 1996 are reported as 45 CFR parts 160-164 and regulate, among other things, the release of medical information.

35 Fair Credit Reporting Act of 1970 codified as 15 USC §1681 regulates the disclosure of credit and related information.

such acts. Greater safeguards are instituted to protect medical information and financial information.

A great deal of effort has been expended over time to insure that the fourth amendment protections from an intrusive government will be properly observed and that transgressions will be dealt with in an appropriate manner. A person has some guarantees of privacy from the prying eye of an overzealous government agent.

Consider the case of Danny Kyllo. Danny was an aspiring farmer whose only cash crop was an illegal drug. Within the confines of his house he tended the plants with care.

Agent William Elliott of the Department of the Interior heard about the venture and went to Danny's house at night with a thermal sensing camera. After observing that part of Danny's house was warmer, consistent with the requirements of the plants he was growing, the agent was able to obtain a search warrant from a judge based upon this evidence.

A conviction ensued but Danny cried foul. How could an agent of the United States Government be allowed to view the house with such advanced tools, he asked the Supreme Court.

The Supreme Court agreed that this was an unfair thing that the government had done. "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."

([35] pg. 317)³⁶

36 533 US 27, *Kyllo v United States*, (2001).

By a 5 to 4 majority Danny's rights were held to have been violated, his privacy molested and the government's case, all based upon the initial observation, became tainted and thereby excluded. A 5 to 4 decision leaves a good deal of doubt because of the slim margin of victory.

Indeed, the minority in this case declared that “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. That is the principle implicated here.” ([35] pg. 320) In other words, there is a schism in the understanding of what privacy is vis-à-vis the fourth amendment guarantee.

Summary

I have traced some of the legal history of privacy in the United States. Through several laws and cases a concept of privacy has evolved. Because privacy is a recent concept, in the law, and not an explicit right, there is no guidance within the law except that which has evolved.

This evolutionary process is a long, slow process that tends to explore paths that lead away from the ultimate goal. It is a tactical approach that is not guided by a strategy. While this can yield a short-term value, often it gets bogged down by indecision.

Simultaneously, technology is proceeding forward with some strategic goals. In a race between the two, technology is the more likely winner in the short term with law surpassing eventually.

CHAPTER 3 – DEFINITION OF PRIVACY

We have surveyed the historical and legal perspective on privacy. Now we get to the heart of the matter: what is privacy?³⁷

In their seminal law review article, Warren and Brandeis define privacy as the “... right to be left alone.” ([38] pg. 29) Warren and Brandeis proposed their definition prompted by photography's ability to capture a face without the permission of a person. Even more invasive is the ability to capture a situation that might be compromising to one or more participants while invading the area of privacy that might be reasonably expected by them.

There are situations that give rise to a reasonable expectation of privacy. Married couples within their own bedroom certainly can expect protection from outside prying. What if they are not married? What about a rented room such as a hotel or motel room?³⁸

Defining privacy using examples falls short of a satisfactory method. Engaging in casuistry will leave an expanding number of cases that must be classified.

Attempts to draw a conclusion from the legal tradition also have their limitations. A variety of courts and judges coupled with case decisions lead us to nearly

37 I approach this task from the vantage of a white male living in the United States. What I say may not be the same for everyone and in fact probably is not. Hopefully, understanding the bias in which it is written will help the reader to understand the points I am making.

38 This is the approach that the Supreme Court took in the “Roe vs. Wade” decision. Enumeration of the various situations was neither exhaustive nor was it memorable. This case is well remembered but only for the abortion part of the decision, not for the privacy aspect. [16] pg. 236 410 US 113 (1973)

the same end. Appellate courts do provide some relief by giving us more generalized decisions based upon some philosophical analysis or guidance.

Courts are passive elements of society. They cannot go out to make new rules; they must wait for a concrete case to come before them. As such the case can either be a specific instance that is decided solely on its own merits, or they can be taken as an opportunity for a court to expound a broader theory that it feels will fit the case.

What have emerged from the legal system are Prosser's four torts, “without any attempt to exact definition ...” These are:

1. “Intrusion upon the plaintiff's seclusion of solitude, or into his private affairs
2. Public disclosure of embarrassing private facts about the plaintiff
3. Publicity which places the plaintiff in a false light in the public eye
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness “ ([38] pg. 59-60)³⁹

Though not a definition, these four categories do well in circumscribing the legal definition, but there are still holes in the legal fabric. There must be a guide for differentiating one case from another when the cases are on the edges of what has been decided. This is what Dean Prosser offered to the community.

Definition

Thinking of the variety of activities that have been cloaked in privacy, it can be appreciated that the subject is complex. There is an ultimate privacy that is inviolate and there is the bulk of privacy that can be violated. I define something as “naturally

³⁹ Dean William Prosser wrote these in his article “Privacy [a legal analysis]”. Dean Prosser, dean of the law school at University of California, Berkeley, is an acknowledged authority in the legal arena. This article summarizes legal cases in an attempt to find a common thread. Additionally, it should be noted that his summary of the events leading up to the Warren and Brandeis article is somewhat exaggerated.

private” when its existence can neither be discerned nor inferred except through unreasonably invasive measures.

Natural Privacy is a fairly narrow state. At this point I wish to introduce a new term: “personal secrecy.” Much of that which we call private information would be what should be called personal secrecy. Rather than understanding the “right of privacy” as being one of maintaining privacy against others, it becomes a right to maintain a shroud of secrecy around the personal facts and actions of our lives. In the terms above, natural privacy is the inviolate privacy and personal secrecy is the rest.

Natural privacy derives from the natural state of some things. Consider a thought. Someone cannot discern my thought by looking at me. Someone cannot infer the thought by observing me. Someone may discern changes in me that the thought has brought about and someone may infer some aspect of the thought from noticing how another changes in reaction to it, but the thought itself is not accurately understood from any external point.

A thought is naturally private because there is no way to discern it or infer it at this time. Once someone speaks the thought, that speech is personally secret and it becomes a matter of guarding its secrecy.

This is true privacy. But someday there may be a device that allows another person to read my thought without my knowledge. The device that reads thoughts without the knowledge or consent of another is not unreasonably invasive. It performs its work but never performs an act that intrudes upon the person, nor does it restrict movement or the other myriad rights that the person has. What has happened in this case is that the natural order of things has been altered and the natural privacy of thought is now not private but personally secret, although it is maximally secret. A person must now act to thwart the invasion of that thought rather than relying on nature to protect it.

It might be said that it restricts the right of personal secrecy, but does that right really exist, and where can we point and say “This is where the right of personal secrecy originates.” Consider Adam from the first chapter. Alone, with no other person

to invade any aspect of life, even the face of Adam was safe from a misappropriation by a camera wielding paparazzi. There was no personal secrecy because there was no other person to be secret from. Until Eve was created, even the most obvious attribute of Adam was secret.

The right of personal secrecy is a creation of society. Without a society we have nobody to keep out of our secret matters.

The right of personal secrecy is not a natural right. Is it truly a social right? Is it an ethical right weighed against society's desire or need to know?

Indeed, a utilitarian might argue that if society shows a sufficient need to know the secret details of something, that need outweighs the 'right' to personal secrecy. The Constitution of the United States specifies plainly that, "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 ..."

{U.S. Constitution, Amendment IV) A strong statement that we have rights to personal secrecy, but society can have countervailing rights to invade. Further, it states: "No person ... shall be compelled in any criminal case to be a witness against himself ..."

(U.S. Constitution, Amendment V) Again, this is a strong statement that supports Dean Prosser's first two torts. We see that there is a legal right.

Social contract theory states that from some elemental state of man, e.g. the state of nature, groups coalesced around a central focus to form a society by entering into a contractual agreement with each other. This contract states the rights acceded by society and by the individuals. Because a right to personal secrecy depends upon a society to exist, this would properly be a matter for the social contract.

