11-30-2007

Privacy in Database Designs: A Role Based Approach

Gary A. Poe
University of South Florida

Privacy in Database Designs: A Role Based Approach

by

Gary A. Poe

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Information Systems/Decision Sciences
College of Business
University of South Florida

Co-Major Professor: Rosann Collins, PhD.
Co-Major Professor: Donald Berndt, PhD.
Ellis Blanton, PhD.
Stanley Birkin, PhD.

Date of Approval:
November 30, 2007

Keywords: Privacy, Security, Taxonomy, Access Control Systems, Philosophy, Law, RBAC, Role Based Access Control

Table of Contents

List of Tables

List of Figures

Privacy in Database Designs: A Role Based Approach

Gary A. Poe

ABSTRACT

Privacy concerns have always been present in every society. The introduction of information technology information has enabled a reduction in the cost of gathering information, management of that information and the permitted that same information to become increasingly portable. Coupled with these reductions of cost has been an increase in the demand for information as well as the concern that privacy expectations be respected and enforced through security systems that safeguard access to private-type data. Security systems enforce privacy expectations. Unfortunately there is no consensus on a definition of privacy making the specification of security often over broad and resulting in the loss of critical functionality in the systems produced. This research expands the understanding of privacy by proposing a replicable type-based taxonomy of privacy that is grounded in philosophy and law. This type-based system is applied to a Role Based Access Control System to specify and control access to data in a in a hospital setting as a proof of concept.

Chapter 1: Introduction

1.0 Introduction

Every firm, profit and nonprofit, has always required information. Today one problem faced by organizations is how to obtain, manage and use information that is nominated as private information.

With private information the firm faces the following questions every day: What makes an item of information private information? How must they safeguard their customers' and employees' sensitive data? While companies recognize that information privacy is a vital management issue for today's organizations, how do we manage privacy? Do our systems meet current privacy expectations? The privacy environment in which firms must operate is dynamic and constantly evolving. When does the firm correctly anticipate changes in privacy standards and avoid being managed by the environment? How do we evaluate proposed decisions and actions to ensure that they are privacy compliant? While acknowledging that privacy consists of a complex web of political, social, and legal issues which impact the firm daily – what is the character of this environment and how can a better understanding of this environment be achieved? Firms recognize that protection of privacy could create a competitive advantage for the firm – how can we create a sustainable competitive advantage with a privacy strategy? How do we design and implement such a strategy?

In addition to these questions, the tools and design techniques used to manage private information as well as the mechanism of designing privacy into these tools are in their infancy. Privacy concerns are addressed haphazardly and in non systematic ways

(Kayworth et al, 2005) usually at the later stages of system design by placing control mechanisms over a pre-designed data model. Privacy is often designed on a case by case, instance by instance basis using bottom up development and no top down methods to manage the direction of the project. A better tool or design methodology would assist the firm to manage its environment but how do we improve existing tools or create new tools that design privacy into organizational structures and systems?

It has been observed that a societal adoption of a significant technological advancement can affect social values (Inglehard, 1977). Technological development in management information systems and the reduction of costs realized through their use in the areas of communication, procurement of information, processing and storage have enabled greater efficiency and effectiveness in business and fueled their adoption and use.

This adoption of information technology has produced a change in values. In general, people have become angry and frustrated because societal norms and laws have been ill equipped to deal with the changes (Spencer, 2002 and Zweig 2002)). Part of this conflict has produced an increased effort in the enforcement of existing privacy laws but has also resulted in the proliferation of new laws protecting privacy. Because a business operates in a sea of law and societal norms, this makes it difficult and at times impossible to manage the enterprise. As a result, increasingly costs are expanding to provide privacy protections for data as a response to these changes. Decisions are increasingly more difficult to make as often privacy considerations have become part of the decision even though what is or is not private is often not clear. Finally, businesses are increasingly

recognizing that privacy protections are a cost of doing business both from the standpoint of being a good moral citizen as well as from the viewpoint that the failure to do so will result in high social and monetary cost to the enterprise.

This effect on values is demonstrated as concerns about privacy have increased despite the fact that government has made efforts to protect privacy and business have undertaken efforts to manage privacy. Polls conducted by Louis Harris and Associates show increasingly individuals hold a concern that their private lives are being exposed. In 1978, 64 percent interviewed in the Harris Poll expressed concern about their privacy being violated. In 1995, over 80 percent interviewed expressed that same concern (Harris Equifax, 1993). The growing concern stems from the increased use of interconnected media used in business and personal activities (Federal Register, 2000). In 2005 this concern was not abated. Nationally, 67 percent were concerned over privacy of their medical records, 52 percent fear medical insurance information would be used to limit their opportunities, only 30 percent were willing to share health information with health professions not directly involved with their case and only 27 percent were willing to share health records with drug companies (Forester Research, 2005). That interconnected media is embodied in a variety of information technologies.

In the remaining of this chapter I will provide background on the concept of privacy to illustrate the problem privacy faces in an environment of rapid technological change and show the development of the concept of privacy in light of technological changes in Information Systems. Following that I will point out that defining what is privacy has proven very difficult, demonstrating there is no precise definition of privacy

and point out some of the reasons for why there is no agreed upon definition. Next I will outline the privacy research in Information Systems pointing out that research in the field of privacy is of vital importance but such research is in its infancy. Anticipated contributions of this work will follow, after which I will present how I will conduct the study.

1.1 Technology Change and Privacy: Three Examples

Following are three examples of how information technologies have created changes that impact privacy.

- The first example shows that adopted technological change has increased technical capabilities that have permitted invasions into places traditionally thought as private areas. These invasions have forced a reconsideration of the question of what is privacy – that is what places are private, what type of information is protected as private and under what circumstance is information protected as private. For each iteration of technical change, the scope of protection of privacy has been modified to accommodate technological change and preserve traditional notions of privacy.
- The second example shows that the adoption of technological change is often made without any consideration or the foresight of how those increased capabilities enabled by technological change impact upon traditionally held values, norms and laws that were defined when technological capabilities were not as refined. Technological change has enabled an expanded use of certain types of information due to the increased ability to control and compile information.

Because of the previous inability to control or compile this information, this information was deemed to be private-even if it was in the public domain or in the possession of an entity but no formal law or norm prohibited its use. To preserve the status quo and while harnessing new technological capabilities, new restrictions in the form of norms, guidelines and statutes have been placed on the compilation and subsequent use of information to ensure privacy - many of which have been found to be inadequate. Questions exist how do we create effective guidelines and restrictions that ensure values and norms but are flexible enough to permit technological change?

- In the third example, technology changes affecting information use causes corresponding effects upon society, particularly the roles and relationships created by society to protect and ensure privacy. The third example demonstrates that unless change is managed, technological change creates change in those roles and relationships. Certain roles and relationships in society require privacy protection to function optimally. Institutions that encompass these roles and relationships have evolved rules of behavior that protected this information. The adoption of information technology change and the hunger for the information have disabled the effectiveness of these institutional rules- thwarting both the ability of the institution and the individual to control sensitive information. As a response, information providers have adopted counter measures. These counter measures have included the withholding of information, the delay of disseminating

information and the providing of inaccurate information all of which have harmed the effectiveness of the institutions serving the information providers.

1.1.1 Example One: The Telephone

- This example shows that adopted technological change has permitted invasions into places traditionally thought as private areas- under the control of the individual. Each such invasion has forced a reconsideration of the definition of privacy - that is what places, what information and under what circumstance is information protected as private. Upon each iteration of technical change, protection of privacy has been modified sometimes to accommodate technological change, to preserve traditional notions of privacy with restrictions placed upon technology use to preserve the control of the individual.

The invention of the telephone and its adoption by society occurred in 1876. The telephone's advance as an information technology was immediately grasped and incorporated into its every day operations. In 1877, construction of the first regular telephone line from Boston to Somerville, MA, was completed. By the end of 1880, there were 47,900 telephones in the United States. Service between Boston and Providence had been established by 1881. Service between New York and Chicago was initiated in 1892, while service between New York and Boston started in 1894. Transcontinental service by overhead wire was not inaugurated until 1915. Most consumers of phone service were commercial enterprise. Home use lagged largely due to availability and cost but in the 1920's the presence of the phone in the home was more common.

In 1928, government agents seized a telephone conversation of a known bootlegger through the placement of a wiretap on the phone line. The wire tap, enabled police to listen to conversations taking place on the telephone. In his prosecution, the bootlegger sought to have the conversations of this activity excluded from evidence on the ground his right to privacy was violated by the action of placing a wiretap on his phone line and listening to his telephone conversation.

The Supreme Court of the United States upheld his conviction using traditional notions of privacy of the time. Traditional notions of privacy protected places from being intruded upon and as such required a physical trespass into the home of the person to occur. Because the wiretap was made outside the home there was no physical trespass. In this case the “seizure” of the conversation took place outside the individual’s home there was no privacy violation. A second protection of privacy was that persons were protected from unlawful seizures of tangible items such as personal papers and effects. What was seized here was not tangible - what was seized was his conversation - an intangible item not entitled to protection.

Justice Brandeis advocated a broad interpretation of the Fourth Amendment privacy protections to insure that the government refrained from intruding into the privacy of the individual. In his dissent in the Olmstead v. United States, Justice Brandeis stated (Olmstead v. United States, 1928):

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions

> and their sensations. They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

What Brandeis was in effect saying is we must recognize the potential for this new technology and reconcile the changes this technology brings with our value of privacy that a person has the right to be left alone. Brandeis' position in the Olmstead dissent was a minority opinion at the time. This opinion gradually gained momentum over time. In 1965, in the case Griswold v. Connecticut (381 U.S. 479, 1965) opinion, Justice William O. Douglas citing Brandeis found a penumbral right to privacy emanating from the Constitution and its First, Fourth and Fifth Amendments. Later in 1967, in United States v. Katz, the 1928 decision of Olmstead v. United States (389 U.S. 347) was overturned when the judges adopted Brandeis' minority opinion as the decision of the Katz court. The Court in Katz recognized that regardless of technological change, people have a right to privacy even if technology exposes them to some degree.

1.1.2 Example Two: The Computer and Database

- The second example shows that the adoption of technological change is often made without the foresight of how those increased capabilities enabled by technological change impact upon traditionally held values, norms and laws. Technological change has enabled an expanded use of certain types of information due to the increased ability to control and compile information. Because of the previous inability to control or compile information, information

> was deemed to be private-even if it was in the public domain or in the possession of an entity as far as the rule of law applied even though no formal law or norm prohibited its use. While new restrictions in the form of norms, guidelines and statutes have been placed on the compilation and subsequent use of information to ensure privacy many of these laws have been found to be inadequate. Questions exist how do we create effective guidelines and restrictions that ensure values and norms but are also flexible enough to permit technological change?

The Katz opinion occurred at the time people was developing a new awareness that a portion of their private life was subject to being exposed to others. This awareness surfaced in the early 1960's when the advent of computer technology that made it feasible to aggregate and process data in ways never before imagined. Research on the creation and use of computerized databases, which had begun in the 1950's fueled concerns over "Big Brother" collecting information on citizens and invading and controlling their lives. This reached a fever point in the mid 1960's when stories emerged of the federal government constructing super computers and operating them on the individual information of its citizens. A realization was made by the general public that the Federal Government, in its course of doing business had many unconnected data stores on individual people. Should these islands of information be merged, various details of a person's life could become exposed as a result of the merger. Citizens and legislators alike began to contemplate the ways this information if compiled could be abused.

A report entitled *Records, Computers and the Rights of Citizens* (Department of Health, Education and Welfare, 1973) issued by the, made specific recommendations for laws that would implement and enforce the code. Specifically they recommended that governmental organizations that kept automated databases on individuals enact safeguards to protect this data and be required to report to the public each year what databases they were keeping and what information they were collecting. Additionally they set out rights of people whose information was stored would have over the access to and correction of data.

This report recommended a code of fair practice be enacted by Congress for automated personal data systems. For this Code of Fair Practices four principals were enumerated:

- There must be no personal data record-keeping system whose existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuse of the data.

In response to this report, The Privacy Act of 1974 was enacted to insure that individual privacy was maintained in light of the technical advances in the creation and use of computerized databases (Electronic Privacy Information Center, 2003). The Act was far from comprehensive. The Act only applied to U.S. citizens and permanent residents. Not all federal agencies, and no state and local agencies are covered by the act, although all federal, state and local agencies are subject to limits placed on the use of Social Security numbers (Privacy Act of 1974, §7, 2003). Government controlled companies like the Post Office, the military, Executive agencies like the Department of Education, the FDA and the FBI, executive departments; independent regulatory agencies and government controlled corporations are all exempt. Of the agencies under the umbrella of the Privacy Act, only the databases of those agencies which retrieved information by the name of the individual or a personal identifier of the individual (this schema was referred to in the act as a system of records) were subject to its provisions. Should a database contain this information but that information not be retrieved by the individual's name or a personal identifier, that database would be exempt from this act so as to create a huge privacy gap.

The Act required publication in the Federal Register notice that the agency was keeping such records and include the details of their systems, the records and the intended uses of the system. People were allowed to submit data, views and arguments to the agency. An emasculating provision of this act was how change would be managed. Any proposed changes did not require a publication but only required notice to be sent to a committee in the House and Senate as well as to the Office of Management and

Budget.[1] These bodies were charged to evaluate the probable and possible effect of the proposed action on the rights of individuals only. These bodies did not have authority over the agency, no direct ability to stop the proposed action or any ability to propose a compromise solution.

Other provisions of the act limited the collection and use of the information of individuals by the government and provided means in which the individual could monitor governmental activity through requirements of disclosure by government to the individuals of both the information held in their files and its use by the government. Any individual who has access to any records the agency held on him, be allowed to review the record and make copies. If the record were incomplete or inaccurate, the individual could ask the record be corrected and the agency had 10 days to respond by either making the change or telling them why they refuse to make the change. The agency must also provide a name of a supervisor in which to appeal the action taken. If appeal is taken action must be completed within 30 days unless extended for good cause. If the appeal is unsuccessful, the agency must tell the individual how they can pursue this matter in court.

The act required agencies to keep accurate records of when, to whom it has disclosed personal records maintained five years or the lifetime of the record what ever is longer. Agencies are also required to maintain only the minimal amount of information relevant and necessary for its operation. When the information can have an adverse effect upon the individual, effort must be taken to collect the information from the individual

[1] Notices to the House would go to the Committee on Government Operations of the House of Representatives. Notices to the Senate would go to the Committee on Government Affairs of the Senate.

directly. When collecting this information directly, the agency must tell the law which gives them the authority to collect the information, the uses of the information and the effects that might result from the data not being provided. Other collection restrictions include the collection of records describing how an individual exercises rights guaranteed by the first amendment and places limits on data sharing between government agencies.

The act provided both civil as well as criminal penalties for its violation.

Many of the shortcomings of the act are contained in the paragraphs above. As significant as those may appear, there were more. The act required the creation of the *Privacy Protection Study Commission,* whose purpose was to submit recommendations to Congress regarding further implementations and enforcement. The act also required the President to submit a report every two years on the oversight of the Privacy Act. The first and only report made by *Privacy Protection Study Commission* was a report that was issued in 1977. This report concluded that the act was a great step forward but it failed to bring about the benefits intended (Privacy Protection Commission, 2007). The shortcomings of the act were the result of the fact that much of the act's language was unclear and a key term "systems of records" [2]enabled wholesale violations of individual privacy. No action was subsequently taken by Congress to address these shortcomings or limitations. The Act's requirement of the President submitting a report every two years

[2] The Privacy Act applied only to databases where database records were retrieved by name, Social Security Number or other individually identifiable information. These records were the systems of records. If a record contained this information but could be retrieved by another manner that did not use a system of record, it was not subject to the provisions of the act. Conceivably a governmental agency could circumvent the act in this manner causing harm to the individual.

on the oversight of the Privacy Act was repealed in 1995 (Public Law 104-66, 1995). To date there is limited oversight of the Act.

Use for Law Enforcement and the routine use exception continue to erode the effectiveness of the Privacy Act of 1974. Effective law enforcement requires the ability to exclude criminals from the files that involve the investigation of them by a law enforcement agency. Agencies use the law enforcement exception to justify exception to the provision of the act. The effects of 9/11 and the Patriot Act has further limited the ability to keep this provision narrow and have opened up new and greater exceptions.

Agencies can only disclose information to others if they either have the individual's permission or the disclosure meets one of twelve conditions outlined in the act. Examples of such permissible disclosure include a disclosure pursuant to a court order, a disclosure to Congress, a disclosure of compelling circumstances affecting someone's health or safety. Agencies also can disclose information if it is for a routine use an exception that agencies have abused. Routine use is defined in the Act as "the use of such record for a purpose which is compatible with the purpose for which it was collected." This phrasing can often lead to "mission creep" for a system of records, in which the routine uses for a particular database gradually increase until its scope is far greater than its originally stated goals (Electronic Privacy Information Center, 2003). While it is a requirement of law that routine uses be stated in the Federal Register this requirement is met with broad sweeping language which can justify any use under the sun. While some court decisions have limited how broadly an agency can describe

"routine uses" (Britt v. Naval Investigative Service, 1989) a large number of uses can still be covered by a short, general statement.

1.1.3 Example Three: Medical Information and information portability

- Technology changes affecting information use causes corresponding effects upon society, particularly the roles and relationships created by society to protect and ensure privacy. The third example demonstrates that unless technological change is managed it will recreate roles and relationships. Certain roles and relationships in society require privacy protection to function optimally. Institutions have evolved rules of behavior that protected private information. Technology change and the hunger for the information it can produce have disabled the effectiveness of these institutional rules- thwarting both the ability of the institution and the individual to control sensitive information. As a response, information providers have adopted counter measures. These counter measures have included the withholding of information, the delay of disseminating information and the providing of inaccurate information all of which have harmed the effectiveness of the institutions serving the information providers.

The increased use of private insurance in the mid 1960's altered the doctor patient relationship by adding new participants into the relationship such as insurance companies, HMOs, self-insuring companies, ending the era when all medical information remained between the doctor and patient. For a variety reasons such as cost containment, risk management, fiscal responsibility, efficient practice of medicine and or the need to monitor professional practice abuse, the disclosure of medical information and

information given in pursuit of medical treatment was required to be disclosed to these third parties. These third parties had no direct relationship to the patient and no incentive to protect the patient's information. In many cases third parties often profited greatly from having access to this information through either its use or its dissemination with the patient bearing the entire expense (Electronic Privacy Information Center, 2003).

Information technology lowered the cost to share information and created new ways to aggregate and use information. This better enabled better use of information in ways never before imagined. Information technology enabled more reviews to take place of the physician work, and enabled health care organizations to be better able to follow and to review practice guidelines and utilization standards compliance by physicians (Field, 1994). Information technology also allowed more information to be shared outside the medical caregiver context. Insurance companies increasingly ask for more information and use that information to assess risk and implement policy of insurability. Employers are increasingly using private medical information. Employers can assess their employee's potential in new ways. Employers can use the studies compiled from computerized medical records to compare the performance of different managed care plans (Field, 1994). In addition, employers may use this information to screen workers for preexisting susceptibility to workplace health hazards (Field, 1994).

The concern that interconnected medical and insurance information systems caused medical privacy erosion surfaced during the debate of the Health Security Act in 1994. The debates evidenced a concern that the increased ease of transmitting and sharing individual health information resulted in an increase in concern regarding privacy and

confidentiality of that information (Federal Register, 2000). It was found that increased protection of medical information access and use was necessary for the quality of medical care to increase (Rotenberg, 1994).

What fueled the debate was the recognition that the United States as a country expends about one trillion dollars on health care each year (Hoekendorf, 1996). Despite these expenditures, healthcare outcomes in the United States fail to achieve high outcomes. In fact when ranked with other countries, the United States fails to outperform and in many cases lagged far behind other countries in results obtained despite those countries expending less money in total and per capita (Federal Register, 2000)..

When obtaining medical treatment patients must participate with a medical caregiver. For the optimal treatment effects to occur an accurate and full disclosure of relevant facts must be provided by the patient to the treatment giver. It was also found that many of these fact and information required to be provided by the patent to the caregiver are of a personal and sensitive nature (Federal Register, 2000). In studies conducted by the United States Department of Health and Human Services a relationship between trust and treatment outcome was found. When the patient has high trust in the provider, more information and more accurate information is provided to the medical provider by the patient. On high trust situations patients seek care earlier. When the trust is low the patient withholds information, knowingly gives inaccurate information or delays or fails to get treatment. As accurate and full disclosure of information and prompt seeking of medical care is a prerequisite of delivery of quality medical care, it was concluded that health care professionals who lose the trust of their patients cannot deliver

high quality care (Federal Register, 2000). It was specifically found that the medical community in the United States had lost the trust of its patients due to the belief that their privacy in their medical information was violated (Federal Register, 2000).

During this study, patients voiced great concern over the dissemination of their medical information to others outside of the patient caregiver relationship. Many patients noted stories of harm that had come to them by individuals or company or companies acting upon this information. Firings, demotions, loss of upward mobility in the workplace, decreased insurability, loss of insurance, humiliation are just a few of the effects that have been suffered by individuals when this information has became disseminated. In many cases individuals and their families admitted to having delayed treatment or failed to seek treatment resulting in more illness, spread of illness to others, loss of productivity, greater medical costs and in some cases premature death. In a separate study, the United States Department of Health and Human Services has noted these same concerns (Federal Register, 2000). In an effort to foster improved health care information privacy and increase the quality of medical information HIPAA was enacted in 1996.

1.2 Difficulties with the Existing Definition of the Nature and Purpose of Privacy

Gerty expressed the problem faced by lawyers and judges when they attempt to define the nature and purpose of privacy, "…comes not from the concept's meagerness, but from its amplitude, for it has a protean capacity to be all things to all lawyers." And he also provides the warning, "A legal concept will do us little good if it expands like a gas to fill up the available space" (Gerty, 1977).

This problem expands beyond lawyers and judges. Take any group of people and ask them to define the nature and purpose of privacy and you will get varied responses. It should come as no surprise that philosophers and legal scholars have attempted to define the nature and purpose of privacy and have failed to reach a consensus. W.A. Parent, a philosopher, defined privacy as a condition of not having undocumented personal knowledge about one possessed about another (Parent, 1983). It has not been widely accepted. To others control over information is the basis of their definition of privacy. Fried saw privacy as control over personal information about one's self (Fried, 1968). Westin another advocate of control proffers that information privacy is the claim that individuals or groups have to determine the conditions under which information about themselves is communicated to others (Westin, 1967). Froomkin centered on what happens after the proper release of information. Privacy according to him is the ability to control the acquisition and release of information about one's self (Froomkin, 2000).

Privacy has been defined as a necessary condition for the construction of autonomous individuals. This is described in the literature as private psychological space (Zweig and Webster, 2002), or as a condition necessary for the construction of self (Reiman, 1976), a place to construct their identity (Goffman, 1957) intellectual privacy (Cohen, 2003) or emotional space. Privacy has been seen as a right: a right to be left alone, a right to autonomous choice regarding intimate matters, the right to autonomous choice regarding personal matters (Froomkin, 1996). Privacy has been characterized as an individual interest in avoiding disclosure of personal matters and an interest in independence in making certain kinds of important decisions (Whalen v Roe, 1977).

Others define it as a limit on what is known and who may know about one's personal affairs (Gross, 1971). These philosophers discuss this type of privacy in terms of access to the person and information about the person.

Still another group of philosophers focus on privacy as a condition necessary to form relationships. Rachels sees privacy as necessary to maintain the variety of social relationships that we want to have (Rachels, 2006). Fried sees the title to information about oneself and protected by privacy provides the necessary something to the relationship " ... intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone" (Fried, 1968). Reiman finds that privacy protects the individual's interest in becoming, being and remaining a person (Reiman, 1976). Inness defines privacy as a defensive action, protecting intimacy and ensuring freedom of action and the protection of our autonomy (Inness, 1992).

There are many reasons why there is no consensus on a single definition of the nature and purpose of privacy. Some of the reasons discussed here are: the nature and purpose of privacy is socially constructed concept through a process that is influenced from forces within and without society and although the concept is socially constructed it varies both within and across cultures. The defining of the nature and purpose of privacy is a work in progress. Privacy is multidimensional in purpose. It is not only a value that has many dimensions but also is a perspective that orders life. Privacy is a value and process that produces data. It is difficult to translate any value into a control mechanism. Privacy is particularly difficult because the translation process is often attended by self

interest and politics. Often time these specifications are purposefully poorly done. Privacy is a value that encompasses many diverse values and purposes and is not a single valued concept. Finally, definitions and rights of privacy change as technology changes

1.2.1 Reason One: Privacy is a value that is socially constructed

Social construction is subject to influences both from within and without societal boundaries. These influences cause conceptions of what is private often to vary across cultures and within the culture itself.

Conceptions of privacy are socially constructed (Bezanson, 1991, Scanlon, 1975, Rachels, 1975). This social construction is from the summation of all entities in society and is not the conception of privacy of any one individual of that society. As an illustration, in law, Justice Harlan explained that reasonableness of the individual's expectation of privacy entailed a two-part, expectation-driven test. First, the defendant must have an actual or subjective expectation of privacy. Second, the expectation must be "one that society is prepared to recognize as "reasonable" (Katz v. United States, 1967). This illustrates the symbiosis between the expectation of the individual and society's conception of privacy. What a society deems as private is ultimately constructed from the views of its members. While each member of society has their own personal, actual, and subjective perspective as to what is or is not private for it to reap to a level where it is respected and protected, society must sanction that individual view as being reasonable. The conception of the nature and purpose of private is not static. As change occurs in the privacy expectations of individuals so will the construction of privacy change (Spencer, 2002). This change occurs during the periods where individuals express and assert their

perceived conceptions of privacy. During this process societal opinion is examined in light of the assertions made. Some of the new ideas of privacy grow, while others fail to flourish and die. It is only when the majority or dominant opinion of society accepts that individual opinion that a social expectation of privacy is formed. Therefore the construction of privacy is an interactive process between the individual and society itself influenced by forces that influence society itself

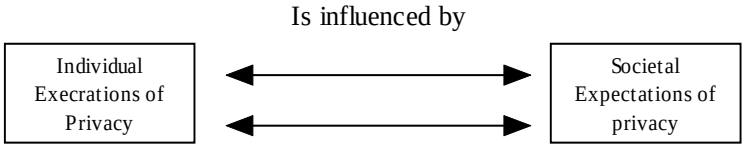

Figure 1 Interactivity of Individual and Society Privacy Expectations

1.2.2 Reason Two: The defining of the nature and purpose of privacy is a work in progress.

The definition of privacy is a work in progress. The definitions of privacy are difficult because not all individuals within society agree with the social construction while social construction determines the extent to which people are expected to expose their lives, their personalities, their attributes and their behavior to public scrutiny (Schauer, 2000). Often entities will express their disagreement openly and work to effect changes in its definition and application even after specification. Additionally an individual entity or group of entities with power and purpose can affect a change in a society's conception of privacy. It has been observed that individuals and groups who use cutting edge technology and knowledge of the legal process have affected societal change in the past (Spencer, 2002).

The environment where privacy is constructed is also undergoing constant change. Technological change places pressures on and affects social values through the changes it makes in economic and social systems making what is private a moving target (Inglehard, 1977). As technological capabilities increase traditional conceptions of privacy have undergone change. "People's subjective expectations of privacy tend to reflect the amount of privacy they subjectively experience; and as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished" (Rosen, 2000).

Because privacy is socially constructed, privacy varies across different cultures, even between strata with in a society, as it is a product of varying social and cultural understandings (Schauer, 2000) as each culture has its own unique environment. What is private appears to depend upon the situation, the type of privacy invasion and the parties involved which has lead to the conclusion that privacy is contextually specific.

1.2.3 Reason Three: Privacy Supports Not One but Many Purposes

Privacy as a value does not support a single purpose. One reason for the lack of consensus on the nature and purpose of privacy is privacy supports many different purposes, sometimes simultaneously and sometimes these purposes conflict. The nature and purposes of privacy include: Privacy stems out of respect, fairness and responsibility due toward others (Innes, 1992). Privacy emphasizes that a person is an agent free to act who is only responsible to others in cases of necessity or agreement (Nissenbaum, 1998). Privacy is the value that a person should be able to construct and shape relationships with others (Reiman, 1976). Privacy also emphasizes the value that the individual should be

able to construct his own self. Privacy also recognizes with in limits, each individual has the right to determine the extent of his thoughts, sentiments and emotions be communicated to others (Brandeis and Warren, no year). Historically privacy has been used to protect a person's property and liberty (Warren and Brandeis, no year). It is also a value that ensures structures that support privacy which in turn ensure a desired way of life such as the ability to have intimate relationships, or to read, study or develop one self in private. Without privacy, life as we know and enjoy it would be very different and less desirable (Inness, 1992). With each purpose the specification of the value of privacy varies contributing to why there is no consensus on a single definition of the nature of privacy.

1.2.4 Reason Four: Privacy is a perspective that orders life.

Through privacy, daily life is regimented through social and technical mechanisms that arbitrate which data (and information) is produced (Agre, 1998). Once a value is created it becomes a perspective that orders life.

> "…(**privacy** is) … **infects our way of experiencing** the social world and which **affects social life** in profound and subtle ways. As a social concept it has normative and descriptive functions that interact with one another. The concept of privacy regulates institutions, practices activities and social and individual life generally. It controls what people feel they have legitimate access to and in this way fosters both possibilities and limitations." (Schoeman, no year)

1.2.5 Reason Five: Privacy is a both a value and a process which produces data

Privacy is a social technical process that produces data. Privacy is translated into definitions, laws and norms (Agre, 1997). These laws and norms create roles of

acceptable and unacceptable behavior that are characterized as rights. It is through rights privacy becomes the arbitrator of what data and information is useable and what data is off limits. Data and information that is designated as not available and useable is private while all other data is public data available for all to use.

It is difficult to translate any value into a control mechanism. This difficulty is increased because the translation and interpretation process is attended by self interests and politics. Additionally confounded definitions of privacy are often created to obtain personal agendas when consensus cannot be met.

In the specification of control mechanisms, values of privacy are translated into laws and norms enabling the realization of desired values of privacy.

1.2.6 Reason Six: Privacy is Not a Rational Concept

We cannot forget that the people who compose society and define their nature and purpose of privacy are both rational and emotional beings. As a result privacy as a concept and construct has both rational and emotional elements. For many people, the personal natures of the decisions which accompany privacy do not wholly allow a person to coldly remove the emotion from the decision. Often a person develops his opinion of privacy, at least in part, in an irrational manner, and subject to their whims and emotions (Inness, 1992). Additionally society is not largely composed of mature rational thinkers. Many more people make their decisions on privacy not on rational thought but on the feeling that they have about the decision. Additionally the construction of the nature and purpose of privacy at least on the part of individuals is often motivated by self interest. Many times individuals looking at the calculus of the situation will weigh out the

advantages and disadvantages of privacy looking for the advantages to them not the benefits that would accrue to others or benefit the whole of society.

1.3 Privacy Research in the Information Sciences

While the field of Information Sciences recognizes that privacy issues present pressing issues to business and is a critical area of research, past research is sparse, inadequate, single paradigmatic in nature, and possesses few theories. Privacy as a term does not have a single agreed upon definition; nor is there an espoused epistemology, ontology or axiology.

Little research on the topic of privacy has been done in the Information Sciences despite Mason's statement that privacy research was one of the most important "ethical issues of the information age" (Mason, 1986). Links between organizational privacy practices, individual perceptions of those practices and societal responses have been recognized (Smith et al, 1996). Davison in 2003 observed that studies in privacy appear not to be keeping pace with the growing interest in privacy (Davison et al, no year). As late as 2005, Greenaway has characterized the present stream of research has been proven insufficient and the research relies upon a single paradigm to explain all organizational level privacy behaviors (Greenaway and Chan, 2005).

When privacy research pursued, it is generally discontinuous with previous studies. While there have been numerous studies conducted in privacy in the MIS tradition, this researcher could find no MIS work building upon previously completed studies in privacy other than an acknowledgement that other researchers had done some type of privacy research. As a result there is a paucity of theory in the Information

Science discipline to guide the understanding of organizational information privacy behavior (Greenaway and Chan, 2005). While calls for a new theory have been made to assist in the understanding of similarities and differences in the information privacy approach among firms (Milne and Culnan, 2002), only Greenaway has offered research in this area that provides new theory.