Historically, Americans have been considered an inquisitive people. We ask a lot of questions about nearly any subject. But, when told to "butt out" we generally stop at least the line of questioning.

Officially, we ask a lot of questions but when the Fifth Amendment is invoked the line of questions, while often still asked, may go unanswered without consequence.

That is the American contract. Other countries have different interpretations or clauses in their contracts. I do not understand them as well so let us continue on with the American contract.

We have a curiosity, but understand that there are limits to what people will answer and what questions most of us will ask. This has probably changed with time. With the increase of urbanization we feel a greater need to have space away from society and we respect that need in others.

But what of those who do not subscribe to the contractarian theory, is there still a “right to personal secrecy” in their theories?

Hebrew-Christian theology has a strong tradition of personal secrecy between men. Jewish law prohibits building a house so that it easily overlooks another person's private space. Christianity has the sanctity of the confessional. Both accept the personal secrecy of a conversation between a person and a religious advisor, and for solitary, meditative communications with the deity.

Utilitarian values, the greatest good for the greatest number, also have some recognition for personal secrecy. Unless intrusion on the private matters of an individual would serve the greater good, such as society's need weighed against a person's desire, the utilitarian would still weigh in on the side of personal secrecy.

Given this acceptance of personal secrecy as a right and the deep desire for most people at different times to seek solitude, its existence cannot be denied. Counter to this right is the decay of the right as evidenced by the current state of affairs. It now becomes a problem to reconcile.

We still have privacy. It is the most intimate information that we control. But, once we express it in some manner it becomes an issue of secrecy.

For example, if someone thinks of an apple as a delicious, edible piece of an apple tree, that is private. If that person now writes that thought down on a piece of paper with a pencil, the thought has been expressed and now stands revealed waiting for someone to read it. This is personal secrecy. Now, if that person burns the paper, they have made it harder to read and then if they stir the ashes they have made it improbable that others can read it, but not impossible. It is still a secrecy issue, but steps have been taken to insure the secrecy of it, but it has not been made private again.

Only a mind-reading machine would take thoughts out of the realm of private and put it into personal secrecy. To thwart the machine a person might need to wear an aluminum hat, but there might be an improvement that renders that ineffective.

Is the introduction of personal secrecy as a concept distinct from natural privacy really necessary or is it really only natural privacy in a less strict form? I do not believe that this is a real issue; rather I think that the term is required to divorce ourselves from the commonly used term privacy. Everybody knows what privacy is, but almost no one can define it. By making privacy a strictly defined term and then surrounding it with the less strict term “personal secrecy” we are freer to discuss the concept without the baggage that the term privacy brings with it.

Figure 2 shows a schematic of how I envision “privacy”. At the center is the most absolute form of privacy. It is never expressed nor has it ever entered a realm of lesser privacy. It is small and pure and called natural privacy. Next come the three rings of personal secrecy. Varying degrees of expression or release to the public have taken place and now the only restraint to further proliferation is the reluctance to bring the matter to the public by all those who have access to the secret either through explicit or implicit consent. Finally, the entire white area depicts the public arena in which the information has been made available to the public at large. While this expresses the idea in a schematic form, secrecy is actually a continuum proceeding from natural privacy to common public knowledge. Any single piece of information that enters the secrecy realms can progress to the common public knowledge realm. But it can also lodge at a

more secret realm and even revert to a more secret realm over time. It can even cross the border to natural privacy again once all trace of it and the people who knew it is gone.

Consider some thought that pops into my head. It starts to circulate within my brain. I may stare into space or smile, but the thought is not revealed to anyone. This is absolutely private. No one can share it without either my active effort to make it available or a very good mind reading machine⁴⁰.

This thought works its way around in my brain and I decide it is a good thought that ought to be let out for the world to know. At first the expression might consist of my relating bits of it to others for their comments. Eventually, I might write it down.

Let us suppose that it is the idea for the next great work of literature. Writing it becomes the first expression that undergoes revision, communication and eventually production and mass dispersal. At various stages of the life of the thought and its sequelae it was either naturally private or had some level secrecy attached to it. It could always go from more secret to less secret.

Secrecy requires an investment of energy to ensure its protection. If left to its own a secret might spread unless the original possessor puts up barriers. Even with the barriers the spread might happen with a single breach of trust.

What we have is a picture of privacy that moves along a continuum from private to secret to public. Maintaining the privacy of anything requires energy and effort. Therefore, there is a presumed tendency for private information to become public that only an active counter-effort can thwart or at least slow.

40 Indeed, after writing this I stumbled across an article that indicates that NASA has brought the entire matter of mind reading closer to realization. The NASA system allows scientists there to interpret the nerve impulses sent to the vocal cords as words. This is a form of mind reading because it is able to interpret the sub-vocalized words and words spoken 'under your breath' and make them private. Now, this is not what is traditionally understood to be mind reading, but many people use these processes to reason ideas and the ability to read nerve impulses is a step in the ultimate direction. cf. www.betterhumans.com/News/news.aspx?articleID=2004-03-19-3

DNA and our genetic code are in a state of flux. Natural privacy used to inhere in our genes. In the past, nobody understood the code or even how to evaluate the raw material. Now we can match minute evidence to a suspect through comparison of DNA. We literally shed DNA by dropping hair, discarding partially eaten food, and through a wide variety of bodily functions. That which used to be naturally private is quickly becoming personally secret through the advent of technological techniques. From this example we can see how natural privacy can slowly become an object of personal secrecy through the application of technology.

Privacy and Technology

Technology can be used to degrade or enhance privacy. It seems to me, though, that as technology advances, our natural privacy and personal secrecy erodes further because society is less concerned with personal secrecy than with gathering information.

Printing initiated an explosion of ideas while creating an appetite for information that seems to grow with each generation. Following the press were inventions such as the telegraph, the telephone, radio, television and the internet. Each technology granted freer exchange of information while enabling penetration of more of the secrecy we had.

Mail is an exception. Mail was originally available to be read by unintended recipients⁴¹. Eventually, legislation was created to ensure that only the intended recipient would be the one to read it, except in certain circumstances. Because of this legislation, our society has come to treat mail as private communication and an extension of our own personal secrecy. If someone's mail were opened, it would not be surprising that he or she would be incensed.

⁴¹ Both Rosen [27] and Smith [34] cite the example of colonial America. In the example cited, letters were brought from Europe by sea captains and left in public houses for the recipient. Meanwhile, anyone who walked in could read the unsealed mail, [27] page 70 for example.

Mail is an example of recapturing personal secrecy once control of it has been lost. Legislation and a two hundred year history of acceptance have created this condition.

As we noted in the chapter on legal aspects of privacy, the Fourth Amendment restricts governmental invasion of privacy while remaining silent on non-governmental invasion. As a technology gets older, it becomes more disseminated, allowing more people to use it for either right or wrong.

Ethical considerations of Privacy

What is right in terms of privacy and personal secrecy? Who sets the limits and why?

Consider a person's body. Many people consider that revealing the nakedness of the body to others should only be done in the seclusion of a private area. Others still think that displaying it to others is acceptable provided that there is some acceptance by the other party. Still others feel that public displays of their bodies are acceptable at any time to anyone. And yet others feel that even in the seclusion of a private area there should be some modesty and the lights should be off if anyone else is in the room.

We have a wide range of views. Even the range that is considered normal is fairly broad. The law acknowledges that in a secluded area most displays are acceptable and that even when the level of seclusion is not very good, as long as all parties are accepting the display, there is not a problem. This really only becomes a problem when the display extends to parties that are not willing to accept the display or to certain protected segments of the population, e.g. children.

A normative approach would only yield a general rule with many exceptions and cases that would need to be reviewed by an outside party on the basis of conditions existing at the time. Furthermore, the norms are in an almost continuous fluctuation

causing the edges to blur even further. Some hard and fast rules would need to be applied that would permit variations and yet be clear enough to guide most participants.

What is needed is an overarching privacy rule. Because the information about ones self is really an issue of secrecy instead of some overarching privacy, it becomes incumbent on the individual to set the limits. Society might help by creating some defaults for some sorts of information, but the general rule would need to accommodate the variety of choices that an individual might make. First I am going to look at some aspects of privacy and then draw a conclusion.

Expressive Privacy

In general a person who does not attempt to limit discussion of some aspect of his life is by default permitting it, within social norms, to be spread without controls. ([9] pg. 76-77 and [31] pg. 354) Social norms would limit certain areas of information but as these change the restrictions on the information would change. A practical example of this might be the homosexual status of Oscar Wilde. While it was scandalous at the time and Oscar did not wish it to spread, it would not be important in modern times. Therefore, if Oscar had told his hypothetical friend Joe that he was homosexual, Joe would have had normative pressure to not reveal this during Oscar's time, but if Oscar had lived in the year 2000 and told this to Joe, Joe could have repeated this provided Oscar had not told him to keep the secret.

Now this argument about the norms ignores the need for the state to know some things that social norms would restrict. Indeed there is a need for the government to be able to inquire about certain things that are within the current need to regulate.

Criminals like to keep the details of their crimes secret, but the state has a definite reason to regulate this activity for the safety of its citizens. Social norms prohibit deviant behavior and generally the law requires people with knowledge about these activities to step forward with the information. In this case the needs of the society outweigh the desire of the individual for secrecy.

Another case that is raised concerns the need to protect that which I have classified as true privacy. Efforts are underway to compromise this area of privacy by creating technology that will permit reading of thoughts, indirectly at first but with some greater penetration until the innermost vault of thought can be breached.

Law would need to protect this area if that is deemed desirable. I would hold this would even transcend the social norms.

Thoughts, those deep, unvoiced, unexpressed musings must have a sanctity that transcends even the society's need to protect its citizens. Who among us has not had a thought that we would not wish to express. I think a classical example of this might occur when a beautiful woman passes by a man walking with his wife. That vision of socially unacceptable activity that flashes through the man's mind is primarily irrepressible. He would probably not reveal it to his wife. She probably can guess but the ramifications of this information leaking could destroy the marriage. The thought really is not important. Action or inaction on this thought is really the important thing.

Controlling our impulses, which surely do occur, is really the defining aspect of what we are. The persona that we allow to be revealed is the definition of us. We control what thoughts we act on and how we act on them.

Further, to different people we reveal different personas. To a wife we might confide that while we thought that woman was beautiful, there is no question that we prefer our marriage. To a male colleague we might comment on the attributes of the woman but leave our wife out of it. To a female colleague we might say nothing. To different people we present different revelations. It is the same person expressing some aspect of the innermost thought to another with some of the information censored to preserve our secrecy.

We might even say nothing. This is certainly a valid option that would be the most preserving of our secrecy. If a technology existed that would capture this information despite our desire to limit it what would be the effect?

A person might feel as if there were no refuge to retreat into. No space in which they could pause, gather their thoughts and recuperate. There would be a sense of paranoia that grew in them to the point that they would try censoring their thoughts before they occurred. But of course they would want to censor that, and so on ad infinitum. It surely would be something that might start a descent into insanity.

We all need some space, some private sanctuary that we can use to retreat from society for a while. We all have thoughts that we are ashamed of and that we repress, personas that we project, and skeletons in our mental closets.

Accessibility privacy

Similar to our need for a mental place of privacy, there are times that we need a physical place also. When we want some intimate time with a significant other⁴² we naturally desire to exclude society. What I do with my wife, presuming it is within the law, really is a matter for the two of us.⁴³ I do not wish to have anyone knowledgeable of any aspect of this including the fact that I was secluded with my wife.⁴⁴

What is being expressed here is accessibility privacy: the ability to access a person either physically or virtually through some means. This is the form of privacy that is violated when a policeman breaks down a door or a telemarketer calls at dinner time.

With my definition of privacy as personal secrecy, accessibility privacy maintains its status. The ability to access a particular person is dependent upon the level of secrecy that the person wishes to retain. Deciding whether any particular person will have access depends upon a number of criteria such as time of day, who the person is, what the person wants, what is being intruded upon, etc. Obviously, this is not a simple decision. The person doing the accessing, let us call him Simon, needs to weigh the need to contact the other person, let us call him Rupert, against the possibility that Rupert

42 I do not mean to exclude insignificant others with whom someone might wish to be secluded. I am committed to a monogamous marital relation with my wife and speak from that point of view. I acknowledge that other relationships exist and that they desire seclusion, but I do not feel qualified to speak to that as an example, but I do feel that this treatment of privacy would be inclusive of them.

43 This is a point to which feminists address their criticisms of privacy. In their view the woman is generally made to be submissive to the husband and therefore not a full party to the decisions. I will address this later.

44 There are differing levels of secrecy that people invoke with this activity. I tend to a high level of secrecy, but on the other end there are people who bring cameras in to record the events and eventually broadcast on the web. There are also people at varying levels in between and probably some well beyond these extremes.

wishes to not be contacted. Simon must make the initial assessment, and if the decision is to contact Rupert he then refines the decision based upon the greeting that he receives.

Similarly to the above scenario, a policeman would need to decide if the need to access Rupert is sufficient to pass the test of law. Let us take the case where Rupert is to be arrested. The policeman must decide how many policemen to engage, whether there will be violence, will evidence be destroyed if he does not act quickly, etc. It is also a complex matrix complicated even more by the realization that a mistake on his part could result in serious consequences.

By asserting a right to be unmolested, Rupert is making clear the infringement on his right to accessibility privacy. Simon can only be guided by social norms, any knowledge he has of Rupert, and reference to his personal bias in such a case.

Would Simon calling Rupert represent a violation of Rupert's right to privacy if Rupert did not want to be disturbed? Only if Simon persisted past the point where it was clear that Rupert did not want to be bothered would privacy be violated. This is basically an opt-out model of privacy. Rupert must tolerate a reasonable intrusion if he has not explicitly said 'no' to it.⁴⁵ Once the intrusion starts, Rupert must be able to say 'no' at that point and terminate the access. This is what trespass laws do, this is what harassment laws do, and it is reasonable within our society to do so.

⁴⁵ By saying 'no' I do not mean that literally. Turning on an answering machine to intercept all phone calls, hanging a 'do not disturb' sign on the door, any action that signifies to others that access is unwanted should say 'no' to the other party.

Informational Privacy

This last category defines privacy based upon tracking of a person's actions. When someone goes to the doctor and then the pharmacy, it can be inferred that someone is sick and the doctor either prescribed or recommended some cure. Is it any business on mine to know this? If I am a health insurance provider and have to pay the bills, yes. If I am a nosy neighbor who happened to notice activity this day, no, but there is nothing someone can do to stop me. If I am a stalker prying into someone's life with the intent to find something about them that I can use to their detriment, no, and someone might be able to do something if they know.

In these days of computerized activity, this form of privacy invasion is easy. Using a credit card leaves a trail of information that might be useful. The sheer bulk of data that only a few decades ago would have been enough to ensure some privacy is handled with ease by computers.

We are living in the nascent information age. Records and minutia about our lives flow through the communications networks like water to be saved up in a reservoir, to be tapped when needed. I have some reservations about that but the greater problem is with who does the tapping.

Commercial enterprises need this information to compete efficiently in the modern marketplace. ([7]) Balancing the needs of the business against the right of the individual to personal secrecy is the crux of the problem.