In an effort to assist with privacy concerns, privacy research has increased in many academic fields. In each of these disciplines, they have in place a definition of what is privacy, what is private information, and what is the value of privacy. In some fields, their definitions reference definitions in other disciplines most notably law referencing philosophy on this topic. But in MIS research, we have not referenced another discipline nor have we adopted a definition of privacy. At best, only a handful or researchers have attempted to define privacy or what private information is or what values privacy is supportive. All that exists are general sweeping statements exist about privacy based upon control. As way of example, Greenaway uses the definition that privacy is the ability of the individual to personally control information about them (Greenaway, 2005). Hu and Teo adopt Westin's definition that privacy is an individual's ability to control the terms by which their personal information is acquired and used (Westin 1967).

MIS research has not focused on the axiology of privacy having only tangentially commented on the importance of privacy and the values that privacy supports. Other disciplines have directly explored the values privacy supports directly and from that focus on values, they have defined privacy in ways outside that of control The following is just a sampling of what has been offered as a definition of privacy in past research from fields

outside of MIS through the focus on values: Privacy is the right invaded (Prince Albert v. Strange, 1849). Privacy pertains to the regimentation of diverse aspects of everyday life through social technical mechanism by which data is produced (Agre, 1998). Personal privacy is simply another extension of property rights; like income and wealth, privacy is an emanation of each man's ownership over his own life (Newhard, 2004). It has been described as a right: a right to be left alone, a right to autonomous choice regarding intimate matters, a right to autonomous choice regarding personal matters Froomkin, 1996). "(Privacy is) part of the inner person" (Emerson, 1979). It is the freedom from unreasonable constraints on the construction of ones identity (Clarke, 1994). Privacy can be an interest: "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions" (Whalen v. Roe, 1977). "Privacy is the condition of not having undocumented personal knowledge about one possessed by another" (Parent, 1983). Studies need to be conducted on what is the value of privacy research and what values does privacy support. This will clarify what is privacy and the understanding of the construct of privacy and enable us to construct a better construct.

Writers in other disciplines before espousing theory, have often discussed the philosophical concepts they believe that are directly related to research such as ontology, epistemology, values, ideologies, history, politics, and social and cultural contexts (Patterson, 2000; Paul & Marfo, 2001; Slife & Williams, 1995; Smeyers & Verhesschen,, 2001). Slife and Williams observe that the hermeneutic philosopher Gadamer (Gadamer, no year) contends that before the development of theory there is always an operative

understanding of truth. It is this (pre)understanding of truth that makes it possible to frame any method at all. Without this understanding we could not formulate any method because we would not know what the method should be like—or that we even need a method. This means that understandings of truth produce methods, rather than methods producing truth. Methods, including the scientific method, are only devices we use to convince others and ourselves that our ideas are in some sense sound. Methods do not establish the truth of the matter (Efinger et al, 2004).

In philosophy privacy's epistemology has been exhaustively studied but to date, no attempt been made in MIS research to examine the basic epistemological basis of our construct of privacy. An examination of privacy's epistemology will not only help us in the choice of methods in which to conduct research but also through an specification of an epistemology a paradigms for research will be established. Those paradigms will improve our understanding of privacy. The understanding of the epistemology of privacy will enable the development of theories of privacy in the MIS discipline. It will assist us in the choice of methods to study the concept. Another benefit of this examination is that it will allow us to compare justifications for truth and understand seeming similar studies that differ in conclusions that are in fact not based on the facts of the study but on the epistemology of the researcher.

1.4 Purpose of the Study

This section will identify the audience to which this study is directed and after specifying the audience will specify problems that need to be solved.

1.4.1 Intended Audience

A study of privacy in the MIS tradition can be directed to both the business community and the technical community. It can also be directed to the legal community, particularly where laws impact upon business and business operations. I will address this proposal to all of these audiences.

1.4.2 Problems and Opportunities

To the business and technical community privacy presents many opportunities to the organization that can manage the problems of privacy. Some of the problems that can be addressed from this study include the following:

1.4.3 Address the calls for a better understanding of privacy.

Despite Mason's statement that privacy is one of the most important ethical issues of the day (Mason, 1986), MIS field have not made our statement as what constitutes privacy. We as a discipline are calling for more theory on privacy to support organizational privacy research, but we have no epistemology, ontology nor do we discuss what the value of privacy is. Where privacy definitions have been attempted it has been defined only in terms of control. When we have conducted research, our research does not build upon past research.

To address this problem an exploration of the epistemology of privacy adopted from philosophy will be undertaken. From this a new multi dimensional construct of privacy which encompasses relationships, privilege relationships, personal development and expression, business secrets and public life will be proposed one that will be grounded in philosophy and supported by law which establishes roles of behavior.

1.4.4 Integrate Legal and Business Knowledge and Research in Privacy

The adoption of new media involves the shifting or blurring of the boundaries of public and private. (Meyrowitz, 1985). Due to increases in technical capacity to gather, transfer, store and farm information, a pressure exists to both assure and protect the fundamental values that compose privacy. As a response, seemly endless streams of new laws are being enacted to ensure traditional values, to protect existing norms, and clarify privacy boundaries.

Responding to changes in social and legal privacy mandates has become an ever increasing cost of doing business. Business has high motivations to act in this manner as the penalty for non compliance is high. When any system is found to be insufficient almost certain loss in money and time will occur to the business due to legal action – real or threatened. Other losses include the inability to attract and keep customers, effects on employee productivity, morale and retention, and the inability to keep up with other key players in the industry. In a firm both the business side and the IT side of the firm need to make adjustments in strategy, tactics and operations to meet these mandates for privacy. Business lacks the language and understanding of law to fully recognize these mandates, to interpret and define what is required and to anticipate how best to implement privacy measures in a manner that protects legally and socially mandated privacy protections. This lack of understanding of law also hinders business in making assessments on whether the proposed measures are sufficient to meet both the mandated and anticipated future privacy standards. One cost borne by a firm is the seemingly constant rework of plans and in place systems to meet mandated privacy standards resulting in substantial

costs in time, effort and money. To avoid these costs and to ensure socially and legally mandated privacy, businesses have resorted to implementing plans and systems that are overly specified, costly to implement only to find the resulting system fails to meet the requirements for the business, is cumbersome to use, full of vulnerabilities, and prone to be reworked and redesigned at great cost when the next unanticipated change is mandated.

Laws are that are enacted by legislatures often interpreted by lawyers and judges are done by individuals with no understanding of the implications on the business community. These same individuals do not understand how business operates let alone how their law, or the application or interpretation of law will affect business. Strong criticism has been levied by the business community toward the legal/legislative community on these issues. Recently a call has been made in the legal community to bring together both the legal and business schools of thought to create a single integrated legal/managerial school of thought (Holloway, 2005). From the business side the purpose is to promote a better understanding of law by business decision makers. This would assist business decision makers in the making of decisions that are compatible with law and policy. A second purpose is to provide better tools and methodologies to evaluate that both the decisions made and the consequences of the decision are compatible with law and policy. The end result would enable decision makers to better weigh decisions against the public policy and promote better decisions that affect society growth, stability and direction For the legal and policy practitioner, the purpose is to promote a better understanding of business theory and methodology so that the impact of law and policy

on business theory and methodology can be better assessed. It would also assist lawyers and legal decision makers understand how legal advice and legal analysis can assist the process of business decision making. These goals would assist in the alleviation of the trend toward pervasive regulation of the workplace by law and better instruct law in how it impacts business theory and directives. The end result would promote a better integration of law and business (Holloway, 2005). This study will assist in reaching those goals.

> A specified privacy basis in philosophical and legal terms as well as a better specified construct of privacy will enable both law and business a better understanding of privacy and make clearer the requirements that must be met to enable legal and business privacy solutions to be proposed, selected, implemented more effectively and efficiently and understood more completely. Less time and effort will be spent on reworking systems to add unanticipated functionality or in designing into systems the requirements to meet mandated functionality for both the present and the future. Finally this will provide a better way to exploit technological change and preserve status quo or at least reconcile status quo with technological changes.

1.4.5 Increase Privacy Management Capability

Privacy management is a skill required to meet the problems and opportunities faced by the firm. In many cases privacy management is a potential competitive advantage.

With mandates from law and society for increased privacy protections, business find themselves involved with solving problems or exploiting opportunities. In some instances a business' ability to meet privacy concerns can provide them a competitive advantage over firms that do not meet these concerns. These problems, opportunities or

potential competitive advantage can result from creating better relationships with external customers or creating an better working environment for its employees.

Business strategies are frequently adopted to respect various privacy interests of its external customers. These strategies include building better customer relationships and loyalty, developing and sustaining trust, promoting an image that engenders favorable attitudes toward the business, assisting in the development of brand to name a few. This is especially effective when the company is able exceed the privacy expectations of its customers yet gain maximum benefit for itself. Because individuals have a great concern over the erosion of their privacy, privacy standards and controls can create, build and sustain these conditions especially when used as a methodology of maximizing the value of the customer relationship.

Employers are always looking for ways to increase productivity. In knowledge creation environments, creativity has been found to be stifled when too much control is placed over the individual. The line between what is seen as an invasion of privacy and what is not is critical when developing the optimal work environment for the creation of knowledge. Worker productivity, morale and satisfaction suffers when privacy is invaded in the workplace.

Business however has difficulty in developing these relationships because of these types of questions: How do we capitalize on consumers concerns for privacy and create a sustainable competitive advantage? How do we construct privacy strategies that encompass the concerns of the external customer that enable the solving of problems, exploitation of opportunities and create competitive advantages? How do we provide for

worker privacy concerns yet retain needed control over the workplace? How do we implement and enforce privacy yet remain competitive with our rivals?

> This study will give business a new tool to address problems and opportunities presented by privacy. When initiatives are taken often they fail due to unanticipated functionality and requirements and the inability to develop solutions with existing understandings and tools. Being able better model privacy and from those models create information tools that support the business strategy of capitalizing on consumer and employee concerns over their privacy invasions will result in substantial benefits accruing to business. The specifications of privacy provided by this paper will enable businesses to construct a strong privacy strategy, develop a sound tactical plan and execute the plan to its best potential.

1.4.6 Design privacy into the tools of business to ensure privacy

How do we design privacy into our information tools? A problem exists of how to implement technical controls on private information and solve the issues of planning for privacy in the initial design stage. Should this be accomplished, the result would be lower costs of implementing privacy safeguards, increased performance of systems using privacy safeguards, fewer security concerns, fewer security breaches and less risk of failure.

Presently privacy is designed into the system after the data model has been established. Once the data model is completed, a database tool is implementing on top of the data often using a system of views, privileges and security tools to ensure privacy. Other methods are a series of triggers which utilizing programming to enable those with the correct access codes to obtain information they desire. Oracle has introduced a concept called the Virtual Private Database which matches roles and permits greater

abilities to program security into the system but this too is done after the fact. New methods include notifications issued when certain information is accessed but this suffers as a check on the system and is not proactive. The problems with these after the fact systems are numerous. First is they are very expensive to design and implement. Risk of failure is high due to the fact privacy is not designed at the inception of the system. Privacy controls and protections are placed over the data model. Often these are custom designed. Holes and vulnerabilities are often found once the product has been implemented. Other times the tool fails to provide the level of privacy mandated by law or expected by consumers or fails to provide a required level of service or both.

> This study will assist in the creation of tools, the planning and construction of infrastructure and systems, and the applications of these to the problems and opportunities of the business I propose to create a role based information technology design tool composed of law and social norms and information technology design. This tool will design privacy into the information as well as into the mechanisms that sit on top of the information. Each data attribute will have a sensitivity level as well as certain possible data values with in the range of possible data attributes. I propose that the user's role and view instead of being a first level protection is but a third level of privacy protection. This tool will enable the an evaluation of the instantiation to be made regarding its compliance with legal and social norms, its ability to cope with changing environments, The tool will enable more effective designs, at less cost in term of money, time and resources. The tool will enable better designs in terms of quality. Designs constructed will meet the strictures of society and law, be better able to withstand changes made in the environment by technology changes and the accompanying legal changes made to insure traditional values.

1.5 Nature of the Study

This research study will be conducted using Design Science methodology. Hevner (Hevner, no year) presented a framework for understanding, evaluating, and executing Design Science research in IT. Design Science in the context of Information Technology is ultimately concerned with the construction of solutions to problems as well as the creation and exploitation of opportunities in the business environment.

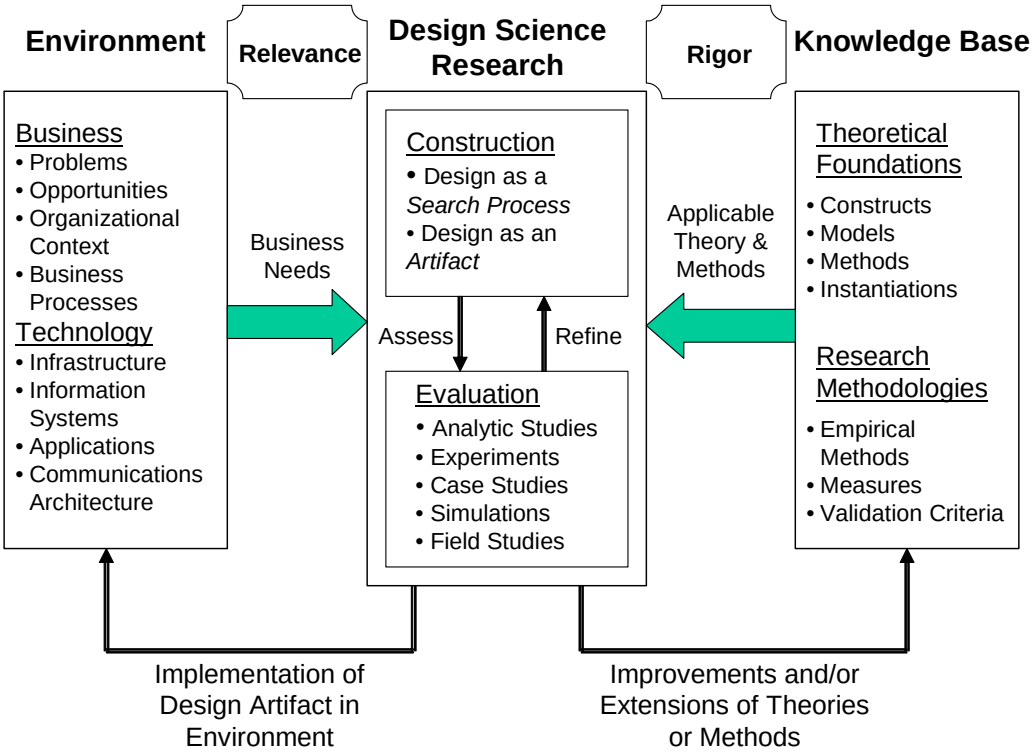

Figure 2 Hevner et al Design Science Model

Business seeks solutions to problems. Problems are the difference between where we are and where we want to be. Business also needs to exploit known opportunities and to create new opportunities. These can exist in the organizational context or in the

business process themselves. For business to meet its objectives efficiently and effectively, technology must be aligned with the business structure and business strategy. There are often issues in the infrastructure, information systems, applications and communications architecture that must be solved in order to better meet business problems and opportunities. Design Science can accomplish this directly through the solving of a business or technology problem or opportunity through the construction of a solution. The solution created can extend human and social capabilities or these solutions can modify the environment to enable a new solution (Heavner, no year). Indirectly these problems can be solved and opportunities created and exploited through design science by the creation of new ways to evaluate proposed solutions. Another indirect solution to problems and opportunities is through the creation of new and or bettering our existing theoretical foundations or through new and or better research methodologies. The goal of design science is to have these new artifacts (solutions, new evaluation techniques, better theoretical foundations or research methodologies) become adopted and "cause humans to abandon their previous problem producing behavior and devices" (Fuller, 1992).

The knowledge base is used in design science to construct both the search and solutions to problems and opportunities and to create new opportunities. The knowledge basis of Design Science is composed of Theoretical Foundations and Research Methodologies. Theoretical foundations include constructs, models methods and Instantiations. Constructs provide a language in which problems and solutions are defined and communicated; Models enable understanding and the exploration of effects of design decisions and changes. Methods provide guidance to solve problems. Instantiations

demonstrate feasibility as well as provide empirical evidence that the artifact achieves its purpose, or enables the researcher to learn and study the real world and how the artifact affects it. Each of these will be examined with the rigor of those fields.

Previously stated privacy presents both a problem and an opportunity for business. Since Design Science is concerned with the creation of solutions to problems and the exploitation of opportunities this makes it an ideal vehicle to conduct this research. The creation of a role based information technology tool and applying it to improvement of privacy in the business makes Design Science a suitable tool for this research. Design Science support the creation of both tools and instantiations to provide a proof of concept.

1.6 Anticipated Contributions

This proposal anticipates four contributions: Provide a better understanding of privacy; Integrate legal and business knowledge; Increase privacy management capability; Increase the ability to design privacy into business tools.

1.6.1 Address the Calls for a Better Understanding of Privacy

Present research in MIS has failed to recognize or define an epistemological, ontological, axiological basis for privacy. The contribution of my study will increase the MIS knowledge base in privacy. My proposal will contain an epistemology of privacy adopted from philosophy. I will also extend from philosophy and law an ontological and axiological base for privacy.

While both law and philosophy have examined privacy, each has approached privacy much like MIS, seeing it as a single construct[3] and attempting to apply it to a variety of situations. This application has created a morass of conflicts making privacy appear to be situational specific. Certain patterns emerge in my examination that show privacy is not a single unified construct but a multidimensional construct which is differentiated by the role information plays for the entities providing or using that information. I will provide a new multi dimensional construct of privacy that captures the control, access and combination elements and explains the purpose behind the role. This will enable future researchers to gain a better grasp on this concept and apply it as a tool both in their research and to define and solve business problems. I will propose a multi dimensional construct of privacy which encompasses relationships, privilege relationships, personal development and expression, business secrets and public life. The proposed construct will be grounded in philosophy and supported by law which establishes roles of behavior.

1.6.2 Integrate Legal and Business Knowledge and Research in Privacy

How can we integrate legal and business? A specified privacy basis in philosophical and legal terms as well as a better specified construct of privacy will enable both law and business a better understanding of privacy and make clearer the requirements that must be met to enable legal and business privacy solutions to be

[3] In philosophy privacy is viewed either as control based, or as access based or relationship based which is a combination of control but not as a combination. When a philosopher takes that stand all things private are examined in that base. Law has applied these concepts in its construction of societal roles that cover a wide variety of circumstances. Law has not however articulated whether the basis is that of control, access or a combination of control and access.

proposed, selected, implemented more effectively and efficiently and understood more completely. Less time and effort will be spent on reworking systems to add unanticipated functionality or in designing into systems the requirements to meet mandated functionality for both the present and the future. Finally this will provide a better way to exploit technological change and preserve status quo or at least reconcile status quo with technological changes

1.6.3 Increase privacy management capability

How do we manage privacy? Privacy management is a skill required to meet the problems and opportunities faced by the firm. In many cases privacy management is the insurmountable problem that sits between high rewards, competitive advantages and mediocrity. This study will give business a new tool to address problems and opportunities presented by privacy. When initiatives in privacy management are taken often they fail due to unanticipated functionality and requirements and the inability to develop solutions with existing understandings and tools. Being able better model privacy and from those models create information tools that support the business strategy of capitalizing on consumer and employee concerns over their privacy invasions will result in substantial benefits accruing to business. The specifications of privacy provided by this paper will enable businesses to better construct a privacy strategy, develop a sound tactical plan and execute the plan.

1.6.4 Increase the ability to design privacy into business tools.

How do we design privacy into the tools of business to ensure privacy? The problems and unrealized opportunities faced by both the business and technical

community in the arena of privacy are in part due to the failure to understand the concept privacy and apply its understandings to its tools. Many business problems and opportunities cannot be resolved because the infrastructures, information systems and the applications are constructed on the present understanding of privacy and fail to effectively and efficiently support levels of privacy service required by business today.

This study will assist in the creation of tools, the planning and construction of infrastructure and systems, and the applications of these to the problems and opportunities of the business. I propose to create a role based information technology design tool based on philosophical and legal concepts and applied to information technology design. This tool will assist in the design of privacy into the information as well as into the technical mechanisms that sit on top of the information in the form of software and hardware. Each data attribute will have a sensitivity level as well as certain possible data values with in the range of possible data attributes. I propose that the user's role and view instead of being a first level protection is but a third level of privacy protection. This tool will enable the an evaluation of the instantiation to be made regarding its compliance with legal and social norms, its ability to cope with changing environments. The tool will enable more effective designs, at less cost in term of money, time and resources. The tool will enable better designs in terms of quality. Designs constructed will better meet the strictures of society and law, be better able to withstand changes made in the environment by technology changes and the accompanying legal changes made to insure traditional values.

1.6.5 Proof of construct

Finally as a proof of concept, I will utilize the proposed new construct of privacy to demonstrate how it will assist in the construction of privacy into a role based data access tool. As proof of the concept, this new method will be compared to existing methods and the systems constructed by those methods in terms of functionality and correctness. This will also demonstrate the capability of the definitional artifact as well as enable an evaluation potential benefit.

1.7 Outline of the Rest of the Proposal

Numerous contributions will be made by this dissertation which will be presented in chapters 2, 3 and 4. In Chapter 2, I will present additions to the MIS knowledge base from the fields of philosophy and law. In Chapter 3, I will present my new construct of privacy. In Chapter 4, I will detail how I will apply this model to a Role Based Access Control System to improve security in the database/data warehouse environment.

Chapter 2: Philosophy and Law of Privacy

In this chapter a review of the privacy literature from philosophy and law is presented. Law and Philosophy are distinct yet related disciplines. Where philosophy debates the course of society, law implements the course society wishes to pursue. For each discipline a historical review of privacy and the methods of philosophy and law are presented in order to facilitate understanding.

The first section will review privacy's epistemological, ontological axiological basis and relate it to rights and values. The section on privacy will conclude by showing the values privacy seeks to protect are rooted in specific ontology which in turn determines a distinct pattern of rights that ensures the various values of privacy.

The second section of this chapter will review privacy law. The purpose of law is to coordinate, motivate and direct human and non human action through use of value based laws. These laws create rights which define roles that direct human action toward desired activities. A case study of American privacy law is presented to demonstrate that over time the law of privacy has undergone changes to meet the ever changing needs of society.

In Chapter Three, this philosophical and legal analysis is used to demonstrate that the existing conceptualization of privacy is inadequate. Chapter Three will conclude with a new conceptualization of privacy.

2.1 Philosophy and Privacy

This section of the review includes a discussion of philosophical analysis as a method that debates the course of society. Next the epistemological, ontological and axiological bases of privacy in philosophy are presented. From this will emerge three conceptual dimensions of privacy one based on control, another based on access and the final based on both control and access.

2.1.1 Philosophy Is

The word "philosophy" literally translates to “love of wisdom.” It represents a vocation for questioning, learning, and teaching. Philosophy is the pursuit of wisdom pondering questions which are beyond the scope of science. The essence of philosophy is the study of fundamental ideas and methods that are not adequately addressed in specialized empirical disciplines, such as physics or history. Philosophy studies the foundations upon which all belief structures and fields of knowledge are built.

Philosophy is sometimes seen as a particular *method*. The method almost always involves rational inquiry but not all philosophers would agree that rationality is fundamental. Among the rationalists, the form of that rationality varies considerably. As way of example, the Socratic Method focuses on asking questions while the focus of analytic philosophy is on logic and language.

Philosophy can also be seen as the study of a particular subject matter. The subjects of philosophical inquiry are diverse, including metaphysics (the nature of being), epistemology (methods of knowing), and ethics.

Other philosophers see philosophy as a process. Goals of this process include the perfection of the human soul, an answer to the command "Know thyself", seeking the Tao, or, as Ludwig Wittgenstein proposed, an antidote to certain confusions of language

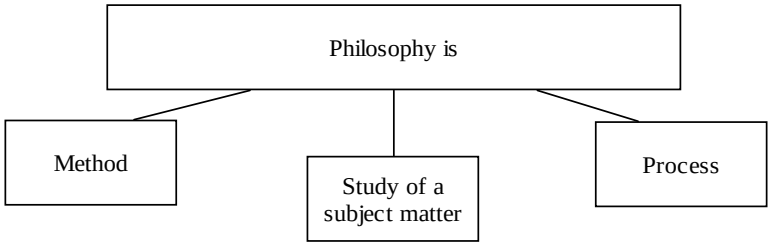

Figure 3 Philosophy Is

The four major orderings of philosophy are Logic, Ontology, Epistemology, and Axiology. From these orderings philosophers conduct their analysis and investigation. Typical concepts analyzed or investigated include existence or being, morality or goodness, knowledge, truth, and beauty. Privacy is one matter studied in philosophy.

2.1.1.1 Rigor in Philosophical Research

Philosophical research is undertaken to discover new facts, to gather new data, to put hypotheses and theories to the test by way of new experimental evidence or calculations all in pursuit of knowledge. Another forum of research in philosophy seeks to refine analyses, develop and advance or criticize interpretations, explore alternative perspectives and new ways of thinking, suggest and apply modified or novel modes of assessment, and promote new understanding. A special case of this type of research is conceptual and methodological critique, involving the scrutiny of the basic concepts

and methodologies of other disciplines, scientific as well as humanistic. Other types of research involve interpretive and evaluative inquiry contributing to the enhancement of our comprehension of ourselves and our world (American Philosophical Association, no year). Philosophical studies also often focus on the meaning of an idea and on its basis, coherence, and relations to other ideas viewing them both microscopically and from the larger perspective of concerns of human existence (Audi, no year).

The purpose of philosophical inquiry is the attempt to think clearly and rigorously about difficult and complex issues and questions. Despite this laudable goal, the American Philosophic Association notes that, "(T)he criteria of assessment of work in philosophy is complex" (American Philosophical Association, no year). This assessment is not always easily made in philosophical circles because of the wide varieties of research conducted on a wide variety of topics. As a rule, research in philosophy must be viewed and assessed in relation to the kinds of issues with which it deals and conform to the norms, standards and practices of the community. Rigor in philosophical research consists of a logical assessment and elucidation assessment. In any assessment of logic of a philosophical work, the quality of the reasoning set forth is paramount. Good logical rigor must not only be logically sound but should not ignore counter examples to the proposed schema even should they be irrelevant or rare. The elucidation requirement is the overall impression of the work asking the question: Does the work create a greater understanding of the matter under consideration?

Agreement with other philosophic work is not a criterion of rigor.

"Disagreement and criticism are among the hallmarks of philosophical life; and it is rare to find two philosophers working in the same area who are in complete agreement with each other. The very best research in philosophy serves more often to generate disputes and differences than to resolve them. It is precisely through such ongoing argument and debate that sophistication with respect to the issues at hand increases, comprehension of them deepens, and understanding concerning them is enhanced" (American Philosophical Association, no year).

2.1.2 Philosophical Underpinnings in Privacy: Epistemology

Epistemology is the branch of philosophy that deals with the nature, origin and scope of knowledge. A basic concept is justified true belief. For something to count as knowledge, it must be true, and be believed to be true. Socrates argues that true alone is insufficient. Additionally one must have a *reason* or *justification* for that belief. Knowledge, therefore, is distinguished from true belief by its justification, and much of epistemology is concerned with how true beliefs might be properly justified. This is sometimes referred to as the theory of justification (Trochim, no year).

There are two different schools of thought in the epistemology of privacy which are diametrically opposed. One school is the Reductionist who believes that privacy is a non meaningful, invaluable concept. The other school is known as the Non Reductionist who take the opposing stance (DeCew, 2002). In the Non Reductionist camp there are two epistemological schools one known as the *Schoeman Distinctiveness Thesis* and the other known as *Coherentists*. The Schoeman School is

Foundationalistic in its epistemology. The *Coherentists* is based in its epistemology in another theory of knowledge known as *Coherentism*.

Epistemological Schools of Thought in Privacy

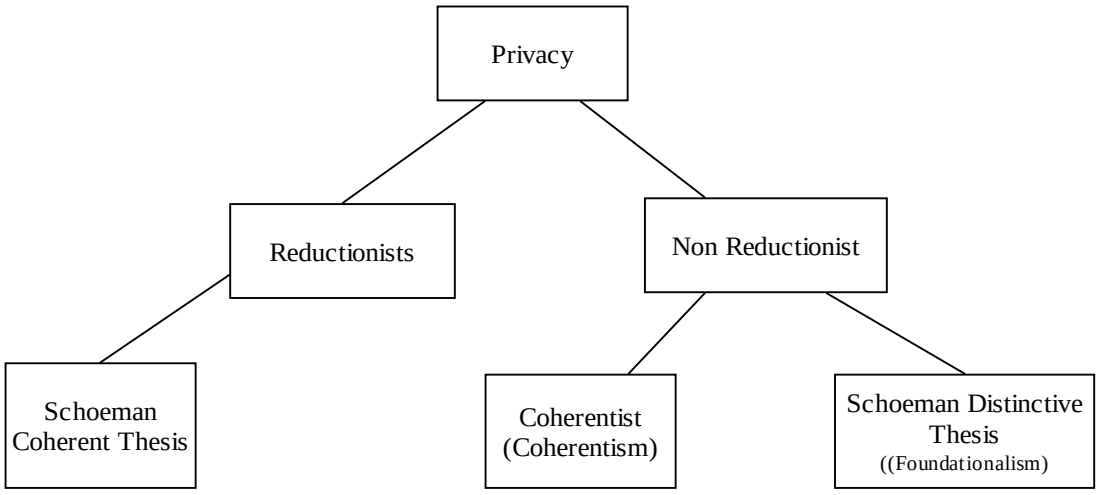

Figure 4 Epistemological Schools of Thought in Privacy

2.1.2.1 Reductionism and Non Reductionism

Reductionists deny that there is anything useful in considering privacy as a separate concept (DeCew, 2002) and that there is "no need to settle disputes within its boundaries" (Thomson, 1975). In reductionism, privacy issues are seen as diverse and disparate and only nominally or superficially connected (Shoeman, 1984). This is supported with the Judith Thompson's observation that with respect to privacy that "no body seems to have a very clear idea what it is" (Thomson, 1975). Besides seeing nothing about privacy is coherent, the reductionist sees nothing that is distinctive or morally and legally illuminating. Privacy is often stated to be represented by a set of

diverse values common to many other social issues that exhaust privacy claims (Shoeman, 1984). Often privacy concerns are viewed as analyzable or reducible to rights and claim of other sorts such as rights over their own person or property (Thomson, 1975) or as a derivative of another construct (Thomson, 1975). When derived, the real basis of privacy is seen by the reductionist not as a concern for privacy but as a concern for one's property interests or for one's right to be his own person (Thomson, 1975) (such as having liberty) or in the stake in maintaining or enhancing his economic or social leverage or defend our concerns in standard moral and legal categories such as emotional distress and property invasions (such as trespass and misappropriation of assets) (Shoeman, 1984).

Thompson elucidates the reductionist position in the following statement:

> "Someone looks at your pornographic picture in your wall-safe? He violates your right that your belongings not be looked at, and you have that right because you have ownership rights – and it is because you have them that what he does is wrong. Someone uses an X-ray device to look at you through the walls of your house? He violates your right not to be looked at, and you have that right because you have rights over your persons analogous to the rights you have over your property and it is because you have these rights that what he does is wrong." (Thomson, 1975)

2.1.2.2 Non Reductionist Conceptualizations

Another school of thought in opposition to reductionism has argued that privacy has conceptual distinctness from other constructs and stands independently on its own. What is interesting is there is a wide diversity of opinion of what makes the concept distinct. All do agree that when privacy is attempted to be reduced something is lost. By

way of example, Inness notes that privacy has been claimed to be composed of the construct liberty and property, yet when examined, a conceptual distinctiveness from liberty and property is found. Privacy claims, according to Inness are conceptually distinct from liberty and property claims as they cohere about intimacy. Claims concerning liberty associated with intimacy might be privacy claims but not all of these privacy claims can be collapsed into liberty. Intimate property claims might be privacy claims but not all property claims are privacy claims (Innes, 1992).