Simon goes to a grocery store. By giving them some personal information he will get a discount. The store assures Simon that they will only use his information to improve their service to him and to provide offers to him that is targeted to his lifestyle. The store then offers to a chicken company Simon's name because he buys a lot of chicken and the chicken company wants to try a new product in Simon's area.

The store will claim that it is making a valuable offer available to Simon and only giving out the minimal information to the chicken company. Simon may not want this sort of activity. Perhaps he hates being a marketing guinea pig and would have told the store this had they asked. Simon's ability to restrict information about himself is not properly being addressed.

Information as property

There are some who claim that the information about an individual is property to be handled as any other property. I do not support this. Personally secret information is not a piece of property; rather it is an attribute that can be controlled with time and space limitations.

Business takes the information we generate, secret or not, and transforms it into tangible property. It owns, sells, rents, transfers and even accounts for this information as any other asset. They have invested work into the gathering, storage, preservation and validation of the information and deserve to derive benefit from it.

On the other hand, a person has invested his entire life, up to that point, in creating the information that represents him. He therefore feels the right to control this information should rest with him. It is not a property that can be bought and sold as if it were a piece of land. It cannot be transferred to another.⁴⁶

Another consideration is the fact that it is copyable with no diminution of the original. A person has lived the event that created the piece of information and the world might have known about it had it cared. Some piece of the world did care and that is why it is recorded.

There is a concept in some legal arenas that is called Habeas Data. ([11] pg. 132)⁴⁷ Other countries have incorporated this concept into their statutes or Constitution to allow an individual to access, correct, dispute, or demand deletion of incorrect data. It extends not only to data about the complaining individual, but can be available to others with legitimate concerns about the data. What this principle acknowledges is that data gathered may be inaccurate, it may be transcribed inaccurately, or it may be inappropriate for the purpose it was collected. It also admits that the information may be harmful.

These laws permit the individual to oversee the data that a company is using and compare it with the reality. It distinguishes between the data and the embodiment of the data by permitting the two to be compared and reconciled.

⁴⁶ Actually, it can but not legally. This is the crime of identity theft.

⁴⁷ EPIC [11] pg. 132 discusses this concept as it is brought out from the Argentine Constitution, article 43. Also, cf. footnote 537, *ibid*.

Feminist Aspects

In a chapter devoted to the subject, DeCew ([9] ch. 5)⁴⁸ discusses the feminist problem with privacy. Essentially the problem is that women, being often the less powerful side of a relationship, can be repressed in the name of privacy or personal secrecy.

Secrecy, it is argued, often is used to suppress information about repression or physical harm that can befall women. The same argument can be made about any individual or group involved with another group or individual where the power is shared unequally. A government can use secrecy to suppress information that would be useful to demonstrate abuses against citizens.

In truth, this is not a secrecy issue. It becomes an issue of unequal power and the need to open the processes. If a woman in a relationship or an individual involved with the government is being abused, there needs to be some form of sunshine that can be poured in. Secrecy is only a shield. If not secrecy then a lack of information by stonewalling would be used to replace it or even elimination of the questioner. In a final state, the individual or the woman would be made to “disappear.”

Therefore, I would argue, secrecy wielded as a tool by those who would repress represents a weak shield that could be penetrated. With proper safeguards and oversight it should be penetrated by those who need to protect the weak. I feel that it

⁴⁸ Also the Rössler book and article. [27] pg. 52 I approach this part of the topic with a purely theoretical point of view.

shows us that there are needs to penetrate the veil of secrecy and that there needs to be those empowered to do so.

There is also an interesting side point to explore in my theory of personal secrecy; the secrecy surrounding the intimate relations within the confine of one's own bedroom is actually an issue of consensual secrecy. The level of secrecy of this situation is the least level of secrecy of the parties involved. In this situation an unequal balance of power could skew the level of privacy. A strong partner with an inclination to hide more than the other partner would like can exert influence. This is part of the basis of the feminist objection.

Typically the male has held the role of the strong partner in the relation, either through social norms or some other force. Therefore, it is argued the woman lacks the ability to enjoy having control. I do not disagree with this; in fact I believe it to be so for most of the world.

This does not contradict what I hold about secrecy, rather it points to another societal problem. Personal secrecy exists as a balance of the person's desire to limit disclosure while society retains some level of desire to reveal the secret or at least to penetrate to the point that some element of society is aware of what the secret is about.

A problem exists in the societal definition of this balance not inherently in the secrecy. Policies to correct this balance are a subset of the level of governmental intervention that we desire in our lives as a whole, the societal secrecy. A remaining element is the need for societal balance to mitigate the uneven power.

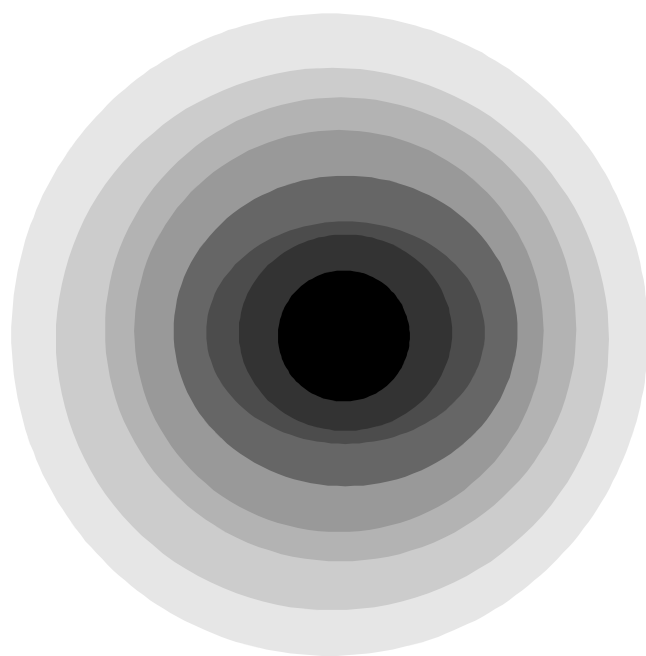
Alternatively, those empowered to penetrate the veil need to do so only when necessary. This is the essential balance that laws such as the Fourth Amendment are attempting to strike. What is needed is some way to encourage and empower the weaker party to report abuses that exceed the societal level of tolerance.

Summary

I have proposed that privacy, natural privacy, is actually that which cannot be discerned or inferred from the outside. All else is personal secrecy in which people have differing levels that they wish to apply to various aspects of their life. In keeping with this concept I have explored several of the traditional arenas of privacy and demonstrated how my definition is still consistent with normative understandings of “privacy.”

I therefore claim that my definition is an acceptable definition and therefore can be useful. Where I differ from the norm is in the emphasis I place on the individual's ability to regulate the information about himself/herself. I am claiming a relativistic secrecy.

I also recognize the need of business and government to possess and use this information. There is a need to strike a balance. I talk about some ways I feel are best to strike this balance in chapter 5.



Legend:





-  White – public
-  Light Gray – moderate secret
-  Dark Gray – most secret
-  Black – private

Figure 2 – The Spectrum of Privacy

CHAPTER 4 – GLOBAL ISSUES

Prior to this point, all the discussion has been directed to the United States. Europe, Asia and even South America have also been undergoing a revolution in the way privacy relates to technology. I discuss some of the issues in these areas of the world and relate my definition of privacy and personal secrecy to these parts of the world. ([11])⁴⁹

A problem with trying to develop a global view of any matter is the parochial perspective within which we have viewed the world. I am a native of the United States. Please bear this in mind as you read my attempt to explain the complexities of privacy in a global context.

Europe

Of all parts of the world, this part is probably closest to the United States in many respects. Privacy is a great concern here and some important actions have been taken to preserve it. In many respects, Europe is ahead of the United States in this area of policy.

⁴⁹ Primary research for this chapter came from the Electronic Privacy Information Center's book "Privacy and Human Rights" [11]

Politically, Europe is a hodge-podge. There are monarchies and democratic republics. Most countries enjoy a single dominant culture that has been in place for centuries. Additionally, there is the European Union that generates policies and laws that the member states may or may not adopt.

Given the tension amongst the various states and between the states and the union, one wonders that anything gets done. But, indeed it does get done.

Privacy and especially the privacy of individually identifiable data is the subject of European Union legislation that has been adopted by a large number of member states. Protection of the individual seems to be important in Europe. And with the increasing number of states joining the union, this concern will be growing.

How do the policies of the European Union compare with the definition I have created? In Europe, the private information that I call personal secrecy is really not as personal. Businesses that trade in personal information must protect the data. Rather than protect and preserve the individuals' personal preferences, it is treated in aggregate and specification of the proper, and improper, handling of the data is given by law.

While a legal specification of what may be done makes it easier for a business to conform to the regulations, it does not take into account the different attitudes that people take regarding their personal information.

Australia

Australia is a unique part of the world. While it is geographically close to Asia, politically and jurisprudentially it is closer to the United Kingdom. Common law in Australia follows English common law and the government is a parliamentary government that is modeled on the English Parliament.

In terms of privacy, Australia has struggled with privacy on its own. The tort of invasion of privacy has only recently been acknowledged by the high court there and several statutes have been enacted to protect privacy, both on the federal and state levels.

Australia passed the Privacy Amendment of 2000 ([11] pg. 140) which put in place some privacy principles. Several of the proposals that I make in the next chapter have been put in place, and this law puts emphasis on the commercial entities to police and enforce their policies themselves. In fact, a company can apply to the government for substitution of an alternative set of privacy principles to replace the proposed principles from the government.

This law also allows the resolution of problems by a private, industry-appointed ombudsman with a right to appeal to a government commissioner. One of the most fascinating ideas, and one I am not sure is truly workable, is stated in principle 8;

“Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organization.” ([11] pg. 141)

Basically this grants the ability to opt-out at the time of the transaction.

In general, Australia operates at a level of privacy closer to the United States than to Europe. This could cause problems for transfer of privacy information to and from Europe.

Asia

Asia is such a huge conglomeration of diverse cultures and politics that to lump it all into a single category is to do it a great disservice. I will therefore break it down into a few of the more important areas, although I do not mean to slight those areas I have left out. For selection I have attempted to take two extremes and middle.

People's Republic of China

As the world's largest country, by population, and the leading Communist country, and one of the most rapidly emerging economies, this country needs to be understood. It is a country in turmoil. Old style Maoist Communism is changing to a new style that incorporates if not embraces capitalistic economy.

Constitutionally, privacy and the rights of the citizens of the PRC are protected. In fact the rule of law has frequently been subordinated to the rule of those in power. Given the Stalinist influence that has directed this country for the past several decades, an intrusion on the rights of people is understandable. With the recent

acquisition of Hong Kong, the influence of jurisprudential guidance has begun to assert itself. Despite this, abuses of privacy remain.

My scheme would be acceptable to this government and in fact might be more easily implemented here. With the strength of the central government, a bureaucracy to retain and administer personal secrecy could be implemented and businesses forced to adhere. It would also be a problem as the information itself with the policy tags would be available for use or misuse by the central government in the name of auditing and the registry might be made compulsory as an alternative way to label dissidents, i.e. those who wish to remain private would be more suspect.

Japan

Japan is one of the primary economic powers in the world today. ([11] pg. 317) With few natural resources, a small land area and a small number of people, it is in the position of significant influence in all economic matters.

Generally, the Japanese have respected privacy and are signatories to several international conventions on the matter. Recently, however, there have been attempts to acquire information that would have previously been protected, with the concomitant outcry of public opinion. For example, license plates will be issued that contain smart chips that contain driver and vehicle information. ([11] pg. 324) Coupled with the existing video surveillance system this would allow police to locate a particular vehicle and then observe it.

Private companies have been coming under regulation of both governmental and private origin. JIPDEC, Japan Information Processing Development Center, has been authorized to license and rate companies that handle personal information with the ability to post ratings and even remove a license from non-compliant firms. ([11] pg. 320) Within this scheme a personal secrecy proposal as I have created would be able to fit and run very nicely.

Republic of the Philippines

The Philippines is a country that was a territory of the United States, so it would be expected that a great deal of the legal and political situation here would mirror that of the United States. ([11] pg. 392) In fact the systems are very similar.

The Philippines seems to take privacy very seriously, having passed several laws to protect the personal information of citizens, especially those citizens who are victims of crimes. As a result of the ILOVEYOU virus that was created and launched by a hacker in the Philippines, the right to secure electronic information has been recognized and codified, with penalties for violations.

South America

As with any of the other continents I am reviewing here, there are a variety of countries, each with their own rules and regulations about privacy. I take three countries and discuss some of the protections afforded privacy.

Argentine Republic

Argentina protects the privacy of its citizens jealously. ([11] pg. 132) Not only are there protections on the data, but the Constitution provides for a habeas data, i.e. the ability to request, review and correct data that is held by anybody, governmental or private. The correction can even be the ability to have the data made confidential, effectively deleting it.

They do well in the area of protecting the privacy of their citizens. The European Union has certified Argentina as being compliant with their data protection requirements. Furthermore, legislation and court decisions have tended to broaden the protections that Argentine citizens enjoy. There are problems, but it seems that there is a high regard for personal secrecy here.

Federative Republic of Brazil

Brazil has strong protections for the privacy of the individual, much like Argentina. ([11] pg. 167) There is a Habeas Data law and restrictions on wiretapping.

Again, the question of how well the theory is realized comes to the fore. In this case, illegal wiretapping has toppled several politicians, which I take as evidence of strong realization in practice of the Constitutional and legislative theory.

United Mexican States

Mexico, a neighbor of the United States, has Constitutional protections for privacy. ([11] pg. 359) There are also laws restricting interception of mail, wiretapping, and other forms of surveillance. This said, the security police have been monitoring their own citizens for years and have expended a great deal of effort against political opponents to the heretofore ruling PRI party. With a new president from the opposition party, there is a vow to change.

Meanwhile, the border with the United States has been the cause of some privacy invasions that need to be discussed. The United States, in an effort to curb illegal immigrants from Mexico, has increased surveillance on the border and has gotten Mexico involved in this activity. Mexico now performs “security sweeps” ([11] pg. 361) of homes near the border with the US.

It is unclear what the Mexican position on privacy really is, one view looks as if it is in favor of strong privacy and then they act to violate that privacy. I think that a greater adherence to their own Constitutional and legal requirements would be more conducive to an implementation of privacy and personal secrecy as I have outlined.

Perhaps the real problem here is the big stick of economic power wielded by the United States, although this is an area fraught with pitfalls. The United States is trying to protect itself from illegal immigrants who can be terrorists, drug dealers, or migrant workers. Does this justify the actions it takes and that it compels Mexico to

take? I think there might be alternatives that are less invasive and I suspect that technology might help here. Mexico is economically dependent to some extent on the United States and practically would find it hard to resist.

Africa

As with Asia, Africa is a diverse group of countries with different cultures, histories and political features. Technologically it is less well developed than other areas of the world. I was not able to obtain information about most of the African states therefore I will report on the Republic of South Africa with the caveat that this is not truly representative of the majority of African states.

South Africa was a colony of the United Kingdom. ([11] pg. 449) In a bizarre twist, when freed from colonial rule the minority was left to rule with a repressive rule that subjugated the majority to second class status. Subsequently, this rule of Apartheid was overturned with the rise of Nelson Mandela.