2.1.2.3 Schoeman School

Schoeman created a refinement on the construct of privacy and further elucidated the differences between the reductionists and non reductionists. What Schoeman was attempting to develop was a sharper contrast between Reduction and Non Reduction thought. In this refinement he created a continuum of construct of privacy, by redefining privacy into two distinct camps at opposite polls — One having no common connection which was called his Coherent Thesis (reductionism), and the other having a common connection which later was called his Distinctive Thesis (Non Reductionism).

A reductionist, according to the Schoeman Coherence Thesis would espouse that while all privacy claims are believed to hold similar justifications and thus hold something in common in fact have no coherence as the very privacy claims they espouse are defended with moral principles independent of the concern with privacy. Therefore there are no moral principles distinctive to privacy and the construct holds no coherence. A member of this group would espouse that a distinctive privacy construct

cannot be constructed because it is a diverse and disparate collection of objects that are only superficially or nominally connected.

At the other end of the spectrum is Schoeman's Distinctiveness Thesis. This thesis recognized that there is something special, fundamental, distinctive and coherent about the human moral or social character that is lost in reductionism. It espouses that privacy captures this in a definable construct that is distinguishable from other constructs and defendable on principles distinctive to the construct of privacy – such as an inviolate personality or human dignity, as a key component in structuring the very possibility of diverse social relationships and making possible the deepest kind of love an individual can share or share a role in protecting private life or individual's intimate self.

2.1.2.4 The Coherentist School – Foundationalism v. Coherentism

A second Non Reductionist School has emerged called Coherentism. Coherentists have rejected Schoeman's Distinctive Thesis while agreeing with Schoeman in the rejection of Reductionist thought. They agree with Schoeman that there is something fundamental and distinctive and coherent about the various values that have been called privacy interests. Also agreed upon is the fact that most individuals recognize privacy as a useful concept and that privacy has value as a coherent and fundamental concept. How the Coherentist school differs from the Distinctiveness Thesis is in the epistemology.

Foundationalism is the epistemological basis of the Schoeman Coherence and Distinctive thesis as well as the Reductionist School. Foundationalism is a theory of

knowledge that requires that all logical arguments stem from an objective true which is a basic self justifying belief. The Coherentist school however bases its epistemology in another theory of knowledge known as coherentism. Coherence theories stress the importance of mutual support among a network of emerging beliefs as a criterion of justification.

> "Coherentism may be thought of as analogous to a ship, the hull of which is constructed of many metal panels, none of which float on their own, but which form a floating whole when appropriately connected. No particular panel on a ship can properly be considered foundational: the ship's ability to float arises spontaneously when a sufficient number of panels are appropriately connected." (DeCew, 2002)

Most commonly, this set of beliefs is held by a particular individual; however it is also possible for Coherentist models to range over the beliefs of a group. If we accept that the nodes in a coherent network are "beliefs", then it is entirely feasible to construct a beautifully consistent network of beliefs which nevertheless bears little or no relation to the world it purports to describe. This can result in strong logical arguments with a consistent network of beliefs that support false conclusions (known as the Isolation Objection).The coherence relationship itself is rather harder to pin down, precisely. It may involve logical or probabilistic consistency, inferential connectedness, lack of anomalies, explanatory value, relevance, and so on. These issues have impaired the cohesiveness of this school of privacy because its members hold quite diverse, and sometimes overlapping, views on what it is that is distinctive about privacy and what links diverse privacy claims (DeCew, 2002).

Unlike the field of philosophy, there is no raging debate in the MIS discipline over the epistemological basis of privacy. This ignoring of epistemology and failing to taking an epistemological stand are two reasons why privacy research has been impaired. Epistemology is important to the conceptualization of a construct. Epistemology accounts for differences on the conceptualization of a construct as the epistemology provides the justification for the knowledge and belief that the construct is true. Privacy researchers fail to note the distinctions present in the different epistemologies of privacy which is one of the reasons there is no consensus on the construct of privacy and is a reason why privacy research appears to be a series of unconnected, context specific studies with little generalization outside the context of the study. It is important that an epistemological basis of the study of privacy be specified so that theories can be constructed, understood and results compared between research conducted with differing epistemologies.

This paper adopts the Schoeman Distinctive Thesis and Foundationalism as its epistemological basis.

2.1.3 Philosophical Basis of Privacy: Ontology and Axiology

Ontology has two questions: How do I define and distinguish the object or entity under inquiry? What are the fundamental categories of being? Any ontology must give an account of which words refer to entities, which do not, why, and what categories result. It must provide what are the essential, as opposed to merely

accidental, attributes of a given object. It must provide what constitutes the *Identity*[4] of an object? What are an object's properties what is its relationship to other entities and how are they related to the object itself?

Axiology is the study of value or quality. Axiology includes the study of ethics and aesthetics—philosophical fields that depend crucially on notions of value. Axiology lays the groundwork for these fields, having strong similarity to value theory and meta-ethics. The term was used in the 19th and early 20th centuries, but in recent decades, value theory has tended to replace it in discussions of the nature of value or goodness in general.

Value theory concerns itself with the value of people and things[5] - or the combination of all these. Research suggests both human beings and at least some other sentient organisms can hold values, which express themselves in behavioral dispositions - the predisposition to act by choice in a certain way, when faced with a certain condition or stimulus which permits different responses. The expression of this predisposition ranges from very primitive behavioral routines, to very complex ones which may be difficult to detect or elucidate.

Values are implicitly related to a degree of behavioral freedom or autonomy which goes beyond a conditioned response; as values *steer* or *guide* the organism, on the basis of internally chosen options. Thus, values imply the (conscious) prioritizing of

---

[4] *Identity* here is used in the sense of what makes the object definable and recognizable in terms of qualities and characteristics that distinguish it from other entities.

[5] Value is said to include worth, utility, trading or economic value, moral value, legal value, quantitative or aesthetic value

different behavioral *alternatives* which are perceived to be possible for the living organism. Conversely, value-conflicts can disorient the behaviors of the organism, throwing it out of balance. Values are at the basis of all moral, political and economic behavior.

The ontology of privacy differs depending upon the axiological view of the person offering the ontology. Three values dominate privacy research in philosophy and law. “Privacy promotes individual autonomy, personal growth, and human relations” (Graham, 1987). Lockian privacy emphasizes the value of being an autonomous free agent responsible to others only in cases of necessity or agreement. Under this view, privacy is necessary to insure that individual actions be free from the influence of others. Privacy allows the individual great autonomy and latitude in the choices available to the individual. Kantian privacy looks to the individual constructing his own self. Kantian privacy emphasizes the importance of a space apart from the gaze of others to develop and live life. The final view of privacy, which is a combination of the Kantian and Lockian schools looks to the necessity of privacy to promote relationships.

2.1.3.1 Lockian Privacy

Frequently privacy is discussed in reference to a distinction between public and private.

> “This public private distinction has sometimes been taken to reflect differences between the appropriate scope of government as opposed to self regulation by individuals. It has also been interpreted to differentiate political and domestic spheres of life. These diverse linguistic descriptions capture overlapping yet non

> equivalent concepts. Nevertheless they share the assumption that there is a boundary marking off that which is private from that which is private." (DeCew, 1997)

The Lockian ideal of the politically free man in a minimally regulated society extends the right to privacy as a necessity to protect the individual against intrusions by others. Locke maintained that governmental, societal or individual power should not infringe upon another person's power, liberty or autonomy except upon exceptional circumstances and then the intrusion should be reasonable and limited. The value of this privacy is it provides the means by which individuals may sustain power, liberty and autonomy against potentially overwhelming forces (Nissenbaum, 1998). Lockes' viewpoint is based upon the belief that everyone has an area of their life where they are not responsible to the state for what they do so long as the rule of law is maintained: rights of others are respected. Accountability of the individual toward society should be minimal unless the individual is either a member of society's administration or some special ground exists why the individual cannot please themselves.

Keeping the rights a society holds over a person reasonable and limited, permits societal roles be constructed to allow considerable autonomy to the individual to choose how they live (Benn, 1975). This justification of privacy has been represented as the power in the individual to determine what to reveal and determine how accessible they want to be (Bellotti, 1998). It has also been stated as justification for privacy in public (Nissenbaum, 1998). These views are in opposition to the totalitarian school which holds that in everything that man does, man's individual action in toto has significance

for society at large. As such, man has both a responsibility toward society and accountability to society members that requires all be revealed (Benn, 1975).

2.1.3.2 Lockean Control Based Privacy

To some, privacy "is not simply the absence of information about us in the minds of others; rather it is the control we have over information about ourselves" (Fried, 1968). Alan Westin's influential account of privacy defines it as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). This has been called the control over information of oneself (Parent, 1983). Privacy is defended as a value that accords us the ability to control the access others have to us (Gavison, 1980, and Allen, 1988). It has also been expressed as a right and duty to make some information generally available concerning their relationship and a right and duty to leave unsigned other information because "in society there is the right and duty of partial display" (Goffman, 1971). It been observed that the control of outflow of information may be of strategic or aesthetic value[6] to the person and the control of inflow of information including the initiation of contact (Samarajiva, 1998).

An appeal of this position is it is seen as more morally neutral than the rights, claims and entitlements approach. Control based privacy theories are not without their criticism. One criticism has been that it is vulnerable to counter examples which make

[6] Aesthetic Privacy violations expose things that victims may feel inappropriate to reveal to others. Strategic Privacy violations compromise the victim in the pursuit of his or her interests see Rule, J.B. et al, eds. *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies,* Elsevier, (1980).

the position appear ill considered. Example: a person lost in a forest has lost control over who has control over his information yet in reality he suffers from the fact that he has too much privacy (Shoeman, 1984). The foremost criticism however is that control based privacy claims are vulnerable to examples of threatened losses where privacy has not been lost but there is an issue of control over disclosure (Parent, 1983). Imagine an X-ray device that can look through the walls of a home. You lose control over the disclosure of the activities in the home even if nobody uses the device. You lose control over privacy in your home only if someone uses this device. What this example exposes is control is not a necessary condition for privacy. Control has also been shown not to be a sufficient condition for privacy. You may have complete control over your personal information but chose to give up your privacy by freely divulging the information. Because you freely disclose this information it makes it difficult to describe it as a loss of privacy on a control based definition of privacy. In this way control is not sufficient condition for privacy (Austin, 2003). In the circumstances where individuals control the outflow of information and initiation of contact subject to some objective rule additional issues of knowing how they and their information is accessible, by whom and when becomes apparent. Control based privacy offers little explanation on why some information should be private while other information is not private except through an explanation based upon social conventions (Parent, 1983). With control based privacy, requirements to control the access easily and intuitively, feedback of who has access to what and personal control, trust development all become issues (Bellotti, 1998). Control based privacy cannot answer the question over what

information we should have control. Further, a definition of privacy as control over personal information depends upon our acceptance of an entitlement to this information, fail to justify an entitlement to privacy and in many cases presuppose an entitlement (Austin, 2003).

2.1.3.3 Kantian Privacy

Privacy can be constructed through the Kantian theory of the morally autonomous man who acts on principles he accepts as rational (Benn, 1975). Our society and culture value people who are independent minded. Characteristics of this type include that they step out and set themselves apart from the masses. Often found to be leaders including leaders of nations, they are champions to causes and blaze new horizons. This type of person is an innovator, inventor and possess the independent mind and inner strength and courage to act upon their principles and to resist the pressure to conform to the rest. These types of person doesnot just appear; they need to be nurtured.

With out development people in general will tend to adopt the views held by others without question. To avoid this, people need to be able to act freely and develop their own character. Former Senator Hubert Humphrey wrote, “We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to all our actions will be altered and our very character will change” (Long, 1967). People need to be spontaneous and not hold back input. Senator Edward V. Long observed, “because of the diligent accumulation of facts about each of us, it is difficult to speak or act today without wondering if the if the words or actions

will appear ‘on the record’. ”(Long, 1967). People need freedom to develop their own principles. They need a sanctuary and a retreat to be their selves and be placed outside the gaze of society while they nurture themselves and develop. People cannot develop into autonomous beings unless they are allowed to practice independent judgment. Privacy must be afforded to the individual so that the individual develops personal autonomy necessary to develop these traits. This is described in the literature as private psychological space (Zweig, 2002), or as a condition necessary for the construction of self (Reiman, 1976), construct their identity (Goffman, 1956), Clark, 1994) intellectual privacy (Cohen, 2003) emotional space.

2.1.3.4 Kantian State of limited access

The ability to control access differs from the ability to control information. This appears to have its basis in Kantian philosophy. The ability to control access creates a zone of non interference or a zone of limited access to private information. This is often used when information has been provided in the context of one relationship and another seeks access to that information.[7] It can also mean a zone of limited access to the person for the purpose of limiting the gathering of personal information (Innes, 1992). During the infancy of the privacy conceptualization, Brandeis and Warren proposed privacy as a right to be left alone. They championed that an individual’s private life should be free from the gaze of the public and others and that same individual had the right to determine the conditions under which access to his person could be obtained

[7] An example of this is an insurance company seeking access to the medical information provided by the patient to the doctor for purpose of diagnosis.

(Warren and Brandeis, no year). One problem with this conception of privacy is there are innumerable ways to leave someone alone that have nothing to do with privacy (Parent, 1983). A second problem related to the concept of liberty. Brandeis and Warren's assertion was based upon their belief that an individual possessed the liberty to enjoy life and property. Liberty is the absence of external constraints or coercion on the individual. The right of liberty embraces the right of persons to make important choices about their lives but this was distinguishable from a right of privacy which condemned the unwarranted acquisition of personal knowledge. Liberty constructs placed constraints and restrictions on the individual control over information and did not create a zone of non interference. A need for more conceptual clarity was apparent. Later definitions attempt to avoid this by stating that privacy is a condition in which others are deprived of access to you (Reiman, 1976) or to self (Garrett, 1974, and Gavison, 1980). When privacy is defined in operational terms, this capability is often coupled with an ability to control access (Bellotti, 1996) with this control over access enhancing personal expression and choice (Shoeman, 1984) or some combination of these (DeCew, 1997).

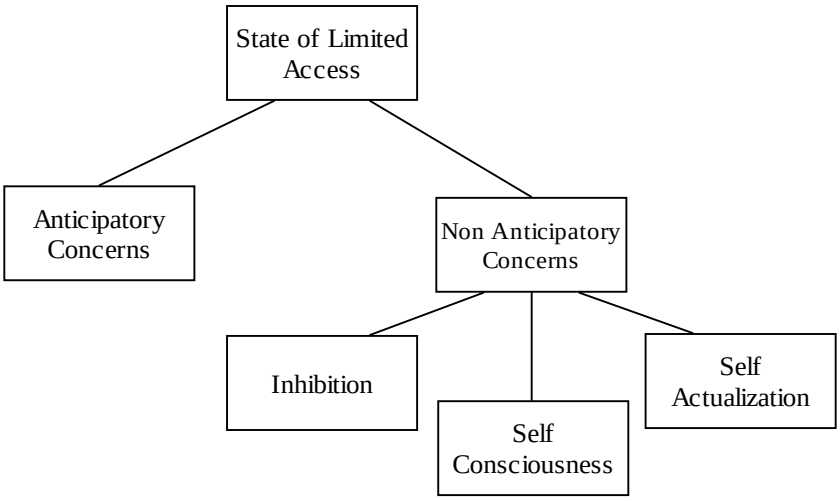

Figure 5 Taxonomy of Limited Access

2.1.3.4.1 Anticipatory Concerns – Limited Access

There are many values that are supported by the creation of a zone of limited access. Anticipatory concerns have been expressed over the possible abuse of power by a corrupt government which gathers information to weed out undesirables (political or religious) and dissidents. In private relations, anticipatory concerns include certain information about ourselves if known to others it would leave us vulnerable to harassment, discrimination, identity theft and other types of abuse (Information and Privacy Commissioner of Ontario, no year).

Non anticipatory concerns – Inhibition

Zones of no access support other values, these of a non anticipatory nature. Where there is a zone of no access, individuals have fewer inhibitions and do what they would not do without it because of a lack of fear of an unpleasant or hostile reaction from others" (Gavison, 1980). The types of expression affected include both the

expression of emotion and expression of action. The reason we value freedom from physical access is that it insulates us from "the inhibitive effects that arise from close physical proximity with another individual" (Gavison, 1980). It is not simply that we are identified by others that creates the loss of privacy, but the fact that the identification subjects us to the kind of inhibiting standards of public norms and justification that underlie our concerns regarding being subject to observation and the public gaze (Austin, 2003). Inhibitions will occur even should the anticipated reaction would stop short of harassment and discrimination. In this sense the zone protects our ability to act and think in unpopular ways; as well as it protects individuality understood in terms of our ability to be eccentric.[8]

2.1.3.4.2 Non-anticipatory Concerns - Self Consciousness

While there are many acceptable ways to present our thoughts in public, there are some expressions that are not acceptable (such as the expression of strong emotions). All humans suffer from self consciousness. Self consciousness is affected by the zone of limited access and can be promoted or inhibited. Some aspects of our inner lives, our thoughts, emotions and actions, simply cannot exist if exposed to the public gaze even if these are in some sense wholly conventional. This arises under the circumstance where individuality arises not from the need to be different but the need to express ourselves.

[8] See also Bloustein, "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass."

(This) awareness of how one appears from outside is a constant of human life, sometimes burdensome, sometimes an indispensable resource. But there are aspects of life which require that we be free of it, in order that we may live and react entirely from the inside. They include sexual life in its most unconstrained form and the more extreme aspects of emotional life – fundamental anxieties about oneself, fear of death, personal rage, remorse, and grief. . . .The public gaze is inhibiting because, except for infants and psychopaths, it brings into effect expressive constraints and requirements of self-presentation that are strongly incompatible with the natural expression of strong or intimate feeling. And it presents us with a demand to justify ourselves before others that we cannot meet for those things that we cannot put a good face on (Nagel, 1998).

Non anticipatory concerns - Self actualization

Some authors recognize a right to become, to be and to remain a person (Reiman, 1976). A pressure to conform leads to conformity and decreases in diversity but it also leads to a condition where self cannot be actualized. People require some respite from the public gaze to collect our self and form our self through the development and affirmation of our own ideas even should they become the same as our peers. This zone of no access enables us to become distinct individuals to live and remain individual.

The Condition	Value of the Zone of Limited Access
Privacy → Lower Inhibition	Freedom to do and experiment
Privacy → Decreases Self Consciousness	Freedom to express thought, emotion and act
Privacy → Increases self actualization	Freedom to be different, be non conforming, to develop self, to remain self

Table 1 Zones of Limited Access

Problems with a zone of limited access position surface when access is examined as physical proximity as non privacy concepts such as personal property, solitude and peace surface to describe what is at stake by limiting access. If access is described as acquisition of personal knowledge it becomes evident that the limitations of cognitive knowledge are not privacy but are safeguards of privacy. By way of example: A taps B's phone and overhears conversations of an intimate nature. Official constraints are placed on A's activities where A must obtain permission from a judge before listening in on B (Parent, 1983). Access definitions leave open the question of whether privacy is a desirable state and how valuable it is in relation to other things. Additionally access definitions have the advantage of allowing you to separate the question of what if privacy was lost from the question whether a right of privacy has been infringed or violated (Shoeman, 1984).

2.1.3.5 Lockian and Kantian Privacy Combined: Promoting Relationships

Privacy insures autonomy of the individual to be independent it also ensures that individuals form and develop desired relationships of his/her choice.

In forming of a relationship we ask a series of questions: Do I want to consider a relationship which means what is my attitude toward this relater and relationship, what are its benefits and detriments? Is this a desired relationship, is this relationship appropriate for me. If the decision is made to pursue the relationship questions of what should be the character (type) of the relationship and how to develop the relationship follow. These considerations determine how to construct the relationship including the choice and control over the timing of release of information, the nature of information released and to whom is information released and how the relationship is continued in the future. All these decisions require autonomy.

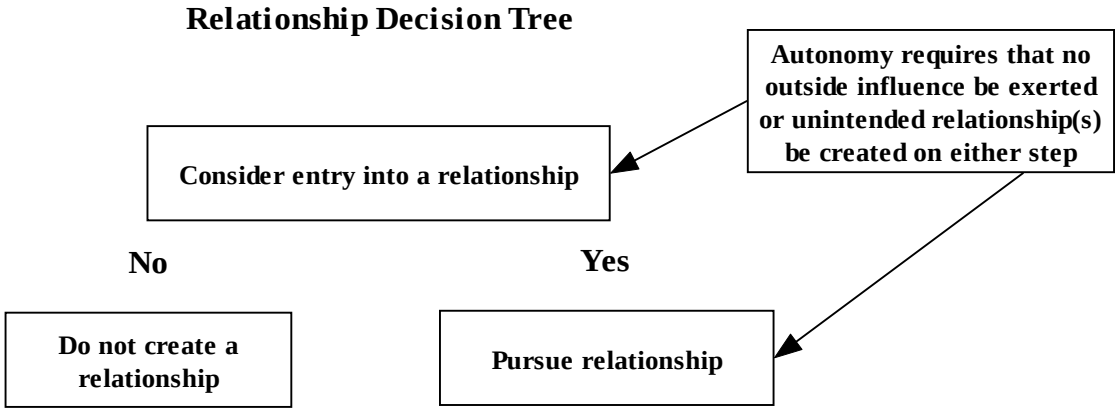

Figure 6 Relationship Decision Tree

2.1.3.5.1 What is autonomy?

Autonomy is the freedom from being manipulated or dominated wholly by others (Westin, 1967). Privacy provides the structure to avoid this manipulation and domination and ensures the autonomous choice of the individual to pursue relationships including the choice of how to construct the chosen relationship[9]. Relationships created with the individual maintaining control over the what, when and who receive the information about them protects the individual from being demeaned, embarrassed, and even disempowerment or fear (Nissenbaum, 1998). Thus it is necessary that when we initially consider a relationship that our attitude toward another relater/relationship and what that relater/relationship may do from us be free from the manipulation and domination of others. It is a form of respect for our potential capacity to develop relationships (Innes, 1992).

2.1.3.5.2 Autonomy while considering entering the relationship

Having the ability to consider both your attitude toward another and what a relationship/relater will do for you implies that a voluntary choice exists in the individual to pursue and shape relationships. Autonomy requires the ability to choose to pursue or not a relationship (Nissenbaum, 1998). A real opportunity to pursue the chosen opportunity must be free from another's interference for autonomy to exist. The capture of private information in public or the use of non private information found in the public domain that enables intrusion into ones privacy causes the loss of this

[9] Autonomy differs depending on the axiology. Locke would see the individual having the requisite privacy to ensure the being live as a free being in a social setting, while Kant would see autonomy ensuring the requisite freedom to become the person desired.

autonomy because of the influences capable of being placed upon individual that interfere with this choice. This exists as a result of the inability to insulate self from monitoring by third parties and the aggregation and use of stored information. This part of autonomy flows from the philosophy of Locke.

Third party relaters effect the formation of these relationships through both the influence over the individual's attitude and on the assessment made on the relationship/relater. The third party colors the attitude and the assessment made by the individual effectively interfering with their autonomous choice. This is in derogation of the potential capacity all individuals hold to form relationships.

The third party also affects the choice to pursue. When information is captured and aggregated, relations are shaped based on captured information. With no capture of public information the individual would not consider highly his or her actions in public. The entire focus would be on the relationship pursed by the individual. With public attention the individual must consider the detection and capture of their public information both private and non private. They must consider what relationship could form in addition to the relationship pursued. Individuals will be influenced to adopt behaviors appropriate for that unintended relationship as well as the one initially pursued. In some cases this mediation may not permit a relationship to form or may even impede relationship formation as the information needed to form the relationship will not be disclosed. It may move relationship in a direction not desired by the individual as the individual will make compensating changes in his intended disclosure

to accommodate the potential capture. Unless its scope and reach is limited this rather than the individual, can become the mediator of relationships formed and not formed. After the decision to enter a relationship, the autonomous control over information enables the construction of relationships

Relationships are constructed on information, in particular on information shared between the relater and the relatee. The relater's right to control information and their capacity to share information are key aspects of personal autonomy (Rachels, 2006) of which privacy supports (Nissenbaum, 1998). Information appropriate in the context of one relationship may not be appropriate in the context of another relationship (Shoeman, 1984). This same ability to control information enables the individual to present only relevant and appropriate information needed for the relationship and keeps other information private. Having the power to share information discriminately also enables people to define the nature and degree of the relationship (Rachels, 2006). Privacy empowers the individual to have a choice over what information to share, when and to whom (Rachels, 2006). Autonomous individuals can provide nothing or the entire portfolio of information. They can provide the information now, never or at some time in the future. They can provide the information to no one, to a designated person or to everyone. This part of autonomy flows from Kantian philosophy.

Despite the background in Lockean and Kantian philosophy, the importance of privacy with respect to human relations has an additional variety of emphasis and focus despite the fact that each recognizes to varying degrees the importance of autonomy and a sanctuary for action. The following is not an exhaustive rendering of these

writings but provides the general scope and breadth of the value of privacy as it concerns relationships.

2.1.3.5.3 Rachels

Rachels sees privacy as important because it is necessary to maintain the variety of social relationships that we want to have (Rachels, 2006). Differing behavior patterns define different relationships. There are differing patterns of behavior when relationship type differs. People vary behavior with people due to the different social relationships we have with them. Why we value privacy is the fact that different relationships are marked and constituted by differing degrees of sharing information. Our ability to control who has access to us, who knows what about us, allows us to maintain a variety of relationships with other people that we want to have (Rachels, 2006). This ability is obtained by our ability to separate our associations with others. Separation allows us to behave in a way appropriate to the sort of relationship we have with them without violating our sense of how it is appropriate to behave with and in the presence of others we have a different relationship.

2.1.3.5.4 Fried

Fried wrote on the "Commodity Theory" of intimacy. Fried's intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone" (Fried, 1968). He postulated that close relationships "involve the voluntary and spontaneous relinquishment of something between friend and friend, lover and lover. The title to

information about oneself and protected by privacy provides the necessary something to the relationship.

"Privacy is the necessary context for relationships which we would hardly be human if we had to do without - the relationships of love friendship or trust" (Fried, 1970). The sharing of one's actions, beliefs and emotions is intimacy when that information is not shared with everyone and it is accompanied by a right to not share the information in the first place (Fried, 1970). This operates both as a signal of intimacy as well as constitutes intimacy.

2.1.3.5.5 Reiman

Reiman finds that privacy protects the individual's interest in becoming, being and remaining a person (Reiman, 1976). Right of privacy is a two fold process. The initial process confers the concept of self and conveys to the person exclusive moral rights in their body that permits a person to view his body, thoughts and existence as his own. .The second part of the process confirms and demonstrates respect for developed persons by conferring the right to the individual to control when and by whom the body is experienced and reaffirming that right through the demonstration for the respect of people.

Reiman makes the point that privacy plays a vital role in the creation and maintenance of self. The elimination of privacy essentially results in the destruction of self. Reinman noted that Goffman maintained that the goal of the "total institution" (an asylum) is "the mortification of the self" (Goffman, 1957) and to accomplish this mortification of the individual's self the total depravation of privacy is an essential

ingredient. In the “total institution,” mortification is accomplished through a variety of means. One is by way of information collected about the inmate and made available to the staff and others. From this collected information, discredible facts that are ordinarily concealed can be learned. Also others can also observe these facts directly as being placed in the institution alone are a discredible fact. Inside the institution the lack of privacy is even more evident as the resident is exposed physically, never alone always in the sight of someone. Rei,man concludes that social practices that penetrate the private reserve of individuals (Goffman, 1957) and kill the self of the person suggest that privacy is essential to the creation and maintenance of self (Reiman, 1976).

To have moral ownership of the body requires the right to do with the body as you wish. It also requires the right to control when and by whom the body is experienced. This requires that you have both the power to act and awareness of that power to act. You also need the ability to withhold the awareness you and your actions from others.

This ownership is appropriated actively and cognitively. Something is mine because I have the power to use it or dispose of it. Active appropriation is having the power to use and dispose of as you see fit.

Cognitive appropriation is the right to control when and by whom the body is experienced. Cognitive appropriation enables the individual to know what I know is my knowledge as well as know what I experience is my experience and not the experience of another. To have control over the cognitive apparition requires that individual have control over whether or not his physical existence becomes part of someone else’s

experience. This requires the individual be treated as entitled to determine by whom and when his concrete reality is experienced. (This applies to both thoughts and actions of the individual)

Self is that part of the human that regards his existence, body and his thoughts as his own. Self is not created from some “inborn seed”. Rather, Reinman sees self created through a social ritual and the social interaction between society and the individual (Reiman, 1976). Through this ritual an individual’s moral title to existence is conferred through the social recognition and communication to the individual that his life is his to do with as he or she chooses and through the conferring to the individual the right of active appropriation over his body. An individual must recognize his capacity to shape his destiny by his choices. He must recognize that he has an exclusive moral right to shape his destiny. After conveying to the individual that his body is a body in which he has some exclusive moral right society subsequently confirms and demonstrates respect for the personhood of already developed persons by conferring the right to the individual to control when and by whom the body is experienced and reaffirming that right through the demonstration for the respect of people.

2.1.3.5.6 Benn

For Benn, the right to privacy stems from this respect for persons as choosers. “Every man who desires that he himself not to be an object of scrutiny has a reasonable, prima facie case of immunity” (Benn, 1975). In order for this to be upheld it must have as its basis either an intimate connection between one’s self and one’s body, through

cultural norms or be required to ensure the character of life and ideals of persons (Benn, 1975).

A person through their attempts to steer themselves through the world through their adapting for changes to their life brought about by the world or through their correcting for mistakes he or she makes is a chooser in actuality or potentially. The right to privacy stems from this respect for persons as choosers. “To respect someone as a person is to concede that one ought to take account of the way his enterprise might be affected by one’s own decisions” (Benn, 1975).

All personal relationships need some freedom from interference. Specifically alluding to Locke, Benn states that the average individuals are subject to reasonable and legally safeguarded limits to the power of others and the requirements of social roles which leave considerable breadth and choice of how he lives (Benn, 1975). Specifically citing Kant, Benn states that individuals should remain independently minded and their actions governed by their own principles. We are only free to be ourselves with in an area that observers can be excluded. In order to ensure this there is a need for a sanctuary in order to drop the mask and project the person’s real nature and not the nature that projects the values of peers we adopt to become acceptable to others (Benn, 1975). This sanctuary enables us to become independent in mind. Covert observation and unwanted overt observation deny this respect because they transform the actual conditions in which the person chooses and acts and make it impossible to act in the way the planned or choose in a way he thinks he is choosing (Benn, 1975).

Inness

2.1.3.5.7 Inness

Inness speaks of the need for relationships. Her work is a focus on intimate relationships which she defines as relationships that emanate from “love, caring and like” (Inness, 1992). Her work implicitly adopts the philosophy of Locke that men should be autonomous and free from the influences of others when persons are seeking to form the relationship. Her work implicitly adopts Kant as well noting the need for a sanctuary within which to conduct this activity.

According to Inness, intimate relationships do not result solely from the transfer of information (Inness, 1992). What marks them as intimate is not the behavioral content but the role the activity plays in the life of the individual -they emanate from love, caring and like. Intimate information is restricted information and constitutive of a close relationship. Certain activities are inherently intimate and are protected by constitutional privacy law.[10] Inness cites the case of *Roberts v. United States Jaycees*, for the proposition stated by the court that intimate activities embody the fact that we all depend on the "emotional enrichment of close ties with others."[11] She also cites with approval the dissenting opinion to *Bowers v. Hardwick*, in which Justice Blackmun suggests that intimate activities regulate the nature of an agent's personal associations with others (Bowers v. Hardwick). She concludes that these activities regulate our

[10] See Carey v. Population Services International, 431 U.S. 678,685 (1977) for a list of the cases which outline the reach of constitutional privacy claims.

[11] Note that Roberts v. United States Jaycees contains an explicit warning against limiting the scope of privacy to the family.

relationships with others by regulating our emotional ties, especially the ties of love, liking and care

Given the character of this information, privacy should ensure that the agent has control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions. Since matters draw their meaning and value from the agent's love, liking, or care according to the role they play for the agent, the construction of intimacy lies on the agent's shoulders. Therefore, privacy claims are claims to possess autonomy with respect to our expression of love, liking, and care.