Possibly a legacy of this turmoil is a heightened state of awareness of privacy and the need to protect it. Not only does the Constitution safeguard privacy but it mandates that the individual to whom the data refers shall have access to the information whether in public or private hands. Nothing in the scheme they employ would be contradictory to my definition.

Summary

Most of the countries I have detailed here have a strong basis for privacy and personal secrecy. While this is a good sign, there are a number of areas where the theoretical protections do not translate into actual practice.

While the consciousness about privacy is high, there are forces at work to reduce its realization. Illegal activity and concerns for the preservation of the state or power of the ruling individuals can cause lapses or outright breaches of the law. Without some form of oversight and other safeguarding there can be abuses.

Habeas Data laws are one of the more popular devices that seem to provide the requisite oversight. While the United States has the Freedom of Information Act for review of governmental data, it is much weaker than Habeas Data. In the private sector there is little real substitute in the United States.

Many people see the European Union's Data Protection Directives as a touchstone for privacy and personal secrecy. It is not without problems. Globally there are different environments, cultures and objectives that need to be met. While the EU is culturally diverse, there is a degree of homogeneity when compared to the world.

CHAPTER 5 – POLICY PROPOSAL

Having gotten a definition of privacy and personal secrecy, we now proceed to developing a set of policies to help implement it. First the stakeholders are identified and then the requirements for each are asserted. Because some elements require a prerequisite, the information about policies is presented in a chronological order.

Stakeholders

A stakeholder is someone or some group that has an interest in the subject matter. Stakeholders may be directly involved or may only have some support or even a tangential role. As an example, in the case of regulating motorcycle riders and motorcycles, the rider is directly involved and would suffer greatly from a defect in design that did not allow the motorcycle to be ridden safely. Other drivers want the rider regulated to force him to be aware of the rules of the road so that minimal confusion will occur when the motorcycle is ridden in public. The state has an interest because they own the roads and are responsible for dealing with the after effects of an accident. Insurance companies must pay for the consequences of bad riding or the inability of other vehicles to see or operate safely around the motorcycle. Finally, companies that

manufacture the motorcycle are concerned that the regulations be reasonable, economically achievable and in general reduce the liability of the company for the product.

It might be noticed that there are stakeholders left out of the above. Not only is this correct, but it is almost inevitable. Those directly affected by the regulations are more easily identified than those with indirect connection, and even the directly affected ones are hard to list completely. Therefore, I will attempt to identify stakeholders in the privacy arena and do so with the acknowledgment that there are probably more that I have missed. What I think is the most critical effort in this is not identifying all stakeholders, but rather covering all the possible ramifications of the proposed policies. This too, I attempt knowing that it is at best an imperfect listing.

The first group of stakeholders is individuals. Even though that covers everybody in the world, I am referring to individuals in their capacity as unattached to any other group.

Government is the second stakeholder. Some legislation, some support in the courts and finally some enforcement might need to come from government. Therefore a big question that needs to be answered is how much impact this will have on all levels of government from a cost perspective.

Commercial enterprises represent that third stakeholder. Some companies use personal data as their product, others merely use it as an element of their overall business strategy. In any case the costs and potential impacts on the business need to be weighed.

End-users of information are also impacted. Companies that require personal information on demand to perform some analysis for the final product will need to understand and comply with privacy regulations and norms. This is a cost issue but might also mandate a radical alteration in the way they conduct business. Such a major impact might weigh heavily against one proposed solution and heavily in favor of another.

Law enforcement, considered separately from the government, might be impacted. In some aspects, rapid access to information might be hampered and this should be avoided. In other aspects, they enforce the new regulations and would now need funding, tools, procedures, guidelines and limits.

The last group that is involved with this is the criminal element. Identity thieves, credit information thieves and others who steal personal information need to be hampered in their pursuits by any regulation. Additional penalties or criminal charges would be a secondary benefit that is also worth consideration.

Model

Personal information is not a piece of property, it is something that defines us but does not create us. As such we cannot own the rights to it but we do own the right to say what is done with it. We can desire to spread it to the world or we can desire to keep it a tightly guarded secret. Further, we can tell someone else what we want done with it and consider it a breach of trust if something outside our wishes is done. I think

that we should also have a right to recover from someone who profits from this breach of trust.

Anytime we provide information about ourselves to others there is a notice about privacy and the intended use of the information. This is good but needs to go further. The acceptable use can be unilaterally changed. I therefore am proposing that any personal information be tagged with some additional block of information that identifies the origin, date, and other information. What this does is then provide an ability to trace the origin of data, limit its dissemination and permit the individual to hold accountable those who would defame him or usurp his ability to control the spread of information.

Costs would need to be borne by the companies that hold that information as part of the cost of instantiating personal information into a tangible form. Given the rapid increases in memory and disk available coupled with the reduced cost of storage, the cost of this proposal would actually be minimal. Some fee could be charged to release all the information and tags to an individual, making sure that the request was not a frivolous one, but motivated for some purpose. Further, a purpose might be required to be stated and perhaps would need to conform to a code permitted by law⁵⁰.

Further, transferring data from one source to another would require passing all applicable tags, logging the request by the sender and decrementing forwarding counts, if specified, to note that the information had been passed to someone else.

⁵⁰ This is similar to the permissible codes that the FCRA, as amended, required to get a copy of another's credit report.

Fundamentally, I am seeing a mandate that all information that is instantiated for some purpose, would need to be traceable through its entire life and this information, if mishandled, would subject all persons doing the mishandling to civil and possibly criminal penalties.

Now there is a problem of international data. Let us say a company has some data and wants to send it to another company but does not want to comply with the regulations. What would prevent them from sending the data to some company in a foreign country that does not conform to this scheme and then having that company send the data to the other company with some fake tags that note the data as coming from overseas without tags? We could make it a crime. The problem would be how to prevent a violation.

I think there would need to be several approaches to this problem. First, an international treaty would need to be created that made a common law for all signatories, similar to the Berne Convention for copyrights. Second, all data about citizens from a signatory country would need to have original tags showing origin data before it could be accepted by a company in a signatory country. Third, any company in a signatory country would need to make the off-shore transfer with all appropriate tags and, possibly, to make a notification to some appropriate authority notifying them of the transfer and retaining a list of names included in the transfer. While this is not an exhaustive list of the regulations for foreign transfers, it should be enough to start.

Government

A good set of governmental policies should be minimal, simple enough to express the goal of the policy and no more intrusive than is necessary. We need a set of regulations that will promote privacy while not impacting commerce or individuals with a cumbersome level of red-tape. I propose three alternatives and then express my preference after some analysis.

Proposal 1 involves a greater degree of governmental involvement but guarantees a higher level of protection and punishment. In this proposal, all businesses involved with processing or handling of personally identifiable information would need to register with the government, conform to a set of regulations, provide documentation of audits performed to assure conformance and could be decertified or have a license revoked for some level of abuse⁵¹.

An advantage of proposal 1 is the ability to detect and punish violators swiftly. Only eligible companies could have the data, although there would need to be some exception for organizations that did not use the data for a commercial purpose. These companies would be audited regularly by external auditors and at most one audit period would pass before the abuse would be reported.

51 By abuse I mean non-conformance with regulations in a repeated manner with no effort to rectify the situation. This could be one single large instance or several instances over a period of time. Obviously there would need to be some administrative court system in place to decide when the limit was reached. Alternatively, there could be a privacy ombudsman's office that would take initial action with review and ascent by the administrative court.

Proposal 2 requires that data be tagged with origin, maximal number of trading partners who could possess it, lifetime, and other restrictions. When data was gathered a unique identifier would be created and embedded in the tag as well as being given to the individual. Any use of this information would need to provide the identifier(s) to indicate the source original source.