Inness sees privacy as valuable for three reasons: First, it promotes the creation of close, intimate relationships. Secondly privacy's value stems from our respect for persons as rational choosers. Finally, privacy is valuable because it acknowledges our respect for persons as autonomous beings with the capacity to love, care and like

To ensure the control over decisions regarding intimate matters remains in the individual society must protect that the choice is that of the individual and not another. To accomplish this a zone of privacy must be constructed and respected in which society neither uses them nor fails to treat them as ends in themselves with respect to their intimate lives. Adopting Onora O'Neill's "there are two separate aspects to treating others as persons: the maxim must not use them (negatively) as mere means, but must also (positively) treat them as ends in themselves" (O’Neill, no year). This requires that the freedom of action of the individual must be protected. These are the reasons behind

the cases of *Roe v. Wade* the agent's privacy claim protected her freedom to have an abortion. In *Griswold v. Connecticut,* the agent's privacy claim protected her freedom to use contraceptives. Secondly a duty of noninterference or nonparticipation in the intimate life of the agent on the part of others must exist. This is most evident in the privacy restrictions concerning access, restrictions commonly embodied in tort privacy law.

This zone must have these characteristics a zone in which she possesses autonomy of action and a zone that gives rise to duties of noninterference from external parties. To satisfy the first requirement, the agent requires autonomy with respect to the actions she takes to embody her love, liking, and care; society must not use the agent in such a way that she lacks the autonomy of action to express these emotions. To satisfy the second requirement, the agent requires a zone to which she can regulate the access of others (including informational access); society must not use the agent in such a way that she is rendered incapable of understanding herself as a source of intimacy.

Following is a table which compares these theories.

Author	**Privacies Importance**		**Autonomy**
Rachels	Necessary to Maintain Desired Social Relationships	The individual must have an ability to separate associations with others	Sanctuary
Fried	Provides the necessary something to the relationship	The individual must be able to choose when to share private information	We need an ability to control who has access to us, who knows what about us and allows us to maintain a variety of relationships with other people that we want to have

Reiman	Protects individual's interest in becoming, being and remaining a person and plays a vital role in the creation and maintenance of self.. Privacy is a demonstration of respect toward people.	The individual has a right to control when and by whom the body is experienced	The individual has the ability to conceal information that is private
Benn	Protects the persons right to choose	Average individuals are subject to reasonable and legally safeguarded limits on the power of others and the requirements of social roles which leave considerable breadth and choice of how he lives	Until the right is relinquished no one has a right to access or information about the person
Inness	Privacy first promotes the creation of close, intimate relationships. Secondly privacy's value stems from our respect for persons as rational choosers. Finally, privacy is valuable because it acknowledges our respect for persons as autonomous beings with the capacity to love, care and like—in other words, persons with the potential to freely develop close relationships. Society must protect that the choice is that of the individual and not another	A zone must be provided in which a person possesses autonomy of any decision or action taken that embodies love, like and caring. Society must not use the agent in such a way that she lacks the autonomy of action to express these emotions. Society must respect the individual and neither use nor fail to treat them as ends in themselves with respect to their intimate lives.	We are only free to be ourselves with in an area that observers can be excluded. In order to ensure this there is a need for a sanctuary

Table 2 Summary of Philosophical Theories of Privacy that Combines the Lockian (control) and Kantian (access) Perspectives

2.2 Philosophy and Rights, Claims and Entitlements

This section shall demonstrate that rights, claims and entitlements embody values and determine behavior. It will be further demonstrated that privacy rights, claims and entitlements vary in terms of control and access depending upon the axiological basis of the privacy protection sought.

2.2.1 Rights, claims and entitlements determine behavior

Rights, claims and entitlements determine behavior by enabling and constraining conduct. The traditional conception of rights occurs when some legal or other institutional mechanism is there to enforce them (James, 2003) such as a court or regulatory body. Rights however can exist independent of these institutions.

Hohfeld defined seven normative positions for the purpose of analyzing rights (James, 2003). Hohfeld positions include the following (Hohfeld, 1964):

- X holds a claim that Y performs an act if and only if Y holds a duty toward X to perform act A.
- X holds no claim that Y perform act A if and only if Y holds a privilege against X not to perform act A
- Y holds a privilege against X not to perform act A if and only if Y holds no duty toward X to perform act A
- X holds a power if X holds the ability to create or remove some claim, duty, or privilege (a claim, duty or privilege which might be held by X himself or by someone else
- X holds a power to create some specific duty, claim or privilege for Y if and only if Y holds a liability to have that specific duty claim or privilege created for Y by X
- X holds a right whenever X holds a claim, privilege, power, immunity, liability, or a cluster of the above and if infringed, un enforced or not properly respected X would hold a claim to some form of apology or recompense.

- X holds a disability to create some specific duty, claim or privilege for Y if and only if Y holds an immunity from having that specific duty, claim or privilege created for Y by X

While Hohfeld confined his position to legal rights, this analysis has been found to apply equally well to moral relationship structures (Kramer, 1998). Hohfeld's Normative Position is composed of seven positions: claims, duties, privileges, powers and liabilities, disabilities and immunities (Hohfeld, 1964). A claim exists when a duty is owed to perform an act for the holder of the claim. When no duty is owed to perform an act, a privilege exists. A power enables the holder to create, remove some claim, duty or privilege. The person subject to a power has a liability. Immunity disables a power held by another (Hohfeld, 1964). The holder of immunity has the right to be free of claims, duties and privileges being created or removed. A right exists when a person's behavior is constrained in distinctive ways (Rainbolt, no year). Therefore a person holds a right whenever they hold a claim, privilege, power, immunity a liability or some cluster involving several of one of more of these and if the position were infringed, not enforced or not respected that person would be entitled to some apology or recompense (Cruft, 2004). Rights of others determine constraints on our actions (Nozick, 1974). Conversely our rights determine constraints on another's actions as well.

A system of rights enables the specification of expected behavior of individuals, organizations and government to direct action toward a desired state. In essence rights specify a coordinated model of behavior through the specification of relationships, rules

and actions. When we look at rights in congregate, these rights determine the roles expected to be assumed.

What protections of privacy an entity possesses depends upon the rights, claims and entitlements assigned to that type of privacy. These specify what data and information is private and what is not private as well as how one in possession of the private data can utilize the data. They identify who is entitled to the right and the conditions under which the right can or cannot be exercised by its holder.

2.2.2 Rights, Claims and Entitlements Embody Values That Define Conduct

Right emanate from many value-based sources. The Natural Law tradition holds that some rights are pre legal moral requirements whose existence gives people a reason to introduce laws and enforcement mechanisms that were previously absent (Cruft, 2004). Societal norms are also a source of rights. Norms embody values that a society holds important. Norms can emanate from society, a stratum in society or be conventions of a locale or a group of individuals and agreements are sources of specification of conduct. Norms are often obeyed despite a lack of legal sanction for their violation (Posner, 1998). Private ordering[12] is the name given to the private groups often trade groups like diamond merchants and cattlemen who exist to promote values and rights important to that group. Their efforts are directed toward members only. The enforcement is limited and directed only toward its members and include emotional

[12] *Private ordering* is the process of setting up of social norms by parties involved in the regulated activity (in some manner), and not by the State. *Private Ordering* aims to achieve public goals, such as efficiency, enhancing the market, and protecting rights. *Private Ordering* must adhere to the principle of voluntary acceptance. It can be imposed only on those who have agreed to subordinate his or her activity thereto. See www.isoc.org.il/hasdara/private_ordering.doc accessed March 29, 2005.

appeals, and threats of ridicule, coercion, ostracism or disapproval for those members who value to abide by the rules and values of the group (Posner, 1998). A system of laws and regulations embody values and specify rights.[13] Legislatures enact laws that contain rights that reflect societal values. Agreements whether made voluntary or involuntary are a final source of rights that are value based.

Rights enable values to be specified into codes of conduct. Rights embody the conventions, values and principles of a society and specify behavior consistent with its conventions, values and principles through its laws, norms, private ordering or agreements.

2.2.3 Privacy rights, claims and entitlements are defined by their ontological and axiological basis

Privacy rights are ordained through law, societal norm and/or protected it in agreements to provide for a variety of desired values. Some of values of privacy include to provide for the respect of persons (Benn, 1975), to establish relationships (Rachels, 1975) for the development of varied and meaningful interpersonal relationships (Fried, 1970) Because privacy rights have been touted as necessary for the creation of self, protecting a person's interest in becoming, being and remaining a person (Reiman, 1976) these philosophical principles have compelled law to create zones of privacy that shield from the gaze of others the use of birth control or decisions to abort a pregnancy, membership in certain groups (NAACP v. Alabama), restrict third party access to library records and video rentals (Video Privacy Act) or protect peoples homes, papers

and conversations from outside access (Katz v. U.S.). Others types of rights in privacy have been created in law to protect “special interests” (Scanlon, 1975) such as in the enforcement of trade secrets while others defend it as a broader concept required for human dignity (Bloustein, 1962).

Privacy regiments diverse aspects of every day life through the construction of a complex web of norms and laws that reflect and ensure the values of privacy. Through this regimentation privacy dictates which data is produced (Agre, 1998). Through laws and norms that reflect privacy’s value, the appropriate data and information and use of that data and information a given relationship is specified (Schoeman, 1984). Additionally norms and law arbitrate how, when and what data and information can be possessed and used and by whom. In effect values specify the type of norms and laws necessary to ensure the value is realized. Norms and Laws specify the behavioral roles necessary for privacy to be obtained. Because there are many purposes for privacy, there are many specifications in laws and norms necessary to ensure the purposes are met.

The norms, laws and agreements that specify rights become control mechanisms that structure our behavior through the sanctioning of appropriate behavior and the prohibition of inappropriate behavior for the varied transactions, situations and relationships in which people engage. Through their structures they create roles that embody appropriate behavior, obligations owed and rights. These structures are the building blocks that orders society at all levels of societal interaction and dictates the behavior expected of the individuals within. One aspect of a role created by a law, norm

or agreement is the specification of the appropriate behavior, rights and obligations owed toward information. This includes what is appropriate information to access or possess, who controls access to information and once accessed who controls its use, once information is obtained how can it be used, how much of it can be used, when can it be used and who can use it (Schoeman, 1984). One such ordering is the determination of what information, how much information is fitting and proper and what information is appropriate or inappropriate.

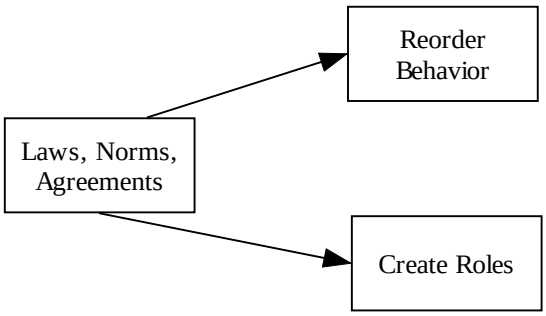

Figure 7 What Laws, Norms and Agreements Do

In each of the above, the privacy rights, claims and entitlements of the entities vary greatly by the axiological basis of the privacy sought. Each type of privacy has a distinct ontology of control and access. Thus ontology specifies privacy rights through the specification of the control and access over data and information that an entity possesses. Therefore two conclusions can be made. First as each distinct type of privacy will bear a unique signature in terms of rights, claims and entitlements that any entity enjoys. Second: As privacy changes, signature of control and access should also change.

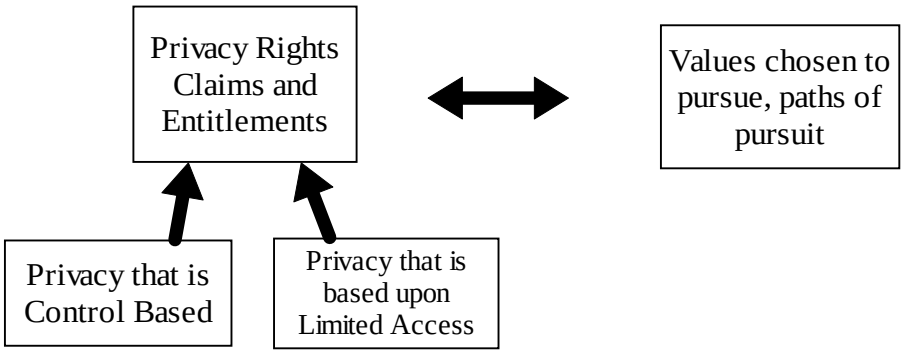

Figure 8 Relationships between Rights, Control and Limited Access

2.3 Law and Privacy

This section will focus on the legal basis of privacy. It includes a discussion of how rigor is accomplished in legal research, the purpose and nature of law and a case study of privacy in American law.

Like philosophy, law is a social science constantly seeking. What it seeks is different from philosophy. Where philosophy seeks the truth, law seeks to implement the truth. In many ways law is pragmatic while philosophy is theoretical. Law is concerned with the coordination, motivation and direction of human and non human action through use of value based rights. Law implements privacy through the establishment of specifications of behavior to ensure information that is private remains private. Law uses control and access to information to implement rights and define roles so privacy can be ensured. A history of the law of privacy is provided that will demonstrate that the topics of privacy at law are broad, covering a wide variety of information under an equally broad situational area.

2.3.1 Purpose and Nature of Law

The nature of law is to find an optimal solution to a wicked problem. The purpose of law is to coordinate, motivate and direct human and nonhuman action through use of value based laws. These laws create rights which define roles. A set of roles creates a relationship. All human relations involve role expectations. Both people and entities structure and evaluate relations according to an understanding of what is expected from the respective roles (Benn, 1984).

Law must be a reflection of society, including its politics, technological state and its social fabric and account for the fact that all are interactive with each other (Lessig and Lemley, no year). Law is not neutral and frequently advances the goals of society's ruling members. The question of law being good or bad is often debated. Whether law is good or bad is often a subjective experience depending on the law's impact. Good law supports goals and aspirations of those advancing it as good while bad law has negative impacts on the debater's goals and aspirations.

Law is not limited to statutes and case law - the formal law, but includes social norms and agreements made between individuals. Laws, norms and agreements are interactive with each other and in a healthy society each supports one another. Frequently they are the formal embodiment of normative rules that are the socially constructed laws of society.

Formal laws can act as a supplement to norms enforcing fundamental social norms (Posner, 1998). Normally, laws are but a reflection of the norms of the society it serves (Posner, 1998) but in some instances law shapes new norms. Agreements enable

the harnessing of law and norms to accomplish societal desired tasks. To a limited extent agreements can modify laws and norms but basic rights insured by law and norms are not capable of change by agreement.

Law is a system based on moral principles, scripted roles and sacred symbols (Edelman and Suchman, 1997). Law, whether it be formal law, norms or agreement, expresses society's values, its moral principles and sacred symbols through the rights defined. These defined rights in turn define roles. Through the definition of rights and obligations, roles are established and protected for every individual, group and organization with in society as well as for government and its relationship with individuals and entities within its control.

Law constructs and legitimates organizations and organizational forms that are socially acceptable or needed.[14] Law determines what types of organizations come into existence. It provides the qualifications and ground rules for organizational forms (Meyer, Boli and Thomas, 1987, and Krasner, 1988) and defines what type of activity and how that activity can be conducted.

Law provides a model of and for organizational life, defining roles for organizational actors and meaning for organizational events and imbuing those roles and meanings with positive or negative moral valence (Geertz, 1983). Law provides the identities and capacities of organizational actors, both empowering and emasculating classes of organizational actors. Organizations adopt these structures and practices for

[14] Typical organizations in the western world would include the corporation, partnership and limited partnership to name a few.

the following reasons. One reason is the socio-legal environment nominates those structures and practices as proper, responsible, legitimate and natural. Organizations look to the law for assurance as to which actions to take and avoid as well as for normative and cognitive guidance. The second reason is their adoption enables them to pursue goals more efficiently and effectively provides them either an advantage or shielding them from punishment.

In one way laws are premised upon the view they seek to minimize harm that society seeks to avoid (Schauer, 2000). Laws announce and provide a record of what is acceptable or not acceptable behavior. Through laws, societal norms find increased respect and compliance through engineering behavior through punishment by legal sanctions when behavior exceeds what is expected.

Rewards are ensconced in law to direct individual and corporate behaviors in ways that improve society. Sanctions are enacted to direct behavior away from other non effective behaviors especially when those behaviors reflect substantial social costs (Posner, 1998).

Economics has advocated the construction of efficient rules to minimize transaction costs in the market thus maximizing the scope of markets over organizational and regulatory hierarchies (Coarse, no year). Transaction cost analysis states that organizations are devices for efficiently governing economic relations when markets fail due to uncertainty, bounded rationality, monopoly, and opportunism. Legal rules may provide for the more effective functioning of society through rights and immunities that enhance or impede the efficiency of individual or organizational

governance mechanisms and affect their desirability relative to markets. The result is that legal rules may provide a substantial influence on individuals and organizations by creating an encompassing framework of basic property rights that includes both structure and substance (Masten, 1990, and Williamson, 1991).

Constitutive law not only defines the basic blocks of organizational forms it also establishes the rules of individual-organizational relations, inter-organizational relations and organizational-governmental relations. Through this structure of categories and definitions relationships can be understood, entered into and manipulated acceptably from this accepted set of routines. It establishes the background understanding that frames social discourse. This provides the fundamental definitional building block for the use of law to meet goals of individuals and organizations and empowers by providing a tool kit that can be drawn upon in their interaction such as contract, tort, and bankruptcy law.

The formal law of privacy, that is the law codified in forms of laws and case decisions establishes and informs the citizenry of the parameters of what is private while coordinating, motivating and directing the roles of the individual, the organizations it enables and creates and society as a whole (Schauer, 2000). Law is a tool that serves society but it is an inexact science; it is constantly evolving in its search to find an optimal solution in an ever changing environment where not only the environment changes but the perceived needs and desires of those within also change (Lessig and Dershowitz, no year).

2.3.2 Rigor in Legal Research

Legal research is marked by some very different approaches, many of which are in their infancy. The following will provide background on legal research. Legal research is accomplished in three schools, doctrinarism, empiricism and grounded theory. Doctrinarism has its purposes in opposition to that of the typical academic faculty member. Despite recent interest in empirical legal research is in its infancy. Finally, legal research in grounded theory will be discussed. While this methodology has been practiced for many years, it is not practiced widely. Legal research using grounded theory similar to research done in academia, adopts the same principles and methodologies utilized in the Information Science field

2.3.2.1 Doctrinarism

Most research in law is conducted in the doctrinarism method. This method is very much different from the methods used in traditional academic settings creating a chasm between legal scholarly research and research conducted in the traditional academic setting. Professors Lee Epstein and Gary King put it very succinctly:

> While a Ph.D. is taught to subject his or her favored hypothesis to every conceivable test and data source, seeking out all possible evidence against his or her theory, an attorney is taught to amass all the evidence for his or her hypothesis and distract attention from anything that might be seen as contradictory information. An attorney who treats a client like a hypothesis would be disbarred; a Ph.D. who advocates a hypothesis like a client would be ignored (Epstein and King, 2002).

This difference is the result that the tasks and objectives of teaching of law and that of research university faculties have traditionally differed. Law faculty have

traditionally trained students to be professional lawyers, who are learned in the law but the "learning consists of a "skill set" for practicing law, not a learning that equips them to participate in the scholarly life of a law professor" (Ulen, 2004) while traditional academic faculty has trained students to be scholars and teachers. To be a successful legal scholar meant addressing in a meaningful way practitioners outside of the academy, principally lawyers and judges rather than scholars from within the academy (Ulen, 2004). In contrast, academic faculty writes for their peers, other scholars, they share their work in progress in seminars and workshops and reduce their teaching load to have more time to write scholarly articles and books (Ulen, 2004). In law, the goal of scholarship is to bring coherence to the practice of law, to impart in the scholar how to have an impact upon judges and lawyers, how to influence the doctrine, how to persuade those in a position to make law to adopt the persuader's view, how to recognize past errors and how to gain standing as a source of guidance and how to reform the law - with indoctrinating its students into the ways of the profession and imparting into them how to be successful (Ulen, 2004). Additionally with doctrinarism rules are confined to a particular area of the law as well as confined to a time or place. As a result commentators would note that vast differences in institutional, cultural, historical and social aspects of legal systems made theorizing about law inapposite (Ulen, 2004). In academia, the goal is to advance the body of knowledge and to accomplish those ends students are taught how to critically evaluate old propositions, construct new propositions and evaluate the tested propositions in light of objective truth. Finally in law, it is the student not the law professors who act as editors and

reviewers of law journals. The student's role is to make certain the articles are complete, containing all relevant cases and arguments advanced in past work. This is in stark contrast to academia journals which advance theory and knowledge in the field through the review of prospective articles by other scholars.

As a result of the above:

> "… law faculty have been wed to a non scientific conception of their scholarship that they do not readily and naturally think of the connection between theory and empirical work that the scientific method necessarily implies" (Ulen, 2004).

In Doctrinal Analysis either a case or a string of cases are examined historically. This case (or cases) is then stripped to the bare factual essentials. From these facts universal rules are constructed and espoused making the output rule centric. This rule centricity tends to relegate its findings to a high level of generality so that its rules can be universally applied. Under this approach rigor is achieved through the framing of issues, analysis of the facts and framing of universal laws.

Examine a case or string of cases
Strip out the unnecessary facts
Construct universal rules
Apply the rules

Table 3 Rigor

2.3.2.2 Empirical Legal Research

To some degree the legal faculty is adopting empirical scholarship like activities similar to those of research universities. At present these activities are in their infancy and are principally confined at the present to law and economics research.

The topic of empirical scholarship has been done in a very limited basis with most of this confined to law and economics studies[15]. For a variety of reasons some law professors today are seeking to establish credentials that compare with the credentials held by faculty in research universities.[16] This interest in empirical work was ramped up in 2001 in a symposium organized at the University of Illinois Law Review (McAdams and Ulen, 2002). This was followed in 2002 through a series of exchanges in University of Chicago law review (Revesz, 2002). In 2004 American Association of Law Schools (AALS) devoted its annual meeting to the topic of empirical research on law. Its President Bill Hines in 2005 announced that designs of this kind of research as a top priority for the legal academy today (Hines, 2005). The theme for the 2006 AALS annual meeting was "Empirical scholarship: what should we study and how should we study it?" Furthermore, there are signs of convergent lines of thinking from different corners of law and social science, pointing toward the possibility of a new synthesis (Erlanger et al, 2005).

This is not to say there was no empirical type of research conducted in law. Nearly all law review scholarship offers some statement about the real world, and thus has an empirical component because nearly all legal scholarship makes empirical claims, it must also satisfy basic inferential rules (Tracey, 2006). Epstein and King

---

[15] Richard Posner has conservatively published over 200 books and articles over the years applying the field of economics to law. *See, e.g.*, GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970); RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (1st ed. 1972).

[16] Richard Posner posits that this change in legal scholarship is motivated because of valuable independent developments in non law disciplines and the dramatic increase in law professors over the years is driving them to seek new ways to distinguish their work from other peers. See in general Posner, Richard, *Legal Scholarship Today*, 115 Harvard Law Review,1314 (2002)

provided some rules in which empirical legal research should be conducted (Epstein and King, 2002). These rules include research should have a clear goal, and its methodology should be subjected to the rules of replicability, it must be a social enterprise – its underpinnings are accessible for review and extension of others in the field. Researchers must acknowledge the uncertainty associated with empirical work, research should engage existing empirical literature, only important research should be conducted with theories with observable implications and make an effort to account for rival hypothesis. In essence there is little disagreement with non legal academics as to the methodology required to be performed. Early papers such as Epstein and Ulen did not distinguish between a descriptive and positive approach, instead they concentrated on conducting legal research in the tradition of the academic although recent studies now are beginning to distinguish between descriptive and positive empirical research (Tracey, 2006).

Epstein and King
Clear goals
The work is capable of being replicated
Underpinnings are available for review and extension by others in the field
Researcher acknowledge the uncertainty associated with empirical work
Engage existing empirical literature
Theories advanced with observable implications

Table 4 Standards for Legal Empirical Research

2.3.2.3 Legal Research in the Case study tradition

Case study research has been preformed as a research method in the law field for a number of years. The earliest example of a contextual case study found is by Walter Nelles (First American Labor Case , 1931). It appears that this type of work was

resurrected in the 1975 article by Richard Danzig (Hadley v. Baxendale, 1975), who is an acknowledged leader in the use of the methodology both as a method of research as well as pedagogy (Danzig, 1978). This method again surfaced in 2003 by Debora L. Threedy, Unearthing Subversion with Legal Archaeology, 13 Tex. J. Women & L. 133, 136-38 (2003). Many legal archeologists freely adopt the principles and guidance provided by Glasser and Straus (Glasser and Straus, 1967) and Yin (Yin, 2003).

The term "legal archaeology" refers to a type of legal history that makes use of case studies. "Legal archaeology[17] involves both a microscopic examination of the shards uncovered by painstaking digging, and a macroscopic assessment of how the component parts fit together to describe and explain the culture left behind" (Maute, 2000).

Legal archaeology is defined by an approach to legal materials that employs a methodology that academics call grounded theory. To "do" legal archaeology is to develop an in-depth study of an individual case by reconstructing its historical, economic, and social context. Legal archaeology posits that there is much to be learned from a case that does not show up in the "official" narrative in the reported opinion and it seeks to recover alternative, "unofficial" accounts of the dispute. These alternative accounts provide a different and complementary way of knowing the law than that derived from more traditional studies

What is so revolutionary about it in the legal field is that it is contrary to doctrinal analysis which is a historical, strips facts to essentials, is rule centric, and

[17] This is a term coined by Debora Threedy to describe grounded theory in legal research.

tends to aspire its findings to a high level of generality so that its rules can be universally applied. It is the methodology in which the bulk of the scholarly research is done in law. Legal archaeology is a philosophical descendant of American pragmatism and its offshoot, legal realism. The legal realists conceived law as being situated in the social fabric of its time and place. The legal archaeologist sees value in the study of a single time and place. Pragmatism and legal archaeology both have a "commitment to finding knowledge in the particulars of experience" (Radin, 1990). Both turn away from abstraction and "atemporal universality" and embrace "historicity, concreteness, situatedness, contextuality, embeddedness, narrativity of meaning" (Radin, 1990).

Doctrinal Analysis	Grounded Theory
High level of generality –	Very specific and detailed
A-historical	Historical
Rule centered. Rules are framed at a high level of generality so to cover a magnitude of factual scenarios	Specific knowledge
Facts are stripped to essentials and abstracted	Factual details in all the multifaceted splendor

Table 5 Comparison between Grounded Theory and Doctrinal Analysis

Threedy provides a primer on how to conduct a rigorous legal archaeology (Threedy, no year). Legal archaeology does not resemble more traditional legal scholarship because it begins where most legal scholarship ends, with a reported case opinion. Once you have the opinion, it is then analyzed. Next you recreate as complete a record of the litigation as possible, including the trial and appellate records. The next step involves placing the litigation in historical context by searching nonlegal sources

for information regarding the events and participants in the litigation, as well as the economic and social background against which the litigation unfolded. These nonlegal sources include archival material, newspaper accounts, biographies and autobiographies, and fieldwork such as interviews and nonlegal secondary literature

Once this is all assembled - describe. At a minimum, processing requires description, that is, the structuring of the information uncovered by the project into a coherent narrative. The purpose of this descriptive narrative is to "get the story straight." Such projects can be analogized to what in sociology is sometimes called "Chicago school" monographs, meaning qualitative data consisting of rich descriptions of social phenomena (Threedy citing Glasser and Strauss, 1967).

Once the description is created you then proceed and begin to investigate explanations and causal connections between the reconstructed facts and the outcome and rule in the excavated case. The best use of legal archaeology projects is to consider them as historical case studies that provide the raw data from which to develop theories about how law operates in society (Threedy citing Yin, 2003).

Threedy goes on to cite Glaser and Strauss's bottom-up theorizing or what has been called "grounded theory." In grounded theory, "one generates conceptual categories or their properties from evidence; then the evidence from which the category emerged is used to illustrate the concept (Threedy citing Glasser and Strauss, 1967). " Another way of describing this type of theorizing is to say that the case method allows "the data to set the theoretical agenda, rather than vice-versa" (Threedy citing Glasser and Strauss, 1967). Each individual legal archaeology project can and should

incorporate grounded theory; by analyzing the raw data of the case study, the legal archaeologist develops insights into the judicial process or the role of law in society. This dissertation shall adopt the case study methodology of Glaser and Strauss.

2.3.3 Changes in what is Private in American Law: a Case Study

The notion of privacy is ancient. The Bible and Aristotle alluded to privacy (DeCew, 1997). John Locke applied this concept to distinguish between private property and property owned publicly or in common with all (Locke, 1988). Anthropologic studies by Margaret Mead and others suggest that the concept of privacy is cross-cultural and present in all but the simplest, most primitive societies (DeCew, 1997). In the realm of health law, one can argue that privacy has always been valued, because the Hippocratic Oath required physicians to keep private what they learned through their physician-patient relationship.

2.3.3.1 Confidences

Historically, privileges were created to protect confidential information. In Elizabethan times the gentleman owed a duty of confidentiality toward those who reposed in them their confidences. This duty required the gentleman to act with honor and integrity and hold this confidential information against all inquiries and forbade them to disclose under any circumstance other than with the consent of the person who reposed in them the information (Annesley v. Anglesea, 1743). This privilege was assaulted in 1562 when an act of Parliament made it a universal duty to testify.[18] While

[18] Act of Punishment of Such as Shall Procure or Commit any Willful Perjury See also Cobbetts State Trials 769. 788 (1612) ("(A)ll subjects, without distinction of degree owe to the king tribute and service

this act interfered with the gentleman's honor to keep confidences shared, this act seriously also threatened confidentiality between the client and the lawyer as with the enactment of this law, judicial search for truth could no longer be obstructed by voluntary pledges of secrecy. Judges of that time soon created an exception and decreed that legal communications formed a special category of exception to testify because of the importance of the client obtaining advice would be hindered by the clients fear of disclosure of his confidences. Later privileges were also extended formally (at law) or informally (by convention) when information subject to privilege is sensitive to the owner of the information[19].

2.3.3.2 Castle Doctrine

"Every man's house is his castle" was a maxim much celebrated in England, as was demonstrated in Semayne's Case (5 Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604))[20], decided in 1603. A civil case of execution of process, Semayne's Case nonetheless recognized the right of the homeowner to defend his house against unlawful entry even by the King's agents, but at the same time recognized the authority of the appropriate officers to break and enter upon notice in order to arrest or to execute

---

not only of their deed and hand but of their knowledge and discovery"- Sir Francis Bacon) Prior to this act the opponent in a jury trial was not compellable to be a witness. Wigmore, J.H., A Treatise on the Anglo-American Law of Evidence, Mc Naughton Rev. Edn, Little Brown, Boston, Section 2217 at 169 (1961)

[19] This information is sensitive because when disclosed, this information often brings both real or potential shame and harm to the individual, family or associates.

[20] One of the most forceful expressions of the maxim was that of William Pitt in Parliament in 1763: "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail--its roof may shake--the wind may blow through it--the storm may enter, the rain may enter--but the King of England cannot enter--all his force dares not cross the threshold of the ruined tenement."

the King's process. Most famous of the English cases was Entick v. Carrington[21], one of a series of civil actions against state officers who, pursuant to general warrants, had raided many homes and other places in search of materials connected with John Wilkes' polemical pamphlets attacking not only governmental policies but the King himself. Entick, an associate of Wilkes, sued because agents had forcibly broken into his house, broken into locked desks and boxes, and seized many printed charts, pamphlets and the like. In an opinion sweeping in terms, the court declared the warrant and the behavior it authorized subversive "of all the comforts of society," and the issuance of a warrant for the seizure of all of a person's papers rather than only those alleged to be criminal in nature "contrary to the genius of the law of England."[22] This case became the basis of the 4th Amendment to the Constitution of the United States which among other things provided, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…”[23]

2.3.3.3 Sentiments and Thoughts

Every person at common law was allowed to determine the extent of sharing their thoughts, sentiments and emotions with others[24] and could not be compelled to share them except in limited circumstances. As justification, Lord Cottenham declared “a man is that which is exclusively his.”[25]

---

[21] 19 Howell's State Trials 1029, 95 Eng. 807 (1705).
[22] 5 Eng. Rep. 817, 818
[23] 4th Amendment to the Constitution of the United States
[24] Yates, J., in Millar v. Taylor, 4 Burr. 2303, 2379 (1769). [p. 198 Note 2 in original.]
[25] Lord Cottenham in Wyatt v Wilson 1820

It was acknowledged in the English courts that “every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends”.[26] The right is lost only when the author communicates (publishes) his production to the public.[27] The produce of mental labor, thoughts, and sentiments preserved by writing was at common law required to be protected as property and provided security, at least before general publication by the writer's consent.[28]

Knight Bruce, Vice Chancellor stated:

> "Upon the principle, therefore, of protecting property, it is that the common law, in cases not aided or prejudiced by statute, shelters the privacy and seclusion of thought and sentiments committed to writing, and desired by the author to remain not generally known" (Prince Albert v. Strange, 1849).

A more liberal doctrine was recognized in Prince Albert v. Strange (Prince Albert v. Strange, 1849) where a less clearly defined principle yet one more broad then mere property right was advanced. The court stated that the mere publishing of a statement that a man had ‘written to particular persons or on particular subjects” as an instance of possibly injurious disclosures as to private matters that the courts would prevent.

2.3.3.4 U.S Constitution

---

[26] Yates, J., in Millar v. Taylor, 4 Burr. 2303, 2379 (1769). [p. 198 Note 2 in original.]
[27] Duke of Queensbury v. Shebbeare, 2 Eden 329 (1758), Bartlett v. Crittenden, 5 Mc Lean 32, 41 (1849)
[28] Knight Bruce, V.C., in Prince Albert v. Strange, 2 DeGex & Sm. 652, 695 (1849). [p. 199 Note 5 in original.]

The U.S. Constitution adopted the law of England as its basis for the obvious reason of the respect the colony had for this body of law. Americans can never be sure what her founding fathers intended regarding federal protection of a right to privacy. A "right to privacy" is not explicitly mentioned in the United States Constitution or the Bill of Rights. In fact, the word privacy never appears in these documents at all, arguably suggesting that the founding fathers thought the states were capable of protecting citizens' privacy rights as a part of their general welfare. Despite this lack of clarity, both state and federal courts, as well as legislatures, have demonstrated a willingness to protect some forms of personal privacy (Eddy, 2000). The concept of a fundamental right to privacy is bifurcated into two distinct rights: one right is based in natural law, [29] the Judeo-Christian law, Aristotle and Locke's philosophy of law and British common law; a second right is implied from the language of the United States Constitution (DeCew, 1997).[30]

The 4th Amendment to the Constitution of the United States provides, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…” Arguably the right to be secure in person is directed to the confidences, right to be secure in houses is an attempt

---

[29] The right of privacy has its foundation in t*he instincts of nature. It is recognized intuitively, consciousness being the witness that can be called to est*ablish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private, and there are matters public so far as the individual is concerned. See Pavesich v. New England Life Ins. Co., 50 S.E. 68, 69 (Ga. 1905).

[30] Ms. DeCew quotes Milton Konvitz pointing out that the Adam and Eve story introduces the feeling of shame at the violation of privacy and emphasizes how Aristotle divided an individual's life into two realms: the polis (the realm common to all citizens) and the oikos (the realm of the private household).

to codify the Castle Doctrine, and the right to be secure in papers is the sentiments and thoughts.

2.3.3.4.1 The Right to be let (left) alone

The famous phrase, the right "to be let alone" has a long history. As far back as 1834, the U.S. Supreme Court mentioned that a "defendant asks nothing — wants nothing, but to be let alone until it can be shown that he has violated the rights of another."[31] This ruling only set the boundary between the government and the governed and did not provide strictures against other violations of individual privacy.

This right to be left alone was extended to individuals in a limited way about 50 years later but indirectly. In 1880, Thomas Cooley, a judge and legal scholar of the day applied the "right to be let alone" doctrine to intrusions by individuals on another individual. He explained privacy as a "right" to one's person or personal immunity.[32] Cooley never created a separate right of privacy but rather used it as a pretext to control access to the individual. Later, in a medical setting, this right to be alone was linked to the term privacy to support a personal injury claim of battery when a woman was observed during childbirth without her consent. In this case, the Michigan Supreme Court held: "the plaintiff had a legal right to the privacy of her apartment at such a time, and the law secures to her this right by requiring others to observe it, and to abstain from its violation." [33]

---

[31] *Wheaton v. Peters*, 33 U.S. 591, 634 (1834).
[32] Thomas C. Cooley, Law of Torts (1880).
[33] De May v. Roberts, 46 Mich. 160 @165-166 (1881)

2.3.3.4.2 The Developing of State Mandated Privacy - Warren and Brandeis

After Cooley, American law began to address privacy in the nineteenth century. At the height of the Muckraking Era, where the forces of industrialization and urbanization began to challenge and change society, Samuel D. Warren and Louis D. Brandeis published an article entitled *The Right to Privacy* in the Harvard Law Review (Warren and Brandeis, 1890). This work further developed Cooley's right of privacy.

They proffered a historical evolution of the law to buttress their claim for the recognition in the legal field of a right to privacy that encompassed thoughts, emotions and sensation. Looking at life, liberty and property they noted the law initially only protected physical interferences with life and property and saw the right to life as freedom from battery, liberty as freedom from actual restraint and right to property limited to tangible things such as land and cattle. Later as the law recognizes a man’s spiritual nature, his feelings and intellect, the right to life expands to include not only battery but the right to enjoy life. Liberty now encompasses freedom from actual constraint but the exercise of civil privilege, and property not only the right to land and cattle but ownership of anything you can possess is it tangible or intangible. When the law recognized sensation further changes were made to these concepts of life, liberty and property.

Legal Remedies	Translation
Physical Interference with life and property	Right to life = Freedom from Battery Liberty = Freedom from actual restraint Right to Property = Right to land and cattle
Recognition of man's spiritual nature, feelings and intellect	Right to life = Right to enjoy life Liberty =Exercise of civil privileges Property = Every form of possession both tangible and intangible
Recognition of Sensation	Protection against bodily injury is expanded to attempts Laws of nuisance develop Slander laws develop
Inventions and Business methods	Require that a step needs to be taken for the protection of the individual and to secure her right to be left alone.[34]

Table 6 Legal Remedies and Translation

Brandeis' and Warren's article stated that "political, social and economic changes entail the recognition of new rights." [35] They saw that advances of civilization (technological change and organizational practices) have intensified intellectual life, emotional life, and heighten the senses of human kind.

> "As the result of the intensification of intellectual and emotional life and the heightening of the senses that came with the advance of civilization made it clear to men that only part of the pain, pleasure and profit of life lay in physical things. Thoughts emotions and sensations demanded legal recognition" (Warren and Brandeis, 1890).

Warren and Brandeis championed a call to protect the privacy of the individual and proposed an extension to privacy, in reaction to a perception that the press was overstepping the bounds of decency: the right to be let alone and the right to be

[34] Cooley on Torts, 2d ed., p. 29. [p. 195 Note 4 in original.]
[35] Ibid

protected from the unauthorized publicity of essentially private affairs. The individual should have full protection in person and property. They urged the common law to vindicate and protect those rights. They further observed that the common law already offered some protection against the mental distress associated with public publishing of private information (e.g., the protection against making private letters available to the public) (Warren and Brandeis, 1890).

They argued this protection should be extended to protect the individual's privacy more generally saying:

> "The principle which protects personal writings and any other productions of the intellect or of the emotions is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relations, domestic or otherwise" (Warren and Brandeis, 1890).

Brandeis and Warren adopted the definition of privacy as "the right of the individual to be let alone" (Warren and Brandeis, 1890).[36] Warren and Brandeis argued that the individual should enjoy, cognizable in the law, freedom from unwanted publicity (Warren and Brandeis, supra note 22, at 206, 1890). They reinforced their argument by the review of various court decisions that protected privacy (but had never used the term privacy) and made the conclusion that an individual had a type of ownership interest in the facts of his private life. From this Warren and Brandeis concluded, that the common law secures to each individual the right of determining,

---

[36] Justice Brandeis dissenting in Olmstead v. United States, a wiretapping case, stated that "[the makers of our Constitution] conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men." 277 U.S. 438, 478 (1928).

ordinarily to what extent his thoughts, sentiments and emotions shall be communicated to others in other words the “right of the individual to be let alone” (Warren and Brandeis, 1890).

Brandeis and Warren conceded their proposed common law right to privacy was not absolute. For example, matters of general public interest or pertaining to public figures could be investigated and published without legal recourse. Further, they stipulated that consent should be a defense to invasion of privacy (Warren and Brandeis, 1890).

Years later Dean Prosser suggested that when Brandeis and Warren spoke of a right to privacy, they were really describing four rights -- a right to be protected from intrusion, a right to control the disclosure of private facts, a right to protect the commercial value of one's name or likeness, and a right to protect against "false light" disclosures. *The Restatement (Second) of Torts* (B, C, D, E) recognizes four common law torts for invasion of privacy. Three of these torts are appropriate for our consideration. Intrusion upon seclusion deals with protecting people against both physical intrusions into the space they claim their own and various forms of eavesdropping in the same protected space. The dissemination of private facts occurs when publicity is given to facts about a person that the person would prefer not to be known, without that persons consent. False light is the publication of facts the person would prefer not publicized, but the person is portrayed in a way that is not true.

2.3.3.4.4 Personal Rights of Privacy – Constitutional Protections

Personal rights of privacy were very limited despite some extension to activities relating to marriage, Loving v. Virginia, 388 U.S. 1, 12 (1967); procreation, Skinner v. Oklahoma, 316 U.S. 535, 541-542 (1942); family relationships, Prince v. Massachusetts, 321 U.S. 158, 166 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925) and Meyer v. Nebraska. *262 U.S. 390 (1922).* Each of these cases stopped short of declaring a constitutional right of personal privacy. Beginning in 1965 and continuing through the 1980's a series of cases began to tout that the right of personal privacy was a right guaranteed by the U.S. Constitution.

For a determination to be made that the U.S. Constitution guaranteed a right of personal privacy, it must be found that privacy was a fundamental right or that privacy was a right implicit in the concept of ordered liberty (Roe v. Wade 410 U.S. 113 (1973)). This did not come all at once. In the case of

In Griswold v. Connecticut (381 U.S. 479 (1965)) the first step was taken. Connecticut law had made it criminal to counsel married couples regarding the use of birth control. In striking down the law as unconstitutional the court found that though the Constitution does not explicitly protect a general right to privacy, the various guarantees within the Bill of Rights create penumbras, or zones, that establish a right to privacy. Together, the First, Third, Fourth, and Ninth Amendments, create a new

constitutional right, the right to privacy in marital relations**:** Privacy is a personal right of non interference

What is important to note is that the ruling in Griswold did not tie the right of privacy to any one amendment of the U.S. Constitution. The First Amendment protected privacy from forms of governmental invasion by limitation upon governmental abridgment of freedom to associate and privacy in one's associations. The Third Amendment prohibited the non consented peacetime quartering of soldiers. The Fifth Amendment reflects the Constitution's concern for the right of each individual to a private enclave where he may lead a private life.

The 4th Amendment provides 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 while prohibiting unreasonable searches and seizures." This was never interpreted as general constitutional "right to privacy" This began to change with the decision of Katz v. U.S. (369 U.S. 347 (1967)) In that case, the Fourth Amendment was recognized as a right to privacy that protected not only tangible property but also protected intangible conversations. Further its protections were extended from the protection of places to the protection of people – giving people the right to be left alone.

In Katz, the court stated:

> "The Fourth Amendment protects people not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection, but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. The Fourth Amendment governs not only the seizure of tangible items, but

> extends as well to the recording of oral statements that are overheard" (Katz v. U.S. 369 U.S. 347, 1967)

Katz extended privacy places to people and places and its protections to tangible items to both tangible and intangible items (conversations) but it had not created a right of personal privacy tied to the United States Constitution.

Another case interpreting the Fourth Amendment was Terry v. Ohio which was decided a year after Katz.. In Terry the court pronounced that in addition to the protections in Katz. the 4th Amendment is a right for a person "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, (which) shall not be violated . . . ." and is :

> "… a right of personal security (that) belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. No right is held more sacred, or is more carefully guarded, by the common law than the right of every individual to the possession and control of his own person, free from all restraint or interference, unless by clear and unquestionable authority of law" (Terry v. Ohio 392 U.S. 1, 1968)

In the monumental case of Roe v Wade (Roe v Wade 410 U.S. 113, 1973), the court noted that "only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty" are included in the (Constitutional) guarantee of a right of personal privacy." The court in its search to find a constitutional basis for privacy noted that the Constitution does not explicitly mention any right of privacy. The court found the Constitution implicitly guarantees a right of personal privacy, or at least

made a guarantee of certain areas or zones of privacy. On basis of its analysis the court announced:

> "the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution".

In Whalen v. Roe this right of personal privacy was said to include "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions" (Whalen v. Roe, 429 U.S. 589, 599-600. 1977). Froomkin, an eminent legal scholar notes that since Roe v. Wade, the law has recognized a right to be left alone, a right to autonomous choice regarding intimate matters, the right to autonomous choice regarding personal matters (Froomkin, 2000).

In the subsequent case of Paul v. Davis (Paul v. Davis 424 U.S. 693, 1976), the Court pronounced when petitioned to extend a right to privacy to the publication of records of official acts such as arrests, that such extension of privacy was not justified as it did not fall under the rubric of privacy rights. The constitutional right to privacy was limited to matters relating to inherently intimate activities such as "marriage, procreation, contraception, family relationships, and child rearing and education." The importance of intimate activities was later discussed in the case of Roberts v. United States Jaycees (468 U.S. 609, 1984). Intimate activities are important as they embody the fact that we all depend on the "emotional enrichment of close ties with others" (Roberts v. United States Jaycees, 468 U.S. 609, 1984). The dissenting opinion of

Justice Blackmun in Bowers v. Hardwick, further emphasizes their importance as intimate activities regulate the nature of an agent's personal associations with others (Bowers v. Hardwick, dissenting opinion, section III).

2.3.3.4.4 The First Amendment Protections: Privacy and Association

In addition to the pronouncement that the Fourth Amendment protected people not places, Katz also recognized that the First Amendment imposed a limitation upon governmental abridgment of the freedom to associate and ensured privacy in one's associations (Katz v. U.S. 369 U.S. 347, 1967).

The freedom of association is protected in two distinct senses. In one line of decisions intrusion of the State in certain intimate human relationships must be thwarted because of the role such relationships play safeguarding the individual freedom that is central to our constitutional scheme. In this respect, freedom of association receives protection as a fundamental element of personal liberty.

Because the Bill of Rights is designed to secure individual liberty the Supreme Court has recognized that it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State (Roberts v. United States Jaycees, 468 U.S. 609, 1984).[37] The Roberts case goes on to state:

> "Without precisely identifying every consideration that may underlie this type of constitutional protection, we have noted that

---

[37] Roberts v. United States Jaycees, 468 U.S. 609 (1984) citing *Pierce* v. *Society of Sisters*, 268 U.S. 510, 534-535 (1925); *Meyer* v. *Nebraska*, 262 U.S. 390, 399 (1923).

certain kinds of personal bonds have played a critical role in the culture and traditions of the Nation by cultivating and transmitting shared ideals and beliefs; they thereby foster diversity and act as critical buffers between the individual and the power of the State. See, *e. g., Zablocki* v. *Redhail*, 434 U.S. 374, 383-386 (1978); *Moore* v. *East Cleveland*, 431 U.S. 494, 503-504 (1977) (plurality opinion); *Wisconsin* v. *Yoder*, 406 U.S. 205, 232 (1972); *Griswold* v. *Connecticut*, 381 U.S. 479, 482-485 (1965); *Pierce* v. *Society of Sisters, supra*, at 535. See also *Gilmore* v. *City of Montgomery*, 417 U.S. 556, 575 (1974); *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 460-462 (1958); *Poe* v. *Ullman*, 367 U.S. 497, 542-545 (1961) (Harlan, J., dissenting). Moreover, the constitutional shelter afforded such relationships reflects the realization that individuals draw much of their emotional enrichment from close ties with others. Protecting these relationships from unwarranted state interference therefore safeguards the ability independently to define one's identity that is central to any concept of liberty. See, *e. g., Quilloin* v. *Walcott*, 434 U.S. 246, 255 (1978); *Smith* v. *Organization of Foster Families*, 431 U.S. 816, 844 (1977); *Carey* v. *Population Services International*, 431 U.S. 678, 684-686 (1977); *Cleveland Board of Education* v. *LaFleur*, 414 U.S. 632, 639-640 (1974); *Stanley* v. *Illinois*, 405 U.S. 645, 651-652 (1972); *Stanley* v. *Georgia*, 394 U.S. 557, 564 (1969); *Olmstead* v. *United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

The personal affiliations that exemplify these considerations, and that therefore suggest some relevant limitations on the relationships that might be entitled to this sort of constitutional protection, are those that attend the creation and sustenance of a family -- marriage, *e. g., Zablocki* v. *Redhail, supra*; childbirth, *e. g., Carey* v. *Population Services International, supra*; the raising and education of children, *e. g., Smith* v. *Organization of Foster Families, supra*; and cohabitation with one's relatives, *e. g., Moore* v. *East Cleveland, supra*.

"Family relationships, by their nature, involve deep attachments and commitments to the necessarily few other individuals with whom one shares not only a special community of thoughts, experiences, and beliefs but also distinctively personal aspects of one's life. Among other things, therefore, they are distinguished by such attributes as relative smallness, a high degree of selectivity in decisions to begin and maintain the affiliation, and

> seclusion from others in critical aspects of the relationship. As a general matter, only relationships with these sorts of qualities are likely to reflect the considerations" that have led to an understanding of freedom of association as an intrinsic element of personal liberty" (Roberts v. United States Jaycees, 468 U.S. 609, 1984).

In another other line of decisions, the Court has recognized a right to associate for the purpose of engaging in those activities protected by the First Amendment -- speech, assembly, petition for the redress of grievances, and the exercise of religion. The Constitution guarantees freedom of association of this kind as an indispensable means of preserving other individual liberties.

Keeping one's membership in a group private may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs (United States v. Rumely 345 U.S. 41 at 56-58). It has been noted that "the State-compelled disclosure of affiliation with groups who are engaged in advocacy may constitute an effective restraint on the freedom of association" (National Association for the Advancement of Colored People v. Alabama ex rel Patterson, Attorney General 357 U.S. 449, 1958). As an illustration of a form of governmental action which might interfere with freedom of assembly, was pointed out in American Communications Assn., "A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature" (American Communications Assn. v. Douds 339 U.S. 382 at 402).

Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs has been found to be an area where privacy is required “particularly in cases where it is shown that on past occasions revelation of the identity of its members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility” (National Association for the Advancement of Colored People v. Alabama ex rel Patterson, Attorney General 357 U.S. 449, 1958). This is so because it may induce the members to withdraw from the association and dissuade others from joining it because of the fear of exposure of their beliefs shown through their associations (National Association for the Advancement of Colored People v. Alabama ex rel Patterson, Attorney General 357 U.S. 449, 1958). Should this occur disclosure of the association's membership is likely to affect adversely the ability of the association and its members to pursue their collective effort to foster beliefs which they have the right to advocate?

2.4 Summary

A rigorous review of the epistemological basis of privacy followed by a review of the axiology and ontology of privacy has been provided. In philosophy three ontology exist- one control based, another access based and the final a combination of control and access.

It was demonstrated that Ontology and Axiology is related to rights theory. Rights, claims and entitlements of privacy determine behavior by enabling and constraining conduct. Through Hohfeld’s Normative Position rights have been shown to be a cluster of enablement or constraints in conduct. Next it was shown that privacy

rights embody the conventions, values and principles of a society and specify behavior consistent with its conventions, values and principles through its laws, norms, private ordering or agreements. It was demonstrated that privacy supports many different values each having distinct rights, claims and entitlement that vary in terms of control and access to ensure the value that is sought to be protected.

The conception of privacy in the field of law was examined. Where philosophy is often seeking and defining ideals; law is pragmatic seeking real life implementations of ideals. In particular, law is concerned with the coordination, motivation and direction of human and non human action through use of value based rights of control and access to information that define roles so that the values of privacy pursued can be ensured. Law implements privacy through the establishment of specifications of behavior to ensure desired societal values are obtained. A history of the law of privacy was provided that demonstrated that the values privacy seeks to protect at law are broad, covering a wide variety of information under an equally broad situational area that is ever changing.

In the following chapter, a multidimensional construct of privacy will be proposed. Any taxonomy should provide the ability to classify into types with each type classification unique and distinguishable from all other types.Through the use of the control/access framework established in philosophy and the examination of privacy laws , five distinct patterns of control and access emerge that reflect a different value of privacy desired and required by society. Each of these patterns has a unique

specification in the control and access of information. These five distinct patterns are then described and distinguished.

Chapter 3: The New Construct of Privacy

3.0 Proposal of a new conceptualization of privacy

When is information private? Under one theory, what is private information is determined by the situation. What this means is that information that is private in the context of one situation may not be private in the context of another situation. By way of example we permit a criminal to tell his lawyer all the details of his actions and expect this disclosure to be protected as private but we do not allow this same protection to be enjoyed by the criminal when they confess their crime to a passer by.

The idea that a social activity demanded privacy was first suggested by Inness in her study of intimacy and privacy. In her work of defining the privacy that attended interpersonal relationships, Inness recognized that the role an activity plays in the life of the person determines whether the activity is intimate and thus entitled to protection through privacy (Inness, 1992). Private information is more than intimate information it is special information that is not subject to general disclosure and access.

It is important to note that the information which is deemed private both enables a created role to be performed and the enables the benefits of the role to be realized. Private information enables the role as on the basis of information control and access it creates the role and at the same time it segregates those inside the role from those outside the role on the same basis of control and access to information. Additionally the quality of the privacy in the information determines the potential benefit of the role. A high degree of privacy in information ensures that a maximum benefit is to be achieved in the roles that require private information. In effect private information has a role – a

role of completing a defined role. In the above example the conveying of information between the attorney and his client enabled the recognized role of attorney-client to be preformed. The role was created because it is valuable. The information being held private enables the role as it segregates those inside the role from those outside the role on the basis of access to information. The fact the information is highly private enables the role to provide its fullest benefit. In contrast, the role between the criminal and passerby is not protected as it is not valuable. Information exchanged between the two parties is not deemed private because of the lack of importance and the fact that a lack of information will not impede the benefit of the role.

Laws, norms, and agreements structure our society and define rights. These defined rights create roles that ascribe the expected conduct for societal entities[38] including the privacy in information. When societal entities interact, they form a relation of which the sum of the mutual ascribed roles and interactions of those roles is a relationship. While a person may engage in many role based activities, not all role based activities or relationships are entitled to privacy protection. For roles where privacy is at issue there is a defined control over and access to information that every relater possesses. Control over information is defined by the degree of control an entity possesses over what information is released, when that information is released and to

---

[38] According to Edelman, organizations in normative models conform because law enunciates social values, ethics and role expectations which organizations and its members elaborate and internalize see Edelman, LB, Petterson, SE, Chambliss E, Erlanger HS, *Legal Ambiguity and the Politics of Compliance: Affirmative Action Officers Dilemna*, Law and Policy Vol 13 pg, 73-97 (1991) and Edelman LB, Abraham SE, Erlanger HS, *Professional Construction of the Legal Environment: The Inflated Threat of the Wrongful Discharge Doctrine,* Law Society Review, Vol. 26 pg 47-83 (1992)

whom the information is released. Access over information is defined by what, when and who has access to the entity and to the information about the entity. The sum of the roles of control and access between relaters define relationships that are privacy-based.

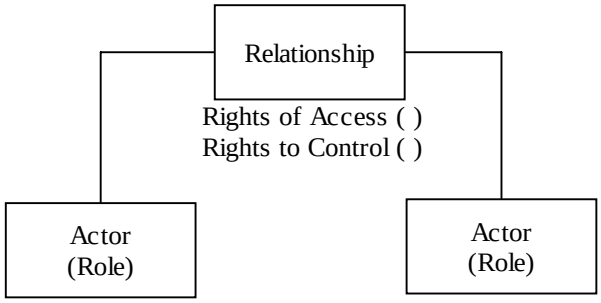

Figure 9 Basic Privacy Model

Five distinct role-based privacy relationships are proposed, each requiring relevant, appropriate and proper information. Each privacy relationship is grounded in a social role. All are composed of one or more entities. These entities can be a person, an organization or society itself. The roles of the relationship are supported by legal theories and imposed by laws, norms and or agreements that define rights of access and control over information that are unique in each relationship and in defining such, dictates to the relaters a unique role each must undertake. These different privacy types are based upon unique roles that entities require and demand in order to maximize their lives and existence and realize optimal benefits of societal life. These same privacy types set forward societal requirements to ensure that life.

These private relationships are as follows: Personal Privacy is a role based activity that ensures personal areas of a person's life remain their own, Privileged

Privacy enables the consultation of and assistance of third parties to be procured ensuring the ability to seek help, comfort and counsel, Intellectual Privacy permits the individual to develop a person's self and intellect, a Intellectual Privacy is a role based activity that protects certain types of secrets so as to ensure the enlistment of help, expertise and assistance of others needed for the attainment of socially desired goals and Secret Privacy safeguards the public domain so that life in private can remain private.

Privacy Type	Purpose
Personal Privacy	Ensures and enables a person so that personal areas of a person's life remain their own
Privilege Privacy	Ensures and enables a person so that they may seek the consultation of and assistance from third parties be procured ensuring the ability to seek help, comfort and counsel. Additionally it may protect certain classes of persons from being interfered with by outsiders.
Intellectual Privacy	Ensures and enables a person in their development of that person's self and their intellect
Secret Privacy	Protects certain types of secrets so as to ensure the enlistment of help, expertise and assistance of others needed for the attainment of socially desired goals
Transitory Privacy	Safeguards public and private spaces to ensure a privacy that meets the needs and expectations of societal members

Table 7 Privacy Types and Purposes

3.1 The Model

3.1.1 Relational Privacy

3.1.1.1 The purpose

This type of privacy is characterized by the belief that humans have the capacity to develop personal relationships and should develop these relationships along the line of their desires without the interference of others. These types of personal relationships run the gamut from structured (employer-employee), casual (friend/friend) to highly intimate (husband-wife). These relationships are important to the individuals involved and are often emotionally based. Often this type of relationship provides great personal value and satisfaction to the individuals involved in the relationship. In some cases these relationships also provide value to society as well. For this type of relationship to flourish, privacy enables the individual both the choice on which relationships to develop and the direction of development.

3.1.1.2 The relationship entities and characteristics of the relationship

In relational privacy one entity in the relationship must always be a person. The other entity generally can be one or more person, but it can be a representative of an organization, an organization itself or society.

Relationships of this type are of two configurations. One type of relational privacy is the formation of relationships between one or more other persons. This relationship requires the ability of the person to autonomously choose, construct and maintain relationships of his or her choosing free from intrusion of any entity even if the choice is irrationally based and made on less than full information

The person disclosing information has full power both to disclose information (or not) and to determine how much information is disclosed. This ensures that recipient of that information should only obtain information reasonable and necessary for the relationship to form and be maintained. The more intimate the relationship, the more sensitive and personal information that is usually be obtained. The disclosure of sensitive and personal information is not confined to intimate relationships. The more professional relationships exchange personal information as well, generally including living addresses, home phone and familial information. Regardless of the character of this relationship, once information is received, only a compelling necessity justifies its release to a third party or enables the disclosee to use this information against the discloser As such this disclosee has a duty to protect this information and permit only necessary access to the information.

Another type of relationship is the situation where there is no formation of any relationship with another individual, organization or society. This is distinguished from the first type of privacy in that while the person has the control over the when what and to whom information is disclosed it is coupled with a condition of no access to either the person or the person's information. In this second type of relational privacy those outside (persons, organizations and society) have no access to either the person, to decisions made by the person or to information about the person. These walled off areas are more limited than in the first instance of relational privacy and confined to certain defined activities, decisions and information about those activities of a person's life in sensitive and intimate areas of a person's life such as in the case where a woman enjoys

complete privacy with respect to her decisions regarding contraception and abortion, to matters involving the rearing of children and childbirth to name a few.

3.1.1.3 Philosophy Type

This relation is based in Lockean philosophy related to control. Locke distinguished between the realm of intimate personal and familial relations and the civic realm maintaining that intimate, personal and familial relations not be invaded or intruded upon by government, organizations, society or others outside those in the relation (Inness, 1992, Rachels, 1975). Locke saw that by restricting access individual control increased, thus enabling individuals to sustain "power, liberty and autonomy against potentially overwhelming forces of government" (Nissenbaum, 1998), and enabling the individual to have the power to live his life separate and apart from the direct and indirect influence of others. The value of privacy is the construction of a zone that enhances the both autonomy to engage or not engage in a personal relationship as well as the liberty to construct personal relationships as desired by the individual. The ability to control access to the individual, the ability to exert control over access to information about the individual, the ability to access the decisions made by the individual and the non interference with our choice to engage or not engage in the expression of our love like and caring (Inness, 1992), are ways to manage role expectation (relations are structured according to our understanding of what they are and what is due to them and from them) (Benn, 1975), as well as a way to avoid individuals being judged out of context (Rosen, J. 2000), and are a way to ensure equality (Rao, 2003).

Role characteristics of Relational Privacy in terms of control and access

A hallmark of relational privacy is the very high levels of control given to individuals coupled with others having low levels of accessibility to both the person and their information. In the area of access two conditions can exist. In some cases the individual has high control over access to their person and to their information. The importance of access limited is to provide a place to freely act and express the self outside the view of others or for the provision of a needed secure physical or private psychological space. In those cases where individual control is not possible norms and laws have traditionally provided limits of access to the person and information about the person. These high levels are necessary to form the relationships desired by people, to have true autonomous choice on what relationships are chosen, how they are constructed and maintained. They also are necessary to protect sensitive information and intimate areas of a person's life

3.1.1.4 Character of Information

The character of the information can be determined by an objective and a subjective test. The objective test is any information reasonable and necessary to form a desired relationship by a person is relational information. This can be information about the person themselves or their family, and generally forms an important part in the familial and/or intimate relationships of the person. It also can be sensitive and intimate information or information embarrassing to the individual or decisions made by the individual that are intimate and sensitive. The subjective test includes information the individual subjectively views as important and personal, intimate or sensitive that they

share purposely for relationship formation or relationship maintenance and growth even should the information shared have no value to a third party.

Certain information is deemed so sensitive and intimate that it is always found to be protected regardless of the person's subjective views toward that information. This type of information includes the decisions about birth control, abortion, family matters and relationships including marriage, child rearing and education

3.1.1.5 Representative Laws and Court Rulings

The following cases have recognized the importance of intimacy and declared a right of privacy exists: Loving v. Virginia, 388 U.S. 1, 12 (1967); procreation, Skinner v. Oklahoma, 316 U.S. 535, 541-542 (1942); family relationships, Prince v. Massachusetts, 321 U.S. 158, 166 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535 (1925) and Meyer v. Nebraska. *262 U.S. 390 (1922*) marriage, e. g., Zablocki v. Redhail, supra; childbirth, e. g., Carey v. Population Services International, cohabitation with one's relatives, e. g., Moore v. East Cleveland, *contraceptive use* Griswold v. Massachusetts and abortion in Roe v. Wade (which specifically recognized a right to be left alone, a right to autonomous choice regarding intimate matters, the right to autonomous choice regarding personal matters (Froomkin, 1996). These rights were reiterated in Paul v. Davis when the court stated the "right to privacy was limited to matters relating to inherently intimate activities such as "marriage, procreation, contraception, family relationships, and child rearing and education.". The importance of intimate activities in the case of Roberts v. United States Jaycees (468 U.S. 609, 1984) were found to be important as intimate activities

embody the fact that we all depend on the "emotional enrichment of close ties with others" (Roberts v. United States Jaycees, 468 U.S. 609 1984)[39] that a constitutional shelter of privacy afforded such relationships reflects the realization that individuals draw much of their emotional enrichment from close ties with others. Protecting these relationships from unwarranted state interference therefore safeguards the ability independently to define one's identity that is central to any concept of liberty. The dissenting opinion of Justice Blackmun in Bowers v. Hardwick, further emphasizes their importance as intimate activities regulate the nature of an agent's personal associations with others (Bowers v. Hardwick, dissenting opinion, section III).