In this scheme the data would be traceable to the original source and all the tag information. If some part of it was not being properly used, the individual could recover damages from all parties concerned either through a small claim or a privacy ombudsman's office⁵². Audits would be needed although a business would need to make sure the data it possessed conformed to regulations and tag information, so the audit would only need to verify that all data had tags and that the cleaning process proceeded regularly. Additionally, it would need to be a crime to possess data without a valid tag attached.

Proposal 3 would eliminate the ability to trade personally identifiable information except in some restricted manner, similar to credit bureau information today. A business would need a legal reason to request the data, logs of the transaction would need to be retained and problems that were reported would be investigated and dealt with in a civil or criminal manner. This differs from proposal in that it eliminates the individual's data from being propagated once a business acquires it. A company could

⁵² This ombudsman could be a separate bureau or part of an existing group. I would imagine the FTC on the national level and state attorney generals and district attorneys on a lower level.

get permission to act as a bureau and then sell the information, but the regulatory burden would be severe enough to make that undertaking only profitable to a larger firm.

This proposal restricts the number of companies that can sell data, and data could only be bought from a bureau or a bureau could buy from other sources. Essentially, the bureaus would be closely watched and they would make the market for this information.

In this case regulation would be minimal for most companies, but heavy for a few. Fewer regulators would be required and their efforts would be turned toward the market making data bureaus. Any other unauthorized use would be traceable and could be dealt with quickly.

Proposal 3 mirrors the existing marketplace. Instead of only credit data, all personally identifiable data is the commodity. But unfortunately, credit bureaus have had a number of problems, regulation has not been as strong as needed and there are several exceptions in the law to allow the selling of data without coming under the regulation of the Fair Credit Reporting Act, the main law regulating credit bureaus.

Proposal 1 imposes a potentially large burden on the government and one starts to wonder how well such a program would be administered given that fact that it would be larger than the credit report market. More companies would be dealing in data and certainly the large number of smaller companies would eventually yield to a few large and powerful data aggregators. This brings us around to the situation of the credit bureaus and the regulatory powers.

Proposal 2 would seem to be a decentralized mess with a plethora of regulators. False claims would possibly abound⁵³ and companies would face a potentially expensive and time-consuming process.

Despite the probable problems with proposal two, I would favor it. Even though the petty thieves would try to use the process to rob companies, there would be some way to address the problem. This having been said, there will eventually be large companies that specialize in the processing of individual data. These companies would need tighter regulation and for them I would see some activity such as in proposal number three. I would still require the tagging and traceability.

Traceability is critical to understand where data comes from, where errors creep into it, and to accommodate the desire for secrecy from the individual. No other proposal given here would permit the individual controls that people desire.

Individuals

An individual could do a lot or a little in this scheme. The fundamental concept that is being protected is personal secrecy, the ability of an individual to specify the use or non-use of individually identifiable data. If an individual wants to share the data with everyone who asks, so be it. If there is a desire to hide the data, fine. It is up to the individual to express these desires and it is up to the handlers of this data to either

53 They always do when there is money at stake.

respect these requests or face the possible fines or strict regulation that would result from a massive public outcry.

It also becomes incumbent on the individual to express his or her policy. Absent such an expression, some set of defaults would be provided, and this would probably be part of the agreement, written in impossible to read fine print.

Let us consider an example of how an individual would express some limit. Smith walks into a grocery store and is asked to apply for a special card. This card will provide a rollback of the outrageous price hike that was just instituted in exchange for some information about the person and his buying habits. Simply swipe the card every time someone shops and he receive a discount.

At this point Smith says, "Fine, but I do not want anyone else to see the information, the store is not to sell or trade it, and it is only good for one (1) year." There would need to be a form to specify this and this data would then go into a tag associated with the data. Smith gets a tag identifier that he can keep in his records. Every time he gets junk mail from someone that bought the information from the store, the tag number would be on the label and Smith could go to the store and collect the appropriate fine. If they did not pay, he could sue, ignore it, or revoke the rights to that data meaning that his card would be deactivated at some point and they would need to erase the data or update the tag to note this fact. Then, after a reasonable time, if Smith gets another piece of mail with the tag, the fine would now be higher and the remedies would be stiffer.

But if Smith did not specify his limitations, the store defaults would apply. Only if the store violated its own policy would Smith be allowed to recover for the damage.

Company Responsibility

Companies would need to monitor their data more carefully. Selling data that did not have the correct permissions would result in a potential liability. Further companies would be required to periodically audit themselves and annually an external audit would be performed to validate the internal audits. The CEO would need to sign a statement that the audits are done and that the company is in substantial compliance with applicable regulations⁵⁴ concerning the proper handling of this data.

Complaints would need to be filed by the company and the individual with some agency. At year end these would be audited and some federal organization could match the company submitted complaints with individual submitted complaints. Again there should be some agreement, perhaps at most 5% of individual complaints can be missing from the company and 50% of the complaints that the company files could have no match with individual complaints⁵⁵ before a regulatory investigation started.

54 Basically a Sarbanes-Oxley act for individually identifiable information. (In Sarbanes-Oxley the CEO is required to sign a statement that says he believes the financial data to be correct.) This is done to force the CEO to lead the company on the ethical path, as prescribed in law.

55 Why the great mismatch? It is more likely that an individual would file a complaint and then not submit the paperwork to the government than the other way around. There is no disincentive to the individual but a great disincentive for the company.

Cost-Benefit Analysis

Any scheme that can be devised incurs costs to provide the benefit desired. A perfect solution would incur no costs to generate enough benefit to cover the needs and desires. Because this is not a perfect world, we are required to settle most times.

Cost-benefit analysis is used to identify the costs and resultant benefits. Typically, this is expressed as a ratio of cost to benefit, with a lower ratio representing a better return on investment.

Let us assume that there are 1,000 businesses involved in handling the data of 1,000,000 individuals. To rule over this there is the equivalent of two full time government employees⁵⁶. Assume that the cost of maintaining data is \$0.01 per week per business per 1,000 names. This results in \$10.00 per week for 1,000,000 names.

If the tag increases costs by 20%⁵⁷, then we see an additional cost of \$2.00 per week or \$104.00 per year. But the benefit to the business is a negative benefit. It costs money to maintain the additional information with no gain for the business. The only gain comes if we consider the potential additional cost for any scheme that is alternative to it. Increased regulatory costs could be high as would the cost of buying

56 I use the abbreviation FTE for full time equivalent. One FTE can be several employees each contributing time to a project with an aggregate value equal to the effort of a single full-time employee. Needless to say, this presumes some average employee.

57 Would this be a reasonable number? It assumes that the data storage overhead is 10% and allocates the additional 10% to overhead for activities such as audit, management and increased maintenance. It is possibly low, but gives a number for analysis.

from a repository even though the repository would probably spend money buying data from the business.

For the individual the cost is minimal. There is a little extra time to express personal secrecy limitations, some time to even consider what limits they want and the cost of checking for unlawful use of the data. There would also be the cost of pursuing a claim which would initially be borne by the individual alone. To put a number to this cost, let us assume that the extra time comes to \$10.00 per year. The benefit would be greater protection of the data for an individual. This is difficult to quantify. A single episode of identity theft could cost tens of thousands of dollars, but the chance of an identity theft for any one person is low, let us assume 0.1%. So, arbitrarily set the cost to \$10,000. By making data attributable and companies liable, there would be more concern for the privacy of information, and the law would make fines for revealing information reducing the chance of identity theft. Let us guess that this theft now is reduced by 80%, making the probability now 0.02%. \$10,000 times the probability 0.02% to get an average benefit of \$2.00. The ratio is 5 for this case.