3.1.2 Privilege Privacy

3.1.2.1 The purpose

When social approval is given to a privilege, security and privacy are enriched substantially (Krattenmaker, 1973). However sometimes disclosure of private matters need to be encouraged in order to achieve the optimum value from the relationship. In the case of privilege privacy individuals when confronted with certain challenges are encouraged to seek professional expertise.The professional often requires information that is highly sensitive, potentially harmful and highly embarrassing to the disclosing party. Under normal circumstances help is not sought or a less than full disclosure is made when it is sought. The encouragement to participate in this relationship comes

[39]. Note that Roberts v. United States Jaycees contains an explicit warning against limiting the scope of privacy to the family.

through a protection that any information provided to the professional will be safeguarded from disclosure. An additional protection of use is also present: unless a competing societal need is present any information disclosed in this relationship can never be attributed to or used against the disclosing party. The success of this relationship depends on the resolve of the agent to keep a purely second order relationship (Benn, 1975), demanding of him or her, a sensitive and reticent understanding of the sensitivity of the information entrusted.

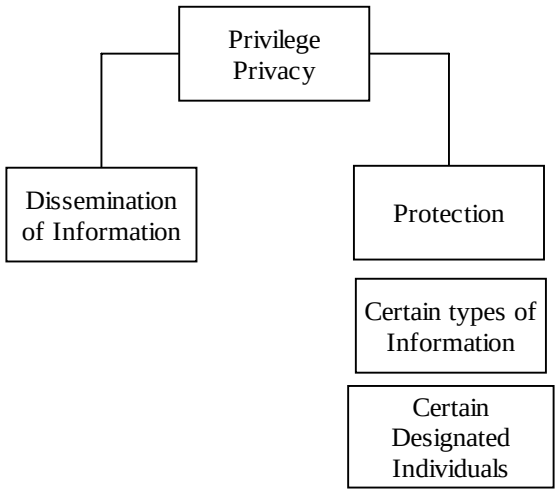

Figure 10 Purposes of Privilege Privacy

This type of information is often couched in terms of privileges. Privileges serve the public interest (Grant v. Downs (1976) 135 CLR 675 @ 685 (Stephen, Mason, Murphy JJ)) promoting values important to the society[40]. When information is covered

[40] A possible effect of ending lawyer/client privileges is should the client fail to disclose confidences due to the lack of privilege, the effectiveness of the lawyers representative maybe impaired while the search for truth not be advanced in the slightest degree.

by a privilege the owner of that information is assured that their information and identity would be protected. Privileges encourage the dissemination of information and the "making a full and frank disclosure of relevant circumstances" (Grant v. Downs (1976) 135 CLR 675 @ 685 (Stephen, Mason, Murphy JJ)). Privilege permits full development of the public self by enabling the individual to exert a control over the audience who receives the information, the timing and release of the information and the conditions under which information is released (Krattenmaker, 1973). Privilege protects the right of individual to form private loyalties (Italia, 2003).

Another rationale for granting privileges and immunities is such privileges and immunities allow the individuals to whom this information is disclosed to carry out their duties independently, without interference by others and without fear of retribution (OPCW, no year). Privileges also promote potential better individual care by professionals who serve the person when a complete disclosure is made (1 My and K 98, 39 Eng. Rep 618, 1833). "(P)rivilege(s) promote the creation of information that might not otherwise exist" (Saltzburg, no year). In the field of law it has been recognized:

> "It is a necessary corollary to the right of any person to obtain skilled advice about the law. Such advice cannot be effectively obtained unless the client is able to put all the facts before the adviser without fear that they may be afterwards disclosed and used to his prejudice."[41]

[41] Lord Hoffmann in R v Special Commissioner and another ex parte Morgan Grenfell and Co Ltd [2002] UKHL 21

Privileges also operate to protect information that was disclosed. By providing incentives in the way of duties and penalties greater assurance is available that the information entrusted to another for their care will not be disclosed. This protection furthers the incentive to disclose sensitive information. In effect, this places a control over the repository of information after the information is shared (right to control disclosed information) Ex Post effect – when provided information is released what are the harms of a particular case of disclosure or non disclosure (Saltzburg, no year).

The relationship entities and characteristics of the relationship

The protections of privilege privacy extend primarily to individuals but organizations and groups of people can fall under its protection as in the case where an organization seeks the services of an accountant or legal counsel. In each case the manner of information disclosure demonstrates the desire to keep the information private. The entity to which the information is disclosed must possess specialized training and expertise or at least the discloser must believe that entity possesses this expertise. It is not important that the information provided is necessary for the expert to act. It is only important that the information is provided to the expert in the hope it will assist the discloser. Often these relationships are limited in time and purpose specific.

Privilege is principally underpinned by Lockean philosophy. The decision to share information, to a person at a time and place is the prerogative of the individual solely. The holder of information determines whether to provide the information or not. Locke also maintained that the individual was not completely accountable to society - his accountability was limited only to essentials necessary for the administration of

society except in the case of where the individual is either a member of society's administration or some special ground exists why the individual should be accountable. The reason given for this is the keeping reasonable and limited the rights society holds over another person permits societal roles be constructed to allow considerable breadth to the individual to choose how they live (Benn, 1975). This has been represented as the capability to determine what one wants to reveal and how accessible one wants to be (Bellotti, 1998). This capacity enables the individual to sustain power, liberty and autonomy against potentially overwhelming forces (Nissenbaum, 1998). For privileged relations the public man of Locke sets the boundary where the person can shape the relationship. Up to that boundary person has complete access. Control over what is privileged and how privileged information can be disclosed and be used by third parties.

This accountability to society is what places the duty the person to whom information is disclosed to protect the information from access by others and ultimate protect the individual being identified by his information. Once information is disclosed, the entity to which privileged information owes a duty to protect this information from others. But the argument can be made that this is very Kantian in that a sanctuary must be created so that neither the person or his information is accessed or accessible. To encourage the decision to share a Kantian strict zones of no access to the person or to information about the person is imposed that provides the necessary sanctuary for the information to be shared.

3.1.2.2. Role characteristics in terms of control and access

3.1.2.2.1 For dissemination of information

There are three issues with respect to privilege privacy. First the individual has a right to share or not share information. This normally produces a duty in others to respect the information provider's choice and not access the information shared or to encourage the individual share information. However in privilege privacy certain type of information is of more value when it is shared, so society creates incentives for the individual that while invading that right produce value for both the individual and society when the information is shared.

A second issue is once information is shared, a duty of loyalty is owed to the sharing party to use the information for his benefit and not take advantage of the donor. Advantage is taken when the individual's information is used in ways not intended, used in a way outside the agreement of use or used in way to harm the individual. Often time this is expressed in the terms of a fiduciary duty, which is a duty of great care owed by the agent for the information entrusted by the principle. These duties are evaluated in terms of value for the donor of information and the anticipate harm that would befall should the information be misused.

A final duty of helping is owed by the agent toward the principal. Here the agent must act in a way that assists the principal. Here we evaluate the process not the outcome, asking was what was done at that point and time reasonable? Whether the trustee is prudent in the doing of an act depends upon the circumstances as they

reasonably appear to him at the time when he does the act and not at some subsequent time when his conduct is called in question

For privilege privacy at the time of initial disclosure the owner of the information has high control over his or her information. Once information is disclosed, the individual loses his control over the information but in its place a duty is placed upon the holder of information to protect the information. Additionally there is a broad and strong zone of low access to both the person and their information that must be enforced by the person to whom the information is disclosed.

3.1.2.2.2 For non dissemination of information

These are characterized by the individual being infirm requiring protection due to minority or the character and nature of the information is such that the information is out of the control of the individual and but for some type of control, the individual will suffer damage. Under these circumstances, strong protections of non access to the individual's information and to the individual are provided.

3.1.2.3 Character of information

This is personal information about the individual that is sensitive to the individual disclosing which in the hands of the wrong person can subject the individual to harm, embarrassment or ridicule. In the case where the information is encouraged most often the information's disclosure will embarrass or ridicule the person, but in may cases it can subject the person to harm such as when a person must disclose details of a crime to a lawyer to prepare for his criminal defense, or when an employer learns of a medical condition of his employee, the employee may be fired, demoted or passed

over for advancement. In the case where we restrict dissemination of information, it is almost always for the purpose of protecting the individual from harm although incidental to this it may also shield them from embarrassment or ridicule.

3.1.2.4 Representative Laws and Court Rulings

To encourage these types of disclosure, historically certain roles are designated as sanctuaries. Inside these sanctuaries it is possible for the individual to share their information and enjoy the protection that their participation in the role as they are aware their information will not be revealed. For this reason it has been stated: "When a claim of privilege is upheld so is the right of privacy" (Krattenmaker, 1973).

Historically, Elizabethian confidentiality existed to protect the honor and integrity of the gentlemen who held confidential information (Annesley v. Anglesea 17 St Tr. 1139 (1743). In 1562 an act in England make a universal duty to testify. [42] This act threatened confidentiality obligations of both the gentleman and the lawyer. With the enactment of this law, judicial search for truth could no longer be obstructed by voluntary pledges of secrecy. Judges of that time decided that legal communications formed a special category of exception to testify because of the importance of the client obtaining advice would be hindered by the clients fear of disclosure of his confidences.

[42] Act of Punishment of Such as Shall Procure or Commit any Willful Perjury See also Cobbetts State Trials 769. 788 (1612) ("(A)ll subjects, without distinction of degree owe to the king tribute and service not only of their deed and hand but of their knowledge and discovery"- Sir Francis Bacon) Prior to this act the opponent in a jury trial was not compellable to be a witness. Wigmore, J.H., A Treatise on the Anglo-American Law of Evidence, Mc Naughton Rev. Edn, Little Brown, Boston, Section 2217 at 169 (1961)

Since that date other privileges have been informally extended but the trend today is to codify these provisions through a formal law.

Examples of the type of privileges in existence today that enable persons to disclose information include: attorney and client (FS 90.502(2)), medical care giver (Florida Statute 456.057(2)), clergy and parishioner (Florida Statute 90.505(2)), psychologist or psychotherapist and their patient (Florida Statute 90.503(2)), accountant and client (Florida Statute 90.5055(2)), domestic violence advocate and the victim spouse (Florida Statute 90.5036(3)), sexual assault counselor and rape victim and family (Florida Statute 90.5035(2)).

The best known privilege is in the medical profession. Historically information provided by the patient to the doctor has been held in the strictest confidence. This tradition has eroded when medicine became a business, and the patient's information became a commodity that had to be exchanged with many persons, unrelated to the diagnosis and treatment of the patient. At times this information has been disclosed to others, or used in a manner detrimental to the patient. These reasons were a major justification for the enactment in 1996, of The Health Insurance Portability and Accountability Act (HIPAA). Justification for the HIPAA act centers on the premise that the provision of high quality health care requires the exchange of personal and sensitive information between the patient and provider (65 FR 82467 Published December 28, 2000). When the patient has high trust in the provider that the provider will protect this information, more information is provided to the medical provider by the patient. When the trust is low, the patient withholds information or fails to get

treatment. Health care professionals who lose the trust of their patients cannot deliver high quality care (65 FR 82468 Published December 28, 2000). Privilege in this way acts as a zone of no access. The zone of no access enables information to be brought into the open. This is the Ex Ante effect – To what extent does the privilege promote the creation of information that does not already exist (Saltzburg, no year)? A zone where information can be created when one in exclusive possession of certain information discloses and subsequently that information is explored.

Laws have been enacted to protect to protect children by limiting access to information about children (COPA)[43] access to certain types of information – Gramm-Leach-Bliley (protect consumer personal financial information held by a financial institution. The Family Education Rights and Privacy Act (20 USC 1232g) – which gave the rights to inspect, and get corrections to school records and a right to have information in school records not to be released unless certain circumstances are met. The Fair Credit Reporting Act and FACTA (Fair and Accurate Credit Transactions Act of 2003 and PL 105-159) additionally protect the credit information of individuals. Sarbanes Oxley was designed in part to protect the financial information of the individual from being disclosed.

[43] Childrens Online Privacy Act (COPA) – giving parents control over what information is collected about their children online and how much of that information can be used,

3.1.3 Intellectual Privacy

3.1.3.1 The purpose

The purpose of intellectual privacy is to promote the development of individual autonomy through self development and self expression.

When people are watched often time they attempt to conform to the watcher (COPA).[44] In these cases often they are inhibited and self conscious. Reiman states that "when you know you are being observed, you naturally identify with the outside observer's viewpoint, and add that alongside your own viewpoint on your action. This double vision makes your act different …" (Reiman, 1995). Reiman goes on to say: "To the extent that a person experiences himself as subject to public observation, he naturally experiences himself as subject to public review. As a consequence, he will tend to act in ways that are publicly acceptable" (Reiman, 1995).

Jed Rubenfeld noted one version of privacy focuses on protection-of-personhood and the second version on freedom from-normalization (Slobogin, 2002). The personhood version views the right to privacy as a means of ensuring individuals are free to define themselves. It protects against state interference in decisions that are "central to the personal identities of those singled out" (Rubenfeld, 1989). The anti-

[44] Shoshana Zuboff writes about the phenomenon of “anticipatory conformity" among persons who believe they are being watched.

normalization version, in contrast, focuses on the extent to which the government action standardizes lifestyles (Rubenfeld, 1989).[45]

Intellectual Privacy enables this self actualization to occur. This is achieved by the providing of a sanctuary that shelters the person from others. It is also achieved by as insulating from others the information about the information the person consumes. The purpose of the sanctuary permits the necessary growth and exploration by the individual to experience life as they desire and become an autonomous being.

There has not always been a respect over ones thoughts and feelings. Early Anglo-Saxon tradition readily recognized tangible right to land and property but largely failed to extend these rights to thoughts feelings and intellectual activity. This was changed in the post enlightenment period when thought gained respect and the individual's right over his or her thoughts and personality began to be given the respect formerly reserved only to bodily integrity and corporeal rights.[46] Still this recognition was of a limited basis until the writing of Brandeis and Warren in 1890 when they proffered that ones thoughts, emotions and sensations should be protected by privacy and made the argument that the law should expand its recognition of an individual's

---

[45] Rubenfeld ("The point is not to save for the individual an abstract and chimerical right of defining himself; the point is to prevent the state from taking over, or taking undue advantage of, those processes by which individuals are defined in order to produce overly standardized, functional citizens."). Its purpose is guard against a particular kind of creeping totalitarianism, an unarmed occupation of individuals' lives. That is the danger of which Foucault as well as the right to privacy is warning us: a society standardized and normalized, in which lives are too substantially or too rigidly directed. That is the threat posed by state power in our century. @ 784

[46] See Georg W.F. Hegel, *Philosophy of Right* (T.M. Knoz trans. 1942) (1821), Immanuel Kant, *The Metaphysics of Morals* (Mary Gregor ed. And translator 1996)(1797), John Locke, Two Treatise of Government,(Peter Laslet ed., 1988)(1690)

interest in his "inviolate personality" (Brandeis and Warren, no year) and forbid others to intrude upon a person's thoughts, emotions and sensations.

Individuals need this inviolate personality to develop their autonomy in thought and action and become autonomous individuals. This is goal of intellectual privacy. The autonomous person does not appear but is a developed being that possesses:

> "(the) strength of mind to resist the pressure to believe with the rest, and has the courage to act on his convictions. He is the man who despises bad faith and refuses to be anything or to pretend to be anything merely because the world casts him for the part. He is the man who does not hesitate to stand and be counted" (Benn, 1975).

Autonomy is a developed trait. In order to be autonomous individuals require a place where they can go and explore outside the gaze of others. This is because when under the watchful eye of another person or entities, a person is often stifled in their development. Philosopher Stanley Benn stated:

> "… we need is the freedom to be something else – to be ourselves to do what we think best, in a small protected sea, where the winds of opinion cannot blow us off course. We can not learn to be autonomous unless we can practice independent judgment" (Benn, 1975).

To become autonomous, we need a private inner life (Reiman, 1995). To develop this character requires a sanctuary and a retreat (Benn, 1975). The private retreat is "a private sphere of some sort to enable the recollection of self that makes self-presentation possible even if, in the end, the ideas that we develop and affirm are the same as those of our peers" (Austin, 2003). This retreat must insulate the individual

from the outside and withstand pressures imposed from without. There must be preserved in each individual a sphere of privacy that will allow his personality to bloom and thrive (Long, 1967) and respect a person's right to his own thoughts.

When we are on display we are unable to form our opinions and say that they are ours. The ability to develop ourselves and determine our being, to be distinct individuals and have an authentic inner life (Austin, 2003) is a value of intellectual privacy. In this sense intellectual privacy protects our ability to act and think in unpopular ways; explore self and ideas. It protects individuality understood in terms of our ability to be different, even eccentric (Blouston, 1962).[47] It enables us to form our own person and to become what we want to become. Privacy is also seen as an essential practice for the formation of a conception of self. .It enables us to find within ourselves the resources for better views which in turn improve life itself (Reiman, 1995). Intellectual privacy promotes for the individual these abilities and attributes by providing a zone of no access to three areas: the individual, the place he or she occupies and the information that is consumed

Individual autonomy is valued by our society. A society of autonomous individual help ensure a functioning, viable democratic society as opposed to an autocratic society where the individual simply accepted the edicts from above.

> The liberal vision is guided by the ideal of the autonomous individual, the one who acts on principles which she has accepted after critical review rather than simply absorbing them

[47] "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass."

> unquestioned from outside. Moreover, the liberal stresses the importance of people making sense of their own lives, and of having authority over the sense of those lives. All this requires a kind of space in which to reflect on and entertain beliefs, and to experiment with them – *a private space*. Deeper still, however, the liberal vision has an implicit trust in the transformational and ameliorative possibilities of private inner life. Without this, neither democracy nor individual freedoms have worth. Unless people can form their own views, democratic voting becomes mere ratification of conventionality, and individual freedom mere voluntary conformity. And, unless, in forming their own views, people can find within themselves the resources for better views; neither democracy nor individualism can be expected to improve human life" (Reiman, 1995).

The development of this autonomy in the individual is a key by product of privacy.

The value of such off limits activity has demonstrated itself in studies involving individual creativity where findings were made that creativity is most evident where the person has more leeway to develop.

3.1.3.2 The relationship entities and type of relationship

The typical entity entitled to the protections of intellectual privacy is the individual. The entities the individual is protected from are organizations and society itself.

Organizations and Society are permitted no relationship with the individual when intellectual privacy is claimed. This is accomplished by providing no access to the individual and no access to information regarding the individual.

Philosophy Type

Intellectual privacy embraces the concept proposed by Kant - the ideal of an independent minded individual whose actions are governed by principles of his own

that he accepts as rational (Benn, 1975). These individuals form their principles “after a critical personal review rather than simply absorbing them unquestionably from the outside” (Reiman, 1995).

3.1.3.3 Role characteristics of Intellectual Privacy in terms of control and access

For optimal results the individual should have high control over the information that is viewed, high control over the place the information is viewed and high control over when it is viewed. In a line of cases characterized by freedom of speech cases, the Communications Decent Act of 1996 (ACLU v. Reno 521 U.S. 844) and Children’s On Line Protection Act (ACLU v. Ashcroft (2004)) were declared unconstitutional. A major reason for these decisions was the restriction in the free flow of ideas and the specter of censorship which threatened the individual’s to access to information ultimately hindering the ability of the individual to develop his or her intellectual self. Due to changes in information capture, aggregation and transfer, and advancements in digital rights management where the holder of the digital right can direct the amount, person and time and place of access individuals and even identify the persons, place and type and amount of access individuals have no or little control over the information they seek in some areas. Awareness that being placed under the gaze of others would produce a chilling effect upon the consumption of some material has produced a number of laws that declare as safe havens that enable patrons to access material freely. Such places as the library, video rental and cable use and pay per view are now subject to laws that restrict access to others of who frequents and what sources are viewed by their patrons This creates a zone of no access to information about the person.

In terms of access to the person a very limited access to the person in his home and access to his papers and effects has been strongly supported[48] creating a strong and strong zone with low interference from others. This would also include access to the thoughts and emotions a person has as a result of such access. Protections exist that are well established that provided others should have no access to the place were information is viewed, consumed or digested including any notes, papers and effects or acts that occur as a result of such access.

3.1.3.4 Character of Information

Intellectual privacy information involves information about the information that the individual is viewing which includes the circumstances of access and how often the information is accessed. This would include among other things what was accessed, the nature and character of the information, where the information was obtained, the time, place and manner of viewing and digesting of this information, what is being done with the information, how the information is being interpreted, used and acted upon and how often the information is accessed. In some limited cases it can be extended to restrict information regarding who the individual associates with (Roberts v. United States 468 U.S. 609).

[48] See Fourth Amendment to the U.S. Constitution which holds a person should be secured in their houses, papers and effects and the Fifth Amendment which reflects the Constitution's concern for the right of each individual to a private enclave where he may lead a private life – see Tehan v. Shott, 382 U.S. 406 @ 416

3.1.3.5 Representative Laws and Court Rulings

Both the Fourth and Fifth Amendment to the United States Constitution recognize the importance of a private place. The Fourth Amendment provides that persons should be secure in their houses papers and effects. The U.S. v. Katz case extended the protection beyond the home and beyond tangible items to include any place where a person held a reasonable expectation of privacy and extended the protection beyond tangible items such as papers and effects to include intangible items such as conversations. A year later in the Terry v. Ohio (392 U.S. 1 (1968)) the court built upon the Katz ruling. In addition to the protections in Katz that the Fourth Amendment is a right for a person "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, (which) shall not be violated . . . ." and is also

> "… a right of personal security (that) belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. No right is held more sacred, or is more carefully guarded, by the common law than the right of every individual to the possession and control of his own person, free from all restraint or interference, unless by clear and unquestionable authority of law"

Later in the case of Tehan v. Shott (382 U.S. 406, 416) the 5th Amendment was interpreted as reflecting the Constitution's concern to provide the right of each individual to "a private enclave where he may lead a private life."

Each of the following acts are designed to protect the individual by providing barrier from which others cannot identify what material the individual is sampling.

Video Privacy Act (18 USC 2710) forbids any video rental company from providing records of people and the videos rented outside those needed for internal control of stock. This was enacted in response to an uproar on capital hill when the video records for Clarence Thomas were subpoenaed and obtained showing the rental of a number of pornographic videos. The Cable Communications Policy Act (47 USC 521 et seq.)[49] forbids cable providers from providing to outsiders the type of cable service a subscriber has as well as what type of shows are rented on pay per view. The American Library Association adopted a Library Bill of Rights (ALA, 2002) that affirms the ethical imperative to provide unrestricted access to information and to guard against impediments to open inquiry recognizing "When users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists." Florida has adopted the Library Confidentiality Act (Florida Statute 257.261) which makes library registration and circulation records private and imposes penalties for their violation. The United Supreme Court on two separate occasions struck down.

3.1.4 Secret Privacy

Secret privacy promotes the engagement of others in cooperative activities that protect or advances the well being of others.

3.1.4.1 The Purpose

Information privacy has long been recognized as important in the business world. For the business, customer lists, work allocation techniques, business process,

[49] Restricts the collection, maintenance and dissemination of subscriber data. Forbids cable providers from releasing information about the subscriber. or from collecting personal identifiable information.

product formulation, names of key employees or anything that provides a business a sustainable competitive advantage are business secrets. These secrets require privacy protection as they enable the distinguishing of businesses one from another, often provide for competitive advantages, provide motivation for innovation, produce better products and are ultimately what produces profit for the business.

Trade secrets are also important for society as well. Certain business information becomes beneficial to society, producing a greater societal benefit when it can remain secret. In general competitive markets tend to produce homogeneous products with business sustaining profits near their margin. A differentiation of product will not only potentially produce greater profit margins for the firm, it also produces greater utility benefits for the consumer as the consumer receives a product it wants, not one it must make use of. A second benefit is both the increased availability of a desired product and increased employment opportunities as employers hire more people to produce it products. There is a also a benefit of information not being lost by the death of the holder of the secret, frailty of mind, or misplacement of secrets. By permitting secrets to be disseminated coordinated strategies can be engaged. Better ideas, products, processes and strategies that are based upon secrets can be realized when you can disseminate the secret to those on the project and engage their minds more fully into the project. The secret can also become more valuable through its dissemination when others with knowledge of the secret can develop the secret itself.

The Brookings Institution estimates that “at least 50 percent, and possibly as much as 85 percent” of the value of American companies is attributable to intangible

assets such as trade secrets (Blair, 2000). Trade secrets are rapidly becoming the intellectual property of choice due to their advantages in the information economy. In the Information Age, trade secret protection is better suited to the fast-moving and non patentable confidential information needed to run our companies.

Trade secrets protect “secrets of the business” from being discovered by outside parties despite the fact they are communicated to members or customers of the business. The purpose of the trade secret is to promote licensing and exchange of non patented know-how between businesses and employees (Dratler, 1991). It has a secondary purpose to prevent improper means to obtain secrets (E.I. DuPont de Nemours and Company v. Christopher, 431 F 2d. 1012 (5th Cir. 1970)) such as breaches of contract and confidential understandings (Samuelson, Pamela Privacy as Intellectual Property? 52 STAN. L. REV. 1125 (2000)).

3.1.4.2 The relationship entities and character of the relationship

In secret privacy, the entities which can possess a secret can be an individual or an organization or a society. Any secret disclosed can be to either an individual or an organization or both. The person against whom the secret is held can be another person, organization or society.

The relationship is often a voluntary relationship created between the parties. In the case where the secret benefits a society often times governments impose the duty to maintain the secrets.

3.1.4.3 Philosophy type

Lockean type philosophy with the principle difference being not only is the individual is free from societal control but also that society gives the individual additional power than others with in society to control who, what and when information is available and accessible.

3.1.4.4 Role characteristics in terms of control and access

Initially the holder of information has high control over all phases of the information (what information, when and to whom). By virtue of this control the holder creates a situation where the information is not accessible to other. In many cases access to the person is not important (unless the person is the information or holds the information) as what is important is access to the information. When the relationship is formed and information is disclosed to third persons, the initial high control yields to a situation where the discloser now has low control over the information disclosed. Once disclosed, the entity to which information is disclosed is granted a conditional license that permits them access to the information and liberty to use the information subject to them the duty of using the information for the owner's self advancement. A duty is also imposed upon them to protect this information from others in most cases even after the relation between the parties has ended. This role creates a high access to information to those within the relationship enabling the relationships purpose to be fulfilled and perpetuates the low access to information for those outside the relationship.

3.1.4.5 Character of information

Secret information can be any information that permits a person or an organization or a society an advantage over another person, an organization or a society because of the possession of the information. This is generally confined to information that is not readily available to others and was originally conceived as the result of effort, study, expertise, experimentation. This information is contextually valuable but outside this context it has no value. Thus secret information has an audience targeted where the information is not to be disclosed. Secret information is information that is neither readily available nor common knowledge to that audience. The character of this information provides the holder of the information an advantage over a defined audience. The value of the information remaining secret is important to the holder of the secret as it is necessary to the holder to serve his selfish purposes.

Representative Secret Information includes the secret formula for Coca Cola, How to the U.S. has organized its national defense, Computer algorithms, how a business has a competitive advantage.

3.1.4.6 Representative Laws and Court Rulings

Trade secrets and information privacy receive slightly different treatment under the law. What distinguishes modern trade secret law from the current state of information privacy law are the procedural and substantive ways in which these issues were addressed in their development. Information privacy is concerned about concealment and control over information. It has as its basis the secrecy paradigm that

views privacy as concealment and control. Trade secrets are based upon the Relative Secrecy Doctrine. This recognizes at times a secret must be disclosed yet provided protection as a secret. A comparison of the Secrecy Paradigm and the Relative Secrecy Doctrine shows the similarities and differences.

The relative secrecy doctrine while it applies to trade secrets, reflects a fact of life that is equally applicable to personal information: we live in a social and interactive community. Since we must engage with others, there are situations in which personal information must be shared. As explained by Daniel Solove:

> "Life in the modern Information Age often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world" (Solove, 2002).

Comparison of Secrecy Paradigm with Relative Secrecy Doctrines	
Secrecy Paradigm	*Relative Secrecy Doctrine*
Privacy is about concealment and control	A secret remains a secret even when it is unconcealed and out of the control of the owner, so long as it hasn't escaped into the mainstream of public knowledge (Pooley, 1975). It is information not generally known or relatively ascertainable even if it is known by multiple individuals or companies (Pooley, 1975). Trade secret owners are not required to exercise all possible efforts to protect the secrecy of their information, but instead only those efforts that is "reasonable under the circumstances" (Uniform Trade Secrets Act § 1 (amended 1985)) "Limited disclosure" in the context of certain relationships does not destroy the trade secret status of information (Stedman, 1962). The extent to which the law will recognize legal rights in the originator will depend upon the circumstances of disclosure (Stedman, 1962).

Privacy is invaded by accessing the person or confidential information and/or exercising a public disclosure of confidential information against the originator's will	A violation occurs when trade secrets are improperly accessed, disclosed or used. Legal protection for trade secrets does not cease when information is disclosed to another. When trade secrets are disclosed by the trade secret owner to serve his purposes, it is generally recognized that an implied duty of confidence arises that (1) prevents the information from losing its trade secret status and (2) renders the subsequent disclosure or use of the information improper (Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d. 1195 (5th Cir. 1986)).
TEST Is there a reasonable expectation of privacy	TEST It is contextually based upon the relationship between the parties. A confidential relationship generally arises by operation of law from the affiliations of the parties and the context in which the disclosures are offered (Burten v. Milton Bradley Co., 763 F.2d 461, 463 (1st Cir. 1985)). In general, the closer the relationship, the easier it is for the trade secret owner to prove that he undertook reasonable efforts to protect his trade secrets. Such relationships are not limited to express or implied contractual relationships but can include any relationship in which a duty of confidence can be implied (Pooley, 1975).

Table 8 Comparison of Secrecy Paradigm with Relative Secrecy Doctrines

Dratler points out that the purpose of trade secrecy law is to promote licensing and the exchange of non patented know-how between businesses and employees and as such the privacy requirement in trade secrecy law is not the absolute privacy required in information privacy but relative privacy (Dratler, 2001). Sandeen defines relative privacy as a state of secrecy that is not "absolute" (Sandeen, 2006). Still, the trade secret must be a secret to some degree. The UTSA defines a trade secret as a condition where information is not generally known or readily ascertainable (Uniform Trade Secrets Act § 1 (amended 1985)). As explained by Roger Milgrim, the phrase

"generally known" means "well known" or "commonly known to the trade in which the putative trade secret owner is engaged" (Milgrim, no year). In trade secrets "Absolute" secrecy would be illustrated, at the extreme, by being known to only a single individual, but a trade secret can be known by the employees of the owner. In this case we employ "absolute secrecy" to denote matter known to only one enterprise and "relative secrecy" to denote that matter may be known to more than one competitor in a trade or industry, but not to all (Sandeen, 2006). Regardless of which definition is used, once it is determined that information is not absolutely secret, the degree of secrecy that is required to maintain information as a trade secret must still be determined (Milgrim, no year). While the term "relative secrecy" is not used in the UTSA, the concept that information can be shared among a small group of individuals or companies without losing its trade secret status is reflected in a number of its provisions.

Trade secret owners are not required to exercise all possible efforts to protect the secrecy of their information, but instead provide only those efforts "reasonable under the circumstances" (Milgrim, no year). The disclosure of information can give rise to the claim that the information was not intended to be a secret and could be used by the person or entity which received the secret. Thus the person to whom information is disclosed is a factor to consider in determining both whether a trade secret exists and whether there was a misappropriation (Milgrim, no year).

One of the ways that the relative secrecy doctrine is applied in practice is by paying attention to the relationships that exist between the trade secret owner and the persons to whom information is disclosed as in some relationships the disclosure of

information imposes a duty to keep the information disclosed, confidential (Protection and Use of Trade Secrets, 64 HARV. L. REV. 976 (1951)). Generally, the closer the relationship, the easier it is for the trade secret owner to prove that he undertook reasonable efforts to protect his trade secrets and in those cases where it is evident there is a confidential relationship and secrecy is strong courts have even relaxed the requirement for reasonable precautions (Pooley, 2004). Such relationships are not limited to express or implied contractual relationships but can include any relationship in which a duty of confidence can be implied (Sandeen, 2006). The relationships that have given rise to a duty of confidence include the employer/employee relationship,[50] the relationship between purchasers and suppliers,[51] the relationship between a licensor and licensee,[52] and the relationship between partners and joint venturers.[53] They also include more attenuated relationships, such as those between a trade secret owner and a prospective licensee, (Nilssen v. Motorola, Inc., 963 F. Supp. 664, 683 (N.D. Ill 1997)) the seller and purchaser of the business[54], and between an inventor and a prospective manufacturer of an invention (Sylmark Holdings Ltd. v. Silicone Zone Intern. Ltd., 783 N.Y.S.2d 758 (2004)).

---

[50] See, e.g., In re Matter of Innovative Constr. Sys., Inc., 793 F.2d 875, 883 (7th Cir. 1986); Elm City Cheese Co. v. Federico, 752 A.2d 1037 (Conn. 1999); Junker v. Plummer, 67 N.E.2d 667 (Mass. 1946); Extrin Foods, Inc. v. Leighton, 115 N.Y.S.2d. 429 (1952); Macbeth-Evans Glass Co. v. Schnelbach, 239 **Pa.** 76 (1913); and Christopher M's Hand Poured Fudge, Inc. v. Hennon, 699 A. 2d 1272, 1276 (**Pa.** Super. Ct. 1997).

[51] See, e.g., Curtiss-Wright Corp. v. Edel Brown Tool & Die Co., 407 N.E.2d 319 (Mass. 1980).

[52] See, , e.g., Hyde Corp. v. Huffines, 314 S.W.2d 763 (Tex. 1958).

[53] See, e.g., A.L. Labs, Inc. v. Philips Roxane, Inc., 803 F.2d 378, 381 (8th Cir. 1986).

[54] See, e.g., Phillips v. Frey, 20 F.3d 623, 631 (5th Cir. 1994); Tri-Tron Int'l v. Velto, 525 F.2d 432, 435 (9th Cir. 1975); Heyman v. AR. Winarick, Inc., 325 F.2d 584, 587 (2d Cir. 1963); Den-Tal-Ez, Inc. v. Siemens Capital Corp., 566 A.2d 1214 (**Pa.** Super. Ct. 1989).

The locus of trade secret law is in the behavior of the non-owner and not the trade secret (Samuelson, 2000). When trade secrets are disclosed by the trade secret owner to serve his purposes, it is generally recognized that an implied duty of confidence arises that (1) prevents the information from losing its trade secret status and (2) renders the subsequent disclosure or use of the information improper (Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d. 1195 (5th Cir. 1986)).

The modern definition of trade secret encompasses any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.[55] Trade secrets can be information, including a formula, pattern, compilation, program, device, method, technique, or process.[56] It is an idea, a physical device, a confidential practice, process, design, or compilation of information such as a customer list or marketing information used by a company to compete with other businesses (Elias, 1998). It is also referred to in some jurisdictions as confidential information. Approximately 40 states have adopted a model law called the Uniform Trades Secrets Act.[57] These types of acts discourage the dissemination of Trade Secrets through the entitlement of damages and injunctions. They also provide protections over the trade secret during the litigation process. Trade Secret protections are offered both in the United States and

---

[55] Restatement of the Law (Third) Unfair Competition § 39 (1995) The two primary requirements are (1) that the information not be generally known in the trade and (2) that the trade secret holder take reasonable measures under the circumstances to protect the information as a trade secret. See generally, Uniform Trade Secrets Act, § 1(4) (Definition of a "trade secret").

[56] California Civil Code 3426.1d, see also Florida Statute 90.506

[57] National Conference of Commissioners on Uniform State Laws, Uniform Trades Secrets Act

many foreign countries (Taiwan Trade Secret Act, 2005). Federal laws also protect the disclosure of trade secrets in open meetings of agencies (5 USCS 552b).

Frequently companies will require employees to sign non disclosure agreements as a condition of employment in order to protect these trade secrets. These agreements are also known as a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement. The purpose of these is to create a confidential relationship between the parties. These have been found to be a legal contract between parties and proven effective as a means to protecting trade secrets or protect any information under a trade secret.

In Florida and other states contracts which restrict the exercise of a profession trade or business are valid (Florida Statute 542.33(1)) and even extend to employment contracts (Sentry Insurance v. Dunn 411 So. 2d. 336 (5DCA 1982)). This restriction also encompasses the situation where a person sells the goodwill of a business, or any shareholder of a corporation selling or otherwise disposing of all of her or his shares in said corporation (Florida Statute 542.33 (2) (a)). Federal courts also uphold employment contracts and covenants not to compete when a state law provides such sanctions (KV Pharm. Co. v Harland (In re Harland) (1999, BC ED Pa) 235 BR 769). Because of the potential effect of forbidding a person to ever gain employment in an area of expertise, the employee is reasonably restricted in terms of place, geography and time of future employment should the parties dissolve the relationship.

Other uses of these agreements are made when discussing the possibility of a joint partnership or the licensing of a patent by either party. These non disclosure

agreements are used between companies as well particularly when discussing or pursuing a joint venture. These agreements are extensively used in the United States, Europe and Asia. One well known agreement was between SCO and IBM where both companies agreed to jointly work on a project keeping trade secrets disclosed during the course of the relationship secret.

Another significant development in the protection of trade secrets is the Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839), which makes the theft or misappropriation of a trade secret a federal crime. This has reach not only in the U.S. but also has international repercussions as well. This law contains two provisions criminalizing two sorts of activity. The first, 18 U.S.C. § 1831(a), criminalizes the theft of trade secrets to benefit foreign powers; the second, 18 U.S.C. § 1832, criminalizes their theft for commercial or economic purposes. As defined in the Economic Espionage Act of 1996, the term trade secret refers to all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

- The owner thereof has taken reasonable measures to keep such information secret, and;

- The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.

Some secrets are protected due to the need to protect one society from another. MIT professor Phillip Zimmerman was placed under investigation for violation of the Arms Export Control Act (22 USCA 2778) after his PGP algorithm was placed on the MIT server and made accessible to the general public. This act which places authority in the President of the United States to control the export of defense articles and services is used as a way to keep technology, information and knowledge out of the hands of undesirable nations and people as a way to ensure the national defense.

3.1.5 Transitory Privacy

3.1.5.1 The purpose

Transitory privacy is information available in public or public places that can compromise a reasonable person's privacy expectations. The purpose of transitory privacy preserve public space as a place of expression as well as preserve traditional notions of privacy, private information and private space

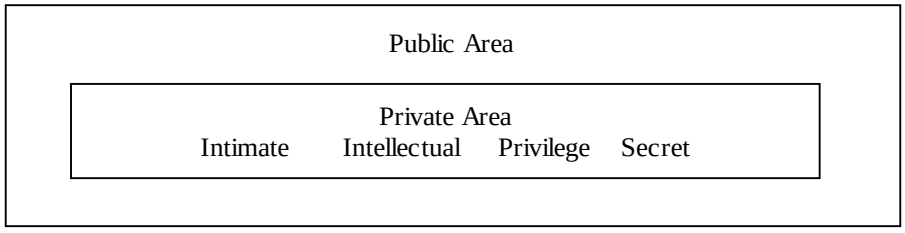

Figure 11 Purpose of Transitory Privacy

People are required conduct at least a portion of their lives and their business in public space in the public eye. We work with others, we walk and talk to others, purchase items at the store; we travel to places from our home on public highways and sidewalks – all without the thought of someone watching and recording our actions. Public space appears as a zone of complete access. Entities in public don't have a place to hide: everything done or said is readily available for others there to observe, hear or record. Other than the limited duties of don't stare, don't stalk, and don't take notes there were few formal duties to respect privacy in public.

Before the adoption of information technology by the public, public spaces despite being open and observable, were very private. Public privacy was "well enough protected by a combination of conscious and intentional efforts (including the promulgation of law and moral norms) abetted by inefficiency in the ability to collect, store and use information (Nissenbaum, 1998). Public spaces provide both low access to the entities in public space and to the information about those entities. This was due to the inability to efficiently monitor, collect information and aggregate the information in public space. Thus entities managed to be in public and keep his or her public life, private because of the inability and high cost to access, capture and aggregate public information. When conscious efforts are necessary private affairs in public spaces were managed easily on a moment by moment basis by behaving in a manner that is appropriate to the setting (Bellotti, 1998). This supplemented information stealth.

Technology has and is fundamentally changing the nature of surveillance (Schneier , 2004*)* as it enables the detection and chronicling of all activities in public

space. Since key developments in information technology have allowed the penetration of public space and collection and analysis of information about people, a problem of privacy in public now exists (Nissenbaum, 1998). Privacy, private information, private space is defined by what places are private, what the appropriate access to those places is and what information is private. These areas were delineated and constructed taking into account the availability and non availability of information in the public realm. By its very definition private places, access to those private places, private information and access to private information means this is not available or accessible to any entity except by those in a private relationship. When public space changed due to the use of information technology, access to private places and information increased to the extent that they were no longer private but part now of an accessible public space. Thus because of the change in the character of public space – the character of private space changed.

A change in the public space brought about by the ability to detect and mine the information that previously was private has changed our ability to protect traditional private places and private information in turn causing discord because assaults mounted on our changing definition of privacy. From information gathered from public sources law enforcement have been able to discern illegal activities that take place in private. By way of example, through surveillance law enforcement can discern the growing of marijuana inside the home through the purchase of specialty lights and fertilizers. It can conclude that the manufacture of moonshine is occurring through the purchase of corn and other ingredients indicative to its manufacture. In the law enforcement community

the fact is well known: The aggregation, collection and use of information gleaned from public sources can and will expose activities conducted in private places. To protect private spaces is one reason search warrants are mandated. When we are unable to protect transitory privacy, we are unable to protect any privacy.

In addition to the ability to detect action occurring in private spaces, private activities conducted in private areas can be influenced from the monitoring of public spaces. Using the examples above, once the activity that violates the law is detected, law enforcement can effect a change in the activities conducted in private areas though interventions such as arrests and the publications of such arrests to alert others of the non tolerance. This abuse is so wide spread that Schneier among others has called for mechanisms to prevent abuse and hold people accountable that the new techniques don't place an unreasonable burden on the innocent (Schneier, 2004).

However this type of intrusion is not limited to illegal activities and could be extended to socially acceptable activities, such as what books are read or DVDs are watched, what are the natures of the secrets of the firm which are protected by intellectual and secret privacy. This has a direct effect on the different forms of privacy. Intellectual and Secret privacy depend upon barriers being respected. The capture of information in public allows these barriers to be penetrated. Relational and privilege privacy are relationship based. When private spaces can be invaded from without these types of relationships are affected. Relationships are not formed due to fear. Relationships are altered due to intrusion. Relationships are created with unintended third parties either through direct or indirect influence on the relationship by use of

information captured in the public domain. What a person does in private could be seriously influenced by those in possession of this information.

3.1.5.2 Character of information

Transitory privacy involves information in the public domain. This information can be either private information (relational, privileged, intellectual or secret privacy type) or non private information. For this later information to be transitory privacy information it must have the character that if captured, possessed and utilized in a certain manner, it can lead to a breach of traditionally held privacy or can affect a socially unintended change in those values.

3.1.5.3 The relationship entities and type of entities

One group of entities is responsible for change. In this group is Society through it processes of social interaction. Another in this group is technology which through technological determinism effects a change. The final is either an individual or single entity (such as an organization) or group of individuals or entities who attempt to effect change. At times individuals or entities will use technology to effect change. The other group is the same entities of the various forms of privacy.

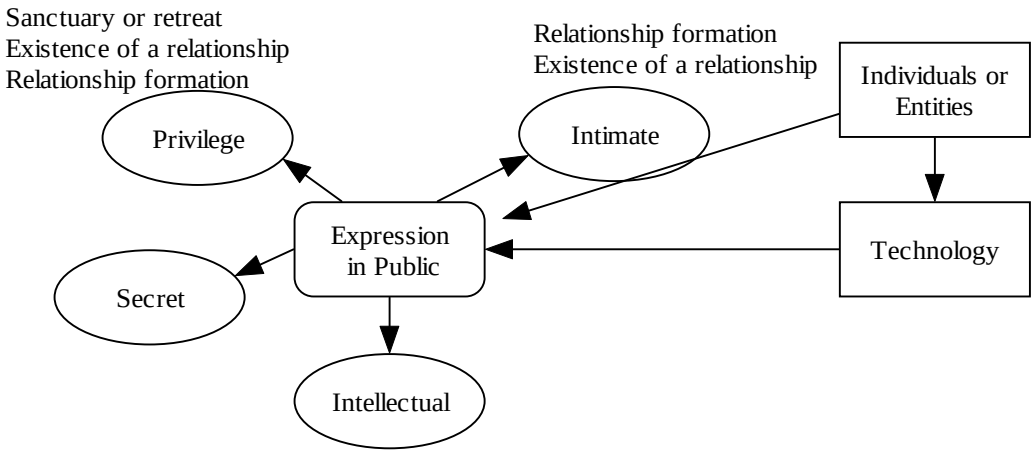

Figure 12 Transitory Privacy's Effect on Intimate, Privilege, Secret and Intellectual Property

The second group is the entities of the various privacy types that are affected by the efforts of change of the first group.

3.1.5.4 Philosophy type

Transitory privacy is underpinned on the Lockean principles of a separation of private and public life. The difference between transitory privacy and the other types of privacy is the impact. When public space permits an invasion of private life it will impact uniquely on each type of privacy as each privacy type protects a particular sphere of individual life.

3.1.5.5 Role characteristics in terms of control and access

In a well structured society, the values and practices of the society are a reflection of its member's. A society's chief role is to define, construct, protect and change its values.

3.1.5.5.1 Define

Society must define its requirements. These requirements are its values and the practice to achieve its values. In a well structured society, the values and practices society must be socially defined from the individual members and entities with in that society. They are an aggregation of individual and entity desires, opinions and beliefs of what is right, important and just. Society must halt an individual, an entity or an outside influence from defining, constructing, changing and imposing upon society values and practices that are not the will of society's membership and must ensure that these processes are engaged by the entire concourse of society. With privacy values must reflect the aggregation of individual and entity desires, opinions and beliefs and not be the product of an influential group or individual or an outside influence such as a technology that transforms society in ways not desired by its members.

3.1.5.5.2 Construct

Once defined, the values and practices of society are constructed by being ascribed into congruent laws and norms that supplement and support these values. These laws and norms encapsulate relationships and impose these relationships on societal entities defining acceptable roles for society's members. These laws and norms place entities on notice of the expectations of the society. In the case of privacy values and norms these dictate the following: What access to the person is permitted and what access is not permitted? What information about the person is knowable and once known what information is capable of being shared? What degree of control does the individual have over their own information and the information of others? A secondary

role is to ensure that the values and practices that are ascribed into law and norms actually supplement and support the values of society and are flexible to be applied to the various events occurring and allow change.

3.1.5.5.3 Protect

All relationships are ultimately created by the entities within society. These entities determine their choice and form of relationship. Society sanctions and even encourages certain relationships through its laws and social norms. Society desires relationships that are supportive of societal values. Society discourages relationships that are antinomical to societal values. This influence is important to be present for the following reasons: Society exerts influence over the formation and evolution of relationships for the purpose of protecting and ensuring its values. Society supports relationships that support and advance the values of society's entities. Other relationships are enacted and sanctioned to re-direct behavior along socially acceptable pathways. Conversely disincentives are also provided by society on those undesired relationships and behavior to discourage behaviors. These influences are accomplished through laws and social norms. Nevertheless despite this influence, relationships at least in the United States are the result of intentional deliberate autonomous acts of its members and at times, society oversteps its bounds.

Transitory privacy provides the structure that ensures the values a society reflects are its member's values. Transitory privacy does so by ensuring that the relationship process proceeds according to the autonomous, desired values of the relaters and enables them to consider and choose to form and develop desired

relationships. It accomplishes this through the maintenance of traditional rights of control and access in public space which thwarts the outside influence on the relationship process.

Society is constructed through relationships which require specific information. Privacy is a relationship that is constructed through specifications of controls over what, when to whom this information is available as well as specifications over whom, what and when access to the entity or information about the entity is permitted. When privacy and private places are constructed it is done in the context of public spaces. Traditionally some of this information was available in public, but it was not easily or readily accessible nor was it economically feasible to utilize. When changes occur in the ability to control and access public space changes occur to private places and to privacy itself change. Transitory privacy protects traditional control and access in public and private places. This operates as an important protection safeguarding relationship formation which ensures member entities can obtain the values they desire. This also ensures social values reflect the values of society's member entities.

A society must make obtainable to its members both those values sought by and promised to its membership (Lessig, 1999). One such value is the ability to autonomously form relationships (Gavison, 1980). Every societal entity forms relationships. An entity permitted autonomous choice and the ability to assert his or her will can obtain the relationships it desires on the terms desired. Society must provide a structure where entities can make autonomous choices in their relationships free from influences of others (Gavison, 1980). Part of this autonomy is the entity's ability to

assert its will and choose when they seek and how they develop relationships (Westin, 1967). That ability to assert the will must be provided even if the desires of their will are personally destructive, an irrational choice or results in less than optimal end result (Inness, 1992).

A society's values also need to be a reflection of the values of its member entities. Entities can not obtain a society that reflects their values unless they can actually realize and obtain their values. Transitory privacy ensures both the values of willfully forming valued relationships autonomously and the value that societal values reflect values of its membership. When an entity from outside a relation can influence a relationship, the relationship no longer reflects the relater's values. Instead the relationship reflects, at least in part, the values of the entity that influenced the relationship. When society seeks to reflect the values of its member in its values it will account for this influence through the sum of the relationships created and capture it as a member value when in fact it is not as this societal reflection will reflect not only the member entity's values but also the influencer's values. *Additionally the outside influencer by the very nature of being able to capture and use information to influence a relationship has formed a relationship with the entities negating their ability to willfully form a relationship.* Therefore it is important that society assure that relationships are constructed willfully and autonomously reflecting the desired values of the relaters. To do this society must thwart unintended and unwanted relaters from forming relationships with its members and influencing the relationship formation process.

3.1.5.5.4 Change

Nothing remains the same. As a result change must occur yet be managed. There are at least two changes society must manage. The first is an orderly change in privacy values. The second is that the change in privacy values is initiated by society and its corporate membership body and not imposed upon them through a powerful entity, individual or group of individuals thrust upon the society through a powerful outside force.

3.1.5.5.5 Orderly change

Society has the role to that changes adopted are incorporated into society in an orderly fashion, minimizing the disruption of its citizen's lives. In a sense societies harness change as change is interpreted in the context of existing laws, norms, relationships and roles. It is debated is the change a benefit or a detriment? Efforts are extended to accept beneficial change and discourage detrimental change. Not all change is debatable. Some change is thrust upon society and the debate must occur even while the incorporation is occurring. Humans change slowly. Rapid change brings confusion and unrest. This is true when values change – particularly when privacy values change. The change in societal values often occur over the period of many years with most value changes taking place in a time no less than one generation.[58]

Change is initiated by society and its members, not a minority or an outside influence

[58] Quote Norris where they look to generational changes in values

A role of transitory privacy is to ensure that changes in values must be initiated by the members of society along the lines desired by the members of society and not dictated by a technological imperative or an influential minority.

Ensuring that technological advancement is examined, embraced and assimilated into the societal network with a minimum of disruption is an important role of society. Challenges exist to create a balance between the avoidance of technological determinism where society is changed as a result of the technological advance and alternative of resisting all change by not adopting the technology.

Technological advancement and change often advances a society's well being. Technological advancement enables more work to be done or to enables the same amount of work to be done more effectively and efficiently. Technological advancement offers changes to everyday life that increases the enjoyment of what life has to offer. Technological changes in the information technologies have enabled the cost of information gathering, storage and transport to drop. They also offer the ability to quickly and cheaply communicate this information across vast distances and geographical barriers. Despite advantages provided by technological advancement these very advancements, unchecked, have produced immediate, profound changes in the social system which have in turn produced shifts in values and practices including privacy values and practices (Inglehart, 1977). This change occurs through a technological imperative, separate and apart from the social process that creates values. It often occurs without thought or awareness when the adoption and use of the new technology is incorporated into the lives of individuals. Changes in information

technology has permitted others the ability to access information in new and more penetrating ways, often in ways never before imagined. This is especially true with the information available in the public sphere that was incapable of being effectively gathered and used due to difficulties and cost of detection, gathering and aggregation. Unless bounded or directed, the new technology will affect immediate changes in values, creating two or more sets of incongruent norms, leaving people angry and frustrated and society norms and laws ill equipped to deal with the changes (Spencer, 2002 and Zweig and Webster, 2002).

Technology alone is not responsible for these changes. Additional influences are brought to value formation and change when powerful individuals or groups seek to impose their values on society. Their motivation is to enable the achievement and realization of their private interests. They create a change in values through using technology in a way that advances or enables the achievement of other socially desired values. Sometimes there is no consideration that traditional privacy values are being assaulted. More often the assault on privacy values is deliberate and calculated to change values that that stand in the way of the goals of the assaulter (Spencer, 2002). They are in a sense thrust upon society in a calculated manner to effect changes in society values through the use of these technological advances. The individual is often powerless to resist this attack due to a number of factors such as asymmetry in information, the inability to organize or power disparities (Spencer, 2002).

Outside the workplace the individual use of this technology have advanced personal agendas and enabled certain values to trump traditionally recognized places of

privacy. In Olmstead, telephone wiretaps permitted the listening in on conversations taking place in a home, outside the earshot of police. In Kyllo v. U.S., police stood on the public road and used a thermal imaging detection device to detect the type of radiated heat that would be indicative of growing marijuana inside a structure. The information gathered was not evasive, it was gathered in public. While the Supreme Court of the United States, after a careful review, concluded the use of thermal imaging scanner on a road outside a residence where marijuana was being grown was an improper invasion of private space using public information we see information in public is capable of revealing what is being done in private places. While in each case the use eventually was forbidden, there are other cases where the value of privacy is being changed by technology or where individuals are accomplishing their own designed change.

As an example in recent times we have seen an assault mounted on traditionally held notions of privacy in the workplace through the employ and use of various types of information technology. These advances have increased the ability to manage nearly all phases of the firm while simultaneously lessened the cost of management through the enabling the employer to monitor calls, emails, break rooms and key strokes. These types of intrusions have been justified by these individuals through a traditional right of the firm to control the workplace. In each of these cases the value of privacy is affected. These changes are altering traditional processes of value formation and change by taking the individual out of both the process.

3.1.5.6 Representative Laws and Court Rulings

The initial ruling in this area was the Olmstead (Olmstead v. U.S.) case which has been detailed earlier in this paper. In Olmstead, the telephone's invention had permitted individual's to conduct life in ways never before possible. At issue was the right of the individual to privacy in his own telephone conversation initiated in a place of expected privacy and the ability to listen into a private telephone call through a wire tap placed outside that place. At the time of the ruling, new technology, the telephone, enabled persons to converse outside their home. Law enforcement placed a wiretap outside the residence intercepting all the telephone conversations to and from the residence. In the Olmstead ruling, the majority of the court found that privacy was protection of a place. The majority also found that since the wiretap took place outside a traditionally protected area and in an area of public domain there was no privacy violation. Additionally privacy only protected tangible items like papers and writing and not conversations and what was seized was a conversation which was not entitled to protection. A strong dissent was written at the time of this opinion that urged that privacy was not limited to specific places but was an entitlement where there was a reasonable expectation of privacy. Additionally it was urged that conversations could be protected even though they were intangible. Forty years later the majority decision was reversed and the dissent adopted by the Katz (Katz v. U.S.) decision. Katz specifically found that privacy protected people not places and was not to be limited to tangible items such as papers and writings but to include all things tangible and

intangible in which individuals held a subjective expectation of privacy in including conversations.

3.1.5.6.1 Right to associate

Privacy should protect the right to associate where the association is for the advancement of beliefs and ideas be they political, economic, religious or cultural.

The Supreme Court in the case of NAACP v. Alabama ex rel Patterson, Attorney General (357 U.S. 449 (1958)) kept private the membership list of Alabama residents who were members in the NAACP. A court from the State of Alabama requested names and addresses of its members and agents of the NAACP. These lists were not produced. As a result the NAACP was adjudged in contempt of court and a fine was imposed. The matter was eventually appealed to the U.S. Supreme Court.

Concerns were raised that should such list be made public a chilling effect on membership in the organization would take place as members would be targeted outside the organization. In its ruling, the Supreme Court the members list not being disclosed. The court stated the NAACP had immunity from state scrutiny of membership lists that was related to the right of the members to pursue their lawful private interests privately, and to associate freely with others. The court found: the NAACP was an organization which engaged members for the advancement of beliefs and ideas. It is immaterial whether the beliefs sought to be advanced by an association pertain to political, economic, religious, or cultural matters. Under curtain circumstances membership in an organization should not be disclosed in particular. This is particularly true when the privacy in group association may be indispensable to

the preservation of freedom of association particularly where the group espouses dissident beliefs (US v. Rumely 345 US 41). The Court in particular found that the NAACP lists of members should not be disclosed because of the chilling effect it would have on the advancement of beliefs and ideas particularly because the groups beliefs and ideals may seem dissident to the people of Alabama.

3.1.5.6.2 Communications Decency Act

This was Congresses first attempt to regulate the content of the Internet in an effort to safeguard the raising of children by their parents in the family home. The purpose of this act was to protect children from pornography over the Internet. At the time the Internet provided ready access to pornography which evidence showed children were accessing in their home. Title 47 U. S. C. A. §223(a)(1)(B)(ii) (Supp. 1997) criminalizes the "knowing" transmission of "obscene or indecent" messages to any recipient under 18 years of age. Section 223(d) prohibits the "knowin[g]" sending or displaying to a person under 18 of any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The CDA prohibited posting "indecent" or "patently offensive" materials in a public forum on the Internet -- including web pages, newsgroups, chat rooms, or online discussion lists. In the case of Reno v. ACLU (1997) this act was struck down for violating free speech rights guaranteed by the First Amendment.

Children's On Line Protection Act (COPA) was a second attempt by Congress to restrict a child's access to harmful material commercially distributed on the Internet.

The Communications Act of 1934 was amended in 1998 through legislation. The purpose of the act was to protect the custody, care and nurture of the child, safeguarding the family unit as the place in which children are raised and insulating that area and minor children from unwanted intrusions in the form of access to material inappropriate to minor children that comes from outside commercial sources[59]. Among the prohibitation was the provision that:

> Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both (47 USC 231).

The act further provided a requirement that restricted the disclosure of any information obtained from a minor younger than 17 years and to take further precautions to ensure that no access to such communications was provided to others outside the maker and the recipient. This act was found unconstitutional due to infringement on the right to speech. Despite the ruling, it illustrates the recognition of a need to protect the home from being intruded upon.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of

---

[59] See in general ACLU v. Reno (ED Penn., 1998) citing Ginsberg v. New York, 369 U.S. 329 @ 339-40 (1968)

requirements on any school or library that receives funding support for Internet access or internal connections from the “E-rate” program – a program that makes certain technology more affordable for eligible schools and libraries. In early 2001, the Federal Communications Commission (FCC) issued rules implementing CIPA (FCC, 2006).

Schools and libraries subject to CIPA may not receive the discounts offered by the E-Rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors, for computers that are accessed by minors. In the case U.S. v. American Library Association (2003) the court ruled that although the U.S. has a compelling interest in preventing the dissemination of obscenity, child pornography or material harmful to minors, the use of software filters is not narrowly tailored to further that interest and as such violates the First Amendment.

3.1.5.6.3 Gramm Leach Bliley

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. These regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities.

There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions. Another provision prohibits "pretexting" - the practice of obtaining customer information from financial institutions under false pretenses. The Pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their

personal financial information under false pretenses. The FTC has brought several cases against information brokers who engage in pretexting.

The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information. The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most - or all - of the information a company has about them. When information is disclosed what can be done with the information depends on whether the customer can opt out of the disclosure. If the customer cannot opt out the service provider may use the information for limited purposes - that is, for mailing account statements. It may not sell the information to other organizations or use it for marketing. If the employee can opt out, and did not In this case, the recipient steps into the shoes of the disclosing financial institution, and may use the information for its own purposes or re-disclose it to a third party, consistent with the financial institution's privacy notice.

GLB Act also impacts how a company conducts business. For example, financial institutions are prohibited from disclosing their customers' account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing or

other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes.

3.1.5.6.4 HIPAA

When HIPAA was enacted in 1996, it occurred at a time when the public voiced great concern about their privacy in general. Initial concerns with personal privacy surfaced in the 1960's when the fear was super computers would become Big Brother. These concerns further increased over the years with the development of data storage and communications technologies that provided new methods of invading one's privacy. By 1994 eighty-four percent (84%) of Americans were either very or somewhat concerned about threats to their personal privacy (Consumer Privacy Survey, Harris-Equifax, 1994, p vi.).

An area of great concern was held by the medical patient. Traditional doctor patient relationships involved a deep seated trust by the patient that the doctor would keep confidential all treatment information disclosed to the doctor. This relationship began to be eroded in the years following 1965, when the enactment of the tax deduction enabled employers to purchase health insurance on behalf of employees.[60] This benefit enabled a greater access to medical care. Eventually insurance premiums rose as demand for care increased. In an effort to contain these costs a number of people became party to the patient's health information, including but not limited to insurance companies, employers, expert third parties hired to monitor benefits or

[60] In 1965 Congress enabled employers to purchase health insurance on behalf of its employees and not be required to pay social security on the premium, as well as allowing the employer to deduct the cost of health insurance as a business cost and employees not to be taxed on the health insurance benefit.

contain costs. Information began to flow in many new directions: from reports from the insurance company to the employer detailing the patient's medical treatment, from the expert third parties hired to monitor these benefits to insurers and employers alike to name a few. Self insuring became an option to some. Increasingly businesses and insurers began to realize the value of this information and began to request and rely upon it more and more to make decisions. This assault on this relationship increased when information technology increased the portability of this information and enabled it to be easily accessible, transported and aggregated. The patient not longer had a privilege to keep their medical information private. Either allow the flow of the information to third parties or receive no employment, no treatment, no payment or insurance.

In the rules that enacted HIPAA, it was noted that the effective management of a country's medical information holds many potential benefits. Potential economic advantages exist such as health care organizations being better able to follow and to review practice guidelines and utilization standards compliance by physicians, employers using the studies compiled from computerized medical records to compare the performance of different managed care plans or screen workers for preexisting susceptibility to workplace health hazards (Field, 2004). Additionally, electronic medical records would have enormous value for public health protection and research (Tsai, no year).

> [G]lobal access to health records would facilitate not only conventional disease reporting but also the development of behavioral risk factor surveillance and other more sophisticated

> analyses of health indicia. And present and future health uses are trivial in scale compared with the actual dissemination of medical information attendant upon reimbursement (Buris, 1995).

It was recognized that these benefits were not being realized. At the crux of the problem was the fact that information was neither accurate nor timely. Reasons provided were patients were being damaged by their own medical histories. In a survey conducted by the California Health Care Foundation and Consumers Union, it was found many people fear their personal health information will be used against them to deny insurance, employment and housing, or expose them to unwanted judgments and scrutiny (California Health Care Foundation and Consumers Union, 1999). Seven percent of respondents in the Harris survey said "they or an immediate member of their family had chosen not to seek medical services due to fear of harm to job prospects or other life opportunities" (Health Information Survey, Harris-Equifax, 1993, pp. 49-50). In the same survey, two percent reported to have not filed a health insurance claim due to concerns of privacy or the lack of confidentiality (Health Information Survey, Harris-Equifax, 1993, pp. 49-50). The Federal Government found that medical conditions were the basis for demotions, firings, being passed over for promotions or even being hired in the first place. The government also found many people were finding themselves unable to get insurance, unable to get affordable insurance or being dropped from insurance altogether.