Proposal 1 would reduce the probability possibly by 90% and proposal 3 might reduce it to 95%. This would make proposal 3 the winner.

But for the companies the cost of proposal 1 would be higher and it would skyrocket for proposal 3. Let us assume the costs for 1 is 50% making the total cost \$15.00 per week or \$206.00 per year. Proposal 3 would probably double or treble the costs because of artificial market restrictions.

Let us further assume that the cost borne by the individual is the same for proposals 1 and 3. It would be much less than proposal 2 because there would be less requirements. So, let us put this number at \$1.00 per year.

The final group in this is the government. Assuming a cost of \$100,000 per year per FTE, proposal 2 would require 2 FTE's for a cost of \$200,000. Proposal 1 would impose more regulation and so the number of FTE's might increase to 10. Proposal 3, with its stronger control on this market might only require 5 FTE's.

Now we start combining numbers to get a societal cost benefit ratio.

Consider this table.

Table 1 Incremental Costs

<i>Entity</i>	<i>Proposal 1</i>	<i>Proposal 2</i>	<i>Proposal 3</i>
Business	\$206.00	\$104.00	\$412.00
Individuals	\$1.00	\$10.00	\$1.00
Government	\$1,000,000.00	\$200,000.00	\$400,000.00
Total	\$1,000,207.00	\$200,114.00	\$400,413.00

The total incremental cost for the three proposals is presented.

The benefits for each proposal are basically the same. We would all gain additional privacy. This means that the cost benefit analysis becomes a simple cost comparison. Because proposal 2 has the lowest costs associated with it, this would be the preferred method.

Summary

I have advocated an approach that leans toward the libertarian in its “hands off” approach. Personally, I believe this approach to be most workable. I have also demonstrated that there is some rational thought about why this is the best result.

Reflectively, if we take privacy to actually be personal secrecy, a desire to enforce our desires for secrecy on others, then we have another basis for this style of policy. A centrally governed agency regulating the secrecy of millions of individuals will tend to promulgate and enforce a set of rules that conform to the majority norms while trying to accommodate the variations. As the variations grow in magnitude, the ability to enforce that right becomes less. There is also pressure from the agency to not be as vigorous in the enforcement because of budgetary constraints. Eventually a homogenous right of personal secrecy begins to take hold as the rule.

My proposal removes this tendency but at the risk of having a weaker enforcement. Unless rights are asserted, they dissipate. Demanding individuals to assert rights in what is often considered to be a minor area is to almost assure that most claims are never asserted, an unfortunate result but one that is consistent with the concept of personal secrecy. If the individual will not pursue the secrecy right that is claimed then how sincerely is the right claimed?

BIBLIOGRAPHY

BIBLIOGRAPHY

Books

- 1) Alderman, Ellen and Kennedy, Caroline, 1995, 1997, *The Right to Privacy*, New York, Vintage Books
- 2) Amar, Akhil Reed, 1998, *The Bill of Rights*, New Haven, Yale University Press
- 3) Arendt, Hannah, 1958, *The Human Condition*, Chicago, University of Chicago Press
- 4) Arendt, Hannah, 1963, 1965, *On Revolution*, New York, The Viking Press
- 5) Berger, Raoul, 1977, *Government by Judiciary: The Transformation of the Fourteenth Amendment*, Cambridge, Harvard University Press
- 6) Brin, David, 1998, *The Transparent Society*, Reading, Perseus Books
- 7) Cate, Fred H., 1997, *Privacy in the Information Age*, Washington, Brookings Institution Press
- 8) Clausewitz, Carl Von, 1976, *On War*, New York, Everyman's Library
- 9) DeCew, Judith Wagner, 1997, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca, Cornell University Press
- 10) Denning, Peter J., 1990, *Computers Under Attack: Intruders, Worms, and Viruses*, 1990, ACM Press
- 11) EPIC, 2003, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments*, Washington, Electronic Privacy Information Center

- 12) Etzioni, Amitai, 1999, *The Limits of Privacy*, New York, Basic Books
- 13) Freedman, David H., Mann, Charles C., 1997, *At Large: The Strange Case of the World's Biggest Internet Invasion*, New York, Touchstone
- 14) Firestone, Charles M., Schement, Jorge Reina, 1995, *Toward an Information Bill of Rights & Responsibilities*, Washington, The Aspen Institute
- 15) Garfinkel, Simson, 2000, 2001, *Database Nation: The Death of Privacy in the 21st Century*, Sebastopol, O'Reilly
- 16) Gunther, Gerald, 1976, *Cases and Materials on Individual Rights in Constitutional Law*, Mineola, The Foundation Press, Inc.
- 17) Hamilton, Alexander, Jay, John, Madison, James, 2000, *The Federalist*, New York, The Modern Library
- 18) Huberman, Bernardo A., Adar, Eytan, Fine, Leslie R., *Privacy and Deviance*, Palo Alto, HP Labs
- 19) Ketcham, Ralph, 1986, *The Anti-Federalist Papers and the Constitutional Convention Debates*, New York, Mentor
- 20) Lessig, Lawrence, 1999, *Code and Other Laws of Cyberspace*, New York, Basic Books
- 21) Levi, Edward H., 1949, *An Introduction to Legal Reasoning*, Chicago, University of Chicago Press
- 22) Levy, Steven, 2001, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*, New York, Penguin Books

- 23) Mill, John Stuart, 1961, *Essential Works of John Stuart Mill*, New York, Bantam Books
- 24) Mitnick, Kevin D., Simon, William L., 2002, *The Art of Deception*, Indianapolis, Wiley Publishing
- 25) Orwell, George, 1949, 1977, 1984, New York, Signet Classic
- 26) Plishkin, Zelig, 19xx, *Guard Your Tongue*, New York, Aish HaTorah Publishers
- 27) Rosen, Jeffrey, 2000, *The Unwanted Gaze: The Destruction of Privacy in America*, New York, Random House
- 28) Rössler, Beate, 2004, *Privacies: Philosophical Evaluations*, Stanford, Stanford University Press
- 29) Rotenberg, Marc, 2003, *The Privacy Law Sourcebook 2003: United States Law, International Law, and Recent Developments*, Washington, Electronic Privacy Information Center
- 30) Schneier, Bruce, 2000, *Secrets & Lies: Digital Security in a Networked World*, New York, John Wiley & Sons, Inc.
- 31) Schoeman, Ferdinand David, 1984, *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, Cambridge University Press
- 32) Schoeman, Ferdinand David, 1992, *Privacy and Social Freedom*, Cambridge, Cambridge University Press
- 33) Shute, Stephen, Hurley, Susan, 1993, *On Human rights: The Oxford Amnesty Lectures 1993*, New York, Basic Books

- 34) Smith, Robert Ellis, 2000, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Providence, Privacy Journal
- 35) Solove, Daniel J., Rotenberg, Marc, 2003, *Information Privacy Law*, New York, Aspen Publishers
- 36) Thoreau, Henry David, 1962, *Walden and Other Writings*, New York, Bantam Books
- 37) DeTocqueville, Alexis, 1945, 1972, *Democracy in America*, New York, Everyman's Library
- 38) Turkington, Richard C., Allen, Anita L., 1999, *Privacy Law: Cases and Materials*, St. Paul, West Group

Recommended Web Sites

- 1) www.epic.org – Electronic Privacy Information Center
- 2) www.comsumer.gov – US Federal Trade Commission – responsible for some privacy regulations
- 3) www.usdoj.gov – US Department of Justice
- 4) www.privacyinternational.org – an international privacy organization that cooperated in the book [11] above.
- 5) www.privacyrights.org
- 6) www.privacy.org
- 7) www.identitytheft.org – excellent site concerned with identity theft, a crime against privacy