The government found evidence that in response to these conditions people were providing inaccurate information when seeking medical diagnosis and treatment

or failing to seek medical care until conditions became acute (65 Federal Register page 82777). This provided one explanation why the United States, despite paying four times more per person for medical services was woefully behind the world in medical treatment results. Significant benefits are available when early treatment is sought. One benefit of early treatment is it results in the reduced spread of disease. But early treatment has other benefits. It was projected if only 7 percent of those who have cancer could be encouraged to seek early treatment, a reduction of cancer mortality of 33 percent would result. This early treatment was projected to save 1.6 billion annually in lost wages (65 Federal Register page 82777). This savings was projected in other areas as well. An annual net economic benefit between 497 million and 795 million was estimated to be achievable in mental health treatment through the encouragement of early treatment (65 Fed R. 250 page 82779). The early treatment of sexually transmitted diseases was found to result in lower mortality rates as well as reduced cost associated with complications.

Individual states had recognized the privacy invasion and enacted some legislation designed to deal with the issue. They were not effective. Prior to the enactment of HIPAA, the American regulatory regime of medical record access has politely been characterized as "fragmented" (Lowrance, 1997). Turlington described this less politely as a "black hole" (Turkington, 1997). Senator Edward Kennedy asserted, "Today, video rental records have greater protection than sensitive medical information" (Kennedy, 1999).

HIPAA was enacted on the premise that it is necessary to restore the confidence in the patient that their medical information will remain confidential. This will be achieved once the traditional patient physician relationship is restored. HIPAA achieves this objective by a number of means. It provides privacy standards for data storage and transmission. Additionally HIPAA provides incentives to protect patient information, penalties for the use of information and restores the bargaining power of the patient to determine when and what information is disclosed and enforce actions when patient privacy is violated.

3.2 How the Model Works: A Basic Analysis of Privacy Using Access and Control

The two positions of access and control are necessary to define and to distinguish between the different types of privacy. The first step in defining the privacy is looking at the laws, norms and agreements which create the relationship and determine the degree of control the entity which possesses this information has over these issues: what information becomes accessible, who gets the information, and at what time the information becomes accessible if at all. The second step involves looking at those same laws, norms and agreements and determining the accessibility of the disclosing entity in terms of access to the entity and access to information about the entity again asking the same questions of what information becomes accessible, who gets the information, and at what time the information becomes accessible if at all. Once the initial disclosure is analyzed a further analysis must take place on the likely possible disclosures of this information resulting after the initial disclosure.

While in some cases it may be true that the control over information alone may dictate that others have low access to the entity and information about the entity it is not necessarily true in all cases. Under conditions of low access, the degree of control necessary to establish and maintain the condition is low. Therefore the effect is not a one way effect based upon control but rather it is an interactive effect based upon the interplay of access and control What also must be examined is after disclosure by an entity, that disclosing entity has lost control over their information as well as lost control over both access to themselves and to the information about themselves as the possibility exists that after the disclosure of information others may obtain the disclosed information and would be free to use this information as they desire.

By way of example, a person seeks the care of a doctor. Initially the patient has high control over who he gives his medical information as well as what information and when it is disclosed. Access to this information is low, as only the patent has this information. In this situation the person also enjoys low access to both his or herself and his or her information in large part because they can control the situation and make themselves and their information low access. However once the information is disclosed a new scenario emerges. The information disclosed to the doctor is now out of the control of the person. That person has now lost both the control over his information as the disclosee can make decisions on how the patient's may be used but they may also determine who has access. Additionally an entirely new access has been introduced. Not only is the information exposed to the caregiver but it is exposed to those in the caregiver's employ. Depending on the situation access may be high to this

information giving the caregiver little control over the information. Additionally patient information can (and usually must) be disclosed to third parties such as insurance companies.

In general the highest state of privacy occurs when an entity has high control over what, when and to whom information is disclosed together with the condition of low access by others to both the person and their information. The least optional state is one where low control over what, when and to whom information is disclosed is coupled with high access by others to the person as well as their information

Control /// Access	High over Person and Information	Low Access to the Person and their information
High control over: To Whom Information goes What Information goes When the Information goes	Moderate Condition for Privacy	Optimal Conditions for any Privacy
Low control over: To Whom Information goes What Information goes When the Information goes	Least Optimal Conditions for any Privacy	Moderate Condition for Privacy

Table 9 Control Over Access

3.2.1 Access to the Entity and their Information

Access to the Entity entails the ability to identify an Entity from their information or the ability to gain access to that Entity either physically or virtually. Access to information is the ability to gain the information of the Entity. Having access to an Entity does not necessarily mean you have access to their information. By way of example you can meet an Entity and from that meeting learn a lot about that Entity, but you may not necessarily know what they really believe or are thinking. Under both conditions there are two levels: high and low This leads us to 4 potential states: High

Access to Information-High Access to Entity, High Access to Information-Low Access to Entity, Low Access to Information-High Access to Entity, Low Access to Information-Low Access to Entity. :

	High Access to Information	Low Access to Information
High Access to Entity		
Low Access to Entity		

Table 10 Access to Entity I

Depending upon the role based activity, these different access patterns can result in a different level of privacy. Low Access to Information and Low Access to the Entity should result in the highest level of privacy while High Access to the Entity and High Access to Information should result in the lowest level of privacy.

	High Access to Information	Low Access to Information
High Access to Entity	Lowest Level of Privacy	
Low Access to Entity		Highest Level of Privacy

Table 11 Access to Entity II

3.2.2 Control over Information

Control over information can be examined in a way similar to access over information.

Control over information is examined in three dimensions, control over what information is disclosed if any, control over to whom that information is given and finally control over the timing of the information disclosure. An entity possibility could have control over all three spheres, over none of the spheres or over only one or two of the spheres. The degree of control can be high, medium or low control. Situations of

control would be highest when the entity possesses high information control over the what, who and when dimension and lowest when low information control is present along all three dimensions. Intermediate positions occur when high positions in one or more areas are coupled with low control in one or more area.

3.2.3 How the various privacies relate in terms of control and access

Each type of privacy is grounded in a social role. Each type of privacy enables values of that role to be realized. This is accomplished through the variance of control and access. The Strongest combination of access and control with the highest level of privacy is the High Control/High Access to Person – High Access to Information. The weakest level of privacy is Low Control/Low Access to Person and Low Access to Information.

	High Access to Entity and High Access to Information	High Access to Entity and Low Access to Information	Low Access to Entity and High Access to Information	Low Access to Entity and Low Access to Information
High Control				Relational Privacy
Medium Control	Secret Privacy			Privilege Privacy
Low Control	Transitory Privacy			Intellectual Privacy

Table 12 Access to Entity III

Relational Privacy demands the highest level of privacy both in terms of access to the entity and information and as to control. In relational privacy, the entity has high control over their information. Entities seeking access to that entity or information about that entity have low access to both the entity and information about the entity. Transitory Privacy by its very definition permits low controls over information coupled

with High Access to both the Person and the Person's information by others. Privilege Privacy has the characteristic of having initially high control in the entity over her/his information. However this control diminishes. This diminishing of control exists because there is a compelling need to obtain assistance, but a precondition to obtaining assistance requires that information must be shared. The same occurs with access to the person's information. Initially others have low access to the entity and information about the entity. Once disclosed, any number of entities can have access to the information despite the fact they may never have contact with the person. In any event, low access to the entity and their information must be maintained. In Secret Privacy, initially the holder of the information has very high control, but has also strong motivations to disclose this information. Once disclosed, not only does the owner of information lose a great deal of control, but they also lose the high degree of protection afforded them in terms of access to themselves and their information as once disclosed the information becomes very accessible. Often time, this accessibility is taken care of by agreements that bring control over the entity to which the information is disclosed. Intellectual Privacy has the characteristic of the entity having low control over the information sought after requiring the entity to have the information made available to them or to seek out the information. Intellectual privacy however demands that the request for information as well as the content of the information consumed should be very highly protected. Additionally, any tests made with that information should also be kept confidential. Therefore access must be low to both the entity consuming the information as well as what information is consumed by the entity.

3.3 Conclusion

Combining the control and access paradigms, five distinct types of privacy have been specified and distinguished in terms of purpose, philosophy type, relationship entities and characteristics of the relationship, role characteristics, and character of information. Each has been illustrated through representative laws and court rulings. A model of privacy roles grounded in social relationships and supported by legal theories using levels of control and access was demonstrated. This model distinguishes the five different types of privacy based upon the optimal level of control and access required in each type of privacy.

In Chapter Four this model will be applied to the design of a security system. Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Security design and implementation is a costly but incomplete, inexact, and imperfect process. For these reasons, demands for better design and implementation of security systems exist.

The both the qualities secure data must possess well as the functional specifications of access systems will next be presented. Two categories of access mechanisms will next be presented with their strengths and weaknesses. Research will next be presented that outlines work done to increase the effectiveness of these mechanisms. Chapter Four will conclude with a proposal for improving data access mechanisms using the model proposed in this chapter

Chapter 4: A Proposed Evaluation

4.0 Proposal

The requirements of a security system are defined by its functional specifications. Using these functional specifications, the security system defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide requisite levels of confidentiality, possession, integrity, authentication, utility and availability required to achieve the functional specification. Good security design and implementation offers the promise of great rewards but the process is costly and often plagued by imprecision. For these reasons, demands for better design and implementation of security systems exist.

A portion of the functional specifications of a security system are the attributes that secured data must possess. This will first be presented using the CIA Triad and the additions offered by the Parkerian Hexad. Next data access mechanisms of mandatory access control (MAC) and discretionary access control (DAC) will be introduced together with their respective strengths and weaknesses. Following this role based access mechanisms (RBAC) will be reviewed. These use levels of indirection which enable and/or disable access and/or functions on objects employing features of the DAC and/or MAC systems. Some extensions based on the proposed legal framework developed in prior chapters will be presented that improve the effectiveness of role based access (RBAC) mechanisms. It will be shown that the research is directed not to add new capabilities to security systems but aimed at easing the administrative burden

of establishing consistent permissions of access and actions on objects to users in similar circumstance and need. Chapter Four will conclude with a proposal to apply the privacy model revealed in the previous chapter to create a new conceptualization of a tiered RBAC access system that is theory based and adds new capabilities to security systems.

4.1 Introduction

As firms compete more often on data analytics, issues of data quality and security become increasingly important. While the ability to protect critical data assets has always been a cost of doing business, data and knowledge management capabilities are now embedded in core business processes. In addition, external forces and requirements, such as Sarbanes-Oxley, make the control and security of data an explicit obligation with significant costs. Increasingly businesses are pursuing security as a strategic goal or even as a way to obtain competitive advantage in the marketplace.

Regardless of whether security is viewed as a cost of doing business, a strategic goal or a competitive advantage, security design and implementation is often not only costly but also incomplete, inexact, and imperfect. After the security system is designed and implemented, there are often unforeseen security gaps, which if not heeded could lead to vulnerabilities, security risks and breaches of security. Because of the high cost associated with rectifying these issues, security systems may be intentionally over engineered, resulting not only in additional costs, but with a loss of functionality and unnecessary restrictions placed on data accessibility. With each loss of functionality, not only does the user suffer a loss of satisfaction with the system but

the system breeds attempts to find ways around the system leading to new security gaps, vulnerabilities, risks and security breaches.

4.2 Functional Specifications

Functional specifications of the security architecture ultimately emanate from social norms, laws, and consumer concerns.

Social norms, laws and customer concerns form the restrictions placed on data. Some of the restrictions come in the form of laws such as privacy and intellectual property laws which establish duties and the corresponding claims when those duties are not fulfilled. From these restrictions confidentiality and possession standards are created which dictate the security model, security technology, cryptograph technology, DBMS Technology for the security system as well as the database and data design and application technology chosen. These standards define the integrity constraints placed upon the data which will determine the authenticity of the data which will affect both the availability of this data but its usefulness as well. Through these integrity constraints availability is defined with authorized individual given access to data and unauthorized individuals prevented from knowing and accessing information. From the access obtained, the utility of the data and ultimately the utility the user are determined.

Social norms, laws and consumer concerns define the functional specifications that the security architecture must ensure. These functional specifications in turn ensure the attributes that data and information must possess.

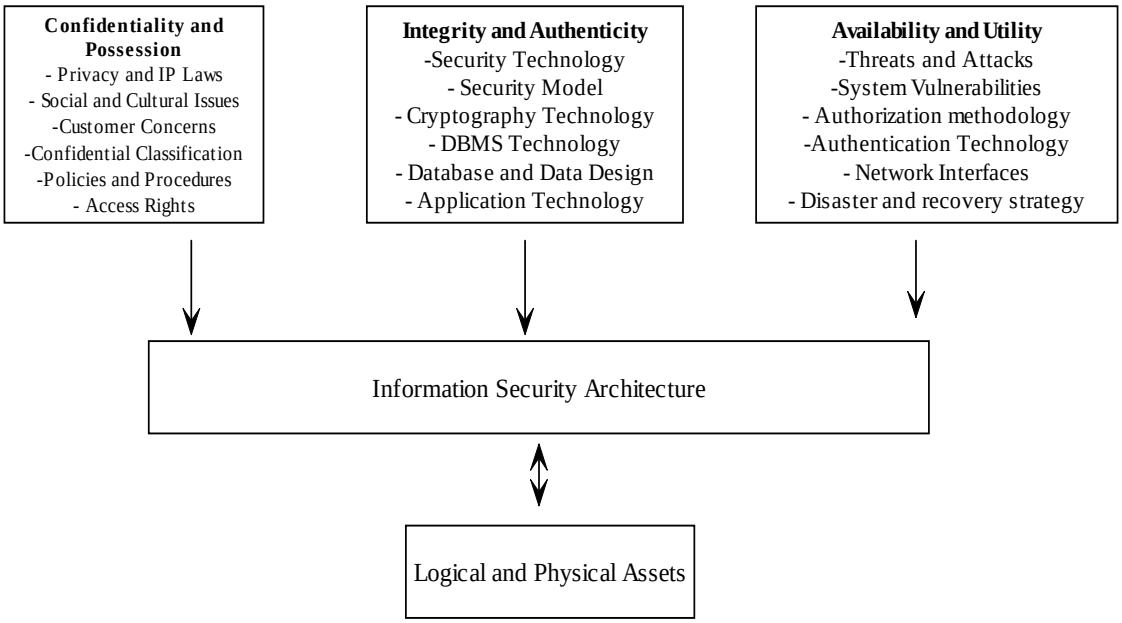

Figure 13 Functional Specifications and the Information Security Architecture

The figure is from Afyouni, Hassan, *Database Security and Auditing: Protecting Data Integrity and Accessibility*, Thompson Course Technology, Boston, Massachusetts, 2006

4.3 The CIA Triad

The CIA Triad and the subsequent additions to the Triad, provide functional specifications that a security system protecting information must possess to ensure social norms, laws and consumer concerns. When provided by the security system, these in turn provide the protected data and information with these attributes.

"Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or

destruction in order to provide confidentiality, integrity, and availability [the so-called "CIA triad"], whether in storage or in transit" (Plone CMS, 2000).

Privacy and security regulations take many forms but ultimately they address portions of the classic CIA Triad – Confidentiality, Integrity and Availablity. The idea of the triad originated with computer security integrity model introduced by David D. Clark and David R. Wilson (Clark and Wilson, 1987). Comparing access to data in the commercial arena with the access mechanisms utilized by the U.S. Department of Defense, they noted that in the commercial realm, emphasis in security was on information integrity. In the Department of Defense, security was deemed more as the enforcement of confidentiality and expressed through a system of classification labels and classifications. They ultimately concluded that confidentiality and integrity were important goals of any security system. This laid the groundwork necessary for the concept of the CIA Triad which later originated with the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee of National Security Systems (CNSS).

The CIA Triad is a data security model used in the design of security systems that protect logical and physical assets. The CIA Triad specifies the *minimal* functional specifications that a security system must provide for data and information. This model has been largely accepted both by government and business. CIA is a mnemonic which stands for Confidentiality, Integrity and Availability – characteristics that secured data should possess after the security system is designed. These attributes in turn support each other and together define the information security architecture.

4.3.1 Confidentiality

Confidentially addresses various aspects of security and emanates from three sources, social and cultural systems, customer concerns and privacy laws (Afyouni, 2006). Confidentiality defines what information must be protected and kept private (Stone and Merrion, 2004). Confidentiality is an assurance that information is not disclosed to unauthorized persons, processes, or devices (CNSS, 2003) or even knowing the information exists (Afyouni, 2006). International Organization for Standardization (ISO) defines the term in a slightly different manner. In the ISO definition confidentiality is seen as "ensuring that information is accessible only to those authorized to have access." Confidentiality has also been defined as the process of safeguarding confidential information and disclosing secret information only to authorized individuals by classifying information and placing restrictions on its access and dissemination (Afyouni, 2006).

4.3.2 Integrity

According to the National Information Assurance Glossary:

> **"**Integrity is the quality of an Information System, reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data" (CNSS, 2003)

The integrity of the information systems depends upon the integrity of the data. In database design there are many aspects of integrity with which the designer must be concerned, such as elimination of anomalies, concurrent reads and committed reads. In

security the concerns differ as the chief aspects of integrity that concern the designer are the prevention of unauthorized modification, insertion or destruction of data in a database regardless of whether it occurs intentionally or as a mistake. Integrity enforcement ensures that data possesses a quality of being complete, whole, sound and in compliance with the intention of the creator of the data, and remain so even after the implementation of the system.

4.3.3 Availability

Availability is the timely, reliable access to data and information services for authorized users (CNSS, 2003). Availability requires the balance of two opposed interests. It must enable access yet enforce confidentiality and integrity which restrict access. In determining availability you must take into account potential threats, risks, and vulnerabilities to the system. Often confidentiality specifications indicate these potential threats, risks and vulnerabilities that potentially threaten data integrity. When providing for availability you must provide an authorization methodology, authentication technology, network interfaces as well as provide for disaster and recovery strategies.

4.3.4 Additions to the CIA Triad

Parker, the renowned security consultant and writer proposed three additional attributes to the CIA Triad, known as the The Parkerian Hexad (Parker, 2002). Parker proposes that information protected by information security should possess in addition to the attributes of confidentially, integrity and availability the following attributes: the

attribute of utility, the attribute of authenticity and finally the attribute of possession (thus adding three additional functional specifications to the security system).

Parkerian Hexad refines the security guidelines to make them more applicable to commercial enterprise. Utility, the quality that the information possesses a usefulness and fitness for a specific purpose adds dimension to the concept of availability. The reason information is needed is the information is useful to the user's purpose. Authenticity, the quality that the information possesses the correct attribution of origin or is the correct description of information supplements integrity. Today in marketing often times the value of the information is not only the data item but the linking of the data item with the source of the data. Possession is similar to confidentiality yet it too is distinctive. Possession is the quality that information is capable of being owned, possessed and controlled in a way that it becomes property. Part of control is preventing physical contact with data. Another aspect is the preventing of copying or unauthorized use of data. Possession in the sense of ownership is of particular value where information has consumption value such as the holder of a copyright to a book or music.

There can be other functional specifications to any security system which would vary depending upon the security needs of the application. Other such proposed

specifications include such specifications such as privacy, repudiation of messages, proof of originality and proof of identification[61].

4.4 How the design and implementation of security is accomplished

From the CIA Triad and Parkerian Hexad the minimal functional specifications that a security system must provide for data and information are determined. In most all systems, high levels of confidentiality/possession and integrity/authenticity are highly desired. However when increasing the levels of either confidentiality/possession or integrity/authenticity, decreases in accessibility and utility occur as a result. Access control models dictate how data is accessible to users and processes. While systems exist that can contain high levels of confidentiality/possession or integrity/authenticity, no system has been able to provide both simultaneously.

4.4.1 Access Control Models and Their Methods

Until Role Based Access Controls (RBACs) were conceived and implemented two types of access control models have been used to provide accessibility to data. Mandatory Access Control (MAC) systems accomplish the security design by designing the access so the system dictates access. This system best ensures confidentiality/possession. Discretionary Access Control (DAC) Systems grant control over data to the owner of the data. DAC systems best ensure integrity/authenticity. Each system has been instantiated in a tool or tools that permit access to data but has

[61] See Dridi, Fredj, Muschall, Bjorn, Pernul, Gunther, *Administration of an RBAC System*, Proceeding of the 37th Hawaii International Conference on Systems Sciences IEEE 2004 where additional functional specifications were set forward to deliver the required security for the Webocracy Project.

been unable to provide simultaneous high confidence/possession and high integrity/authenticity.

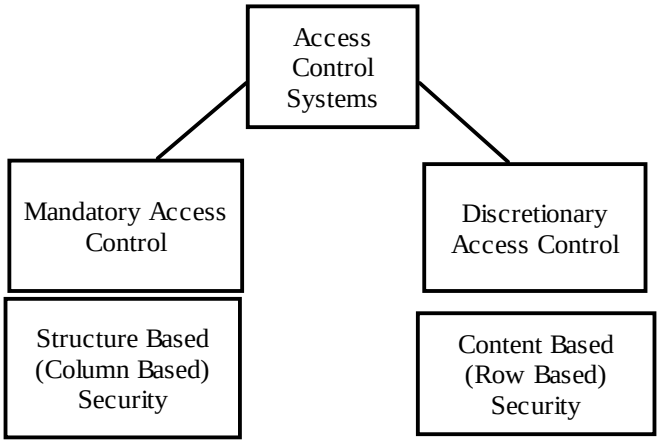

Figure 14 Access Control Systems

4.4.2 Mandatory Access Control

Mandatory Access Control (MAC) systems utilize a confidentially based system where the access policy is determined by the system. These types of systems are called structure or column based security systems because they are implemented using the structure and columns of the data model.

Database features can operate at many levels. MAC uses the most simple and common approach to database security by considering the schema or database structure. In a relational database, the structure is expressed in terms of relations (i.e., tables) and attributes (i.e. columns). A security policy would then explicitly name the tables or columns that particular database users are allowed to read or write. To add a bit more flexibility, many database management systems add mechanisms for grouping users so

that access rights can be more easily granted or revoked. Essentially, these structural approaches to security borrow from the file systems associated with operating system environments. File systems typically provide access controls that grant computer users the right to read, write, or perhaps execute the contents of specific files. This is similar considering only database structure in that file names, but not file contents, are used to assign access rights.

In MAC type systems all subjects and objects have a sensitivity level assigned to them for the subject it is called a security clearance, for the object it is called a security classification (Sandhu, 1996). In the MAC system, the principle sensitivity level is checked at the resource (Miller, Yee and Shapiro, no year). To access the object, the subject must have a security clearance equal to or greater than the sensitivity level of the object they seek to access. Setting fine levels of access granularity at the relation or column level is considered cumbersome and very difficult to maintain over the long term. When required this is often done through setting up separate tables based on the level of granularity of data (Sandhu, 1996).

MAC security mechanisms can be quite inflexible, using only database structure. Access can be granted or denied in an outright manner, but not made conditional on the content or values of attributes. In terms of a medical example, there might be a code attribute that represents the diagnosis associated with a hospital admission. Access to this diagnostic attribute or column can be granted to hospital clinical staff. However, access cannot be granted based on particularly sensitive diseases. A diagnostic code for an arm fracture is accorded the same security as cancer.

The inability to consider the contents of a database does not support the nuanced approaches that more complex security policies require.

Data access processes such as the Bell-LaPudula model utilize a MAC system. This system was designed to prevent theft and tainting of high level information using processes heavily leveraged toward the protection of confidentiality. Originally designed as a Department of Defense project in 1973, access is predicated upon a series of classifications of each user and each data object. In the Bell-LaPudula system, a user cannot write to an audience lower than the user's classification. Neither can a user access documentation that is classified at a higher level. As a result this is known as a read down/write up process.

4.4.3 Discretionary Access Control

At the other spectrum are Discretionary Access Control systems (DAC) DAC systems and their processes that tend to be leveraged toward maintaining integrity, authenticity and utility. In the DAC system, every object has an owner and the owner determines the access policy. The theory is any object without an owner is an unprotected object. This owner determines who has access to the file and what privileges they possess to that object. The owner can also delegate ownership to others. To maintain integrity and authenticity, methods of separation of duty, separation of function and an auditing tool are employed. Often the auditing tool is a log of some type which keeps track of the transactions so that unauthorized access can be detected and any actions taken rolled back to remove any destructive effect on the data. Thus in

this type of system, integrity is highly maintainable but because of the ability of the owner to delegate ownership, confidentiality is not as strong as in a MAC systems.

DAC type systems utilize content based (row level) access control (Sandhu, 1996). Here the access and action capabilities rather than being stored with the object as they are in column-based security, are stored with the subject, with the access capabilities being in the form of a pointer to the object (Miller, Yee and Shapiro, no year). DAC systems are more flexible in terms of the granularity of access to objects than MAC-type systems (Sandhu, 1996). One type of DAC system is the commercial database system from Oracle known as the Virtual Private Database. Essentially, this feature creates a unique view of the database for any specific user. As the Oracle documentation describes, a Virtual Private Database provides the ability to dynamically filter out rows (based on content) rather than columns:

> "Oracle's row-level security (RLS) feature, introduced in Oracle8*i*, provides fine-grained access control—fine-grained means at the individual row level. Rather than opening up an entire table to any individual user who has any privileges on the table, row-level security restricts access to specific rows in a table. The result is that any individual user sees a completely different set of data—only the data that person is authorized to see—so the overall capabilities are sometimes referred to as Oracle's virtual private database, or VPD, feature."

Despite this, pure DAC systems do not possess mechanisms that facilitate the management of access rights of many users. In the MAC system, users similarly situated are granted similar access patterns to objects. In MAC, each user must be explicitly granted every privilege they need to every object they require largely due to

the authorization mechanism being located with the owner and not resident with the object (Sandhu, 1996).

Clark-Wilson type processes utilize DAC type systems. Clark-Wilson type processes use a system of enforcement and certification rules to define data items and processes that provide the basis for an integrity policy that employs well formed transactions that use rules to enable the system to transition from one consistent state to another consistent state. These often include monitoring and archiving of transactions and functions that can rollback the database to a previous stable state should unauthorized actions occur.

In practice MAC and the Bell-LaPudula model is used more often in military applications where confidentiality is a paramount concern. For commercial applications, procedures based upon the DAC and Clark-Wilson Integrity Model is preferred (Clark and Wilson, 1997).

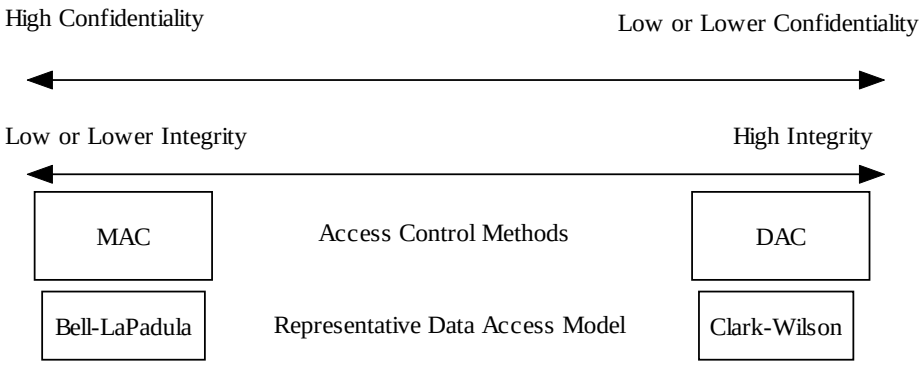

Figure 15 Comparison of MAC and DAC

4.4.4 Role Based Access Control

It has been said that with respect to the design and implementation of security "It is difficult to implement but not impossible if you properly classify your information and design a process to implement and enforce confidentiality (Afyouni, 2006).

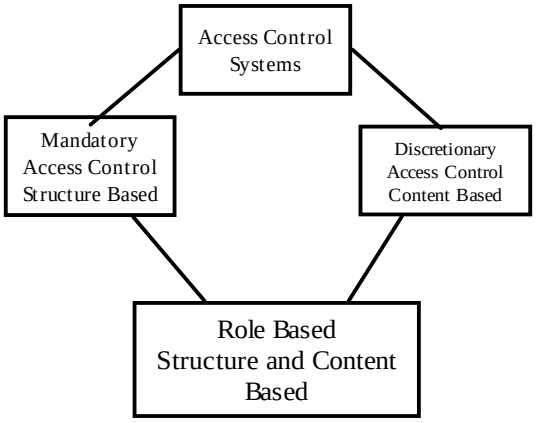

Figure 16 Access Mechanism Family

A role is a semantic construct for formulating security policy (Ferraiolo et al, 2001). Roles are constructed to perform a specific task for the organization and assigned to individuals or processes, objects (Nyanchama and Osborn, 1994) or methods (Izaki et al, 2001) to perform. To perform the task a role must be assigned permissions to access objects and perform functions on those objects. Once permissions are assigned to roles, the various roles are assigned to users to perform their tasks.

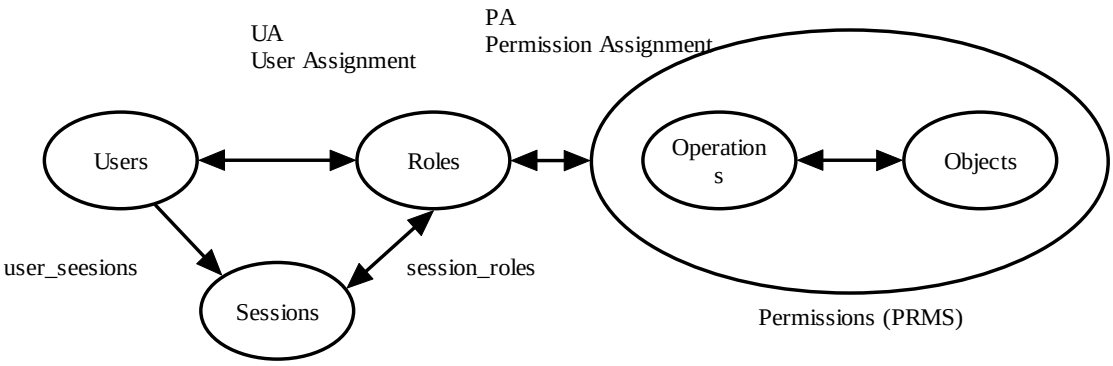

Figure 17 How RBAC Works

Drawing is from Ferraiolo, R., Sandhu, Gavrila, S., Kuhn, D, and Chandramouli, R., *Proposed NIST Standard for Role Based Access Control*, ACM Transactions on Information and Systems Security, Vol 4. No. 3, pp. 224-274 August 2001.

Role based security grants access depending on the current role assigned to the user. Initially, research conducted by Nyancharma, Osborn and Sandhu convincingly demonstrated that role based access system could model a MAC type system (Nyanchama et al, 1994, Osborn, 1997, Osborn et al, 2000, and Sandhu, 1996). Later research conducted by Osborn et al showed that role based access systems could also model DAC type systems (Osborn et al, 2000). This has lead to the conclusion by Chou that role based access control is “a superset of (both) MAC and DAC” (Osborn et al, 2000). Prior to the role being assigned to the user a role is created. Each distinctive role is assigned permissions to columns, rows or both which permits the ability to implement finely grained security. A second advantage of roles is there is no need to set

for each user a unique set of permissions -users similarly situated are assigned the same role. This makes the assignment of security more efficient but also creates greater consistency. The final advantage of role based security is that this three pronged approach of structure, content and role can be used to express very sophisticated security policies.

4.5 Research on Role Based Data Access

Researchers have investigated a number of issues related to Role Based Access Controls. Early timesharing operating systems introduced the notion of a group of users which can occur as a single entity in access control lists. This had the effect of conferring the associated permissions to all members of the group. Some discussion existed at the time whether RBAC was in fact a new term for an old idea (Sandhu, 1996). Regardless of this discussion, it is a vibrantly researched area full of promise and opportunity.

Initial research was directed toward questions on how this would be used. A SETA Questionnaire was administered to a private sector supplier, a federal bureau, and a federal medical system program office to assess user needs regarding RBAC features. The questionnaire had a list of defined RBAC features that might be of interest to potential RBAC users. Results were then reported. Each subject found value in RBAC but varied on how the application would be applied and of use to them (Sandhu, 1996).

While significant research was present before, the seminal model of a role based access system was proposed by Ferraiola, Sandhu, Gavrila, Kuhn and Chandraomouli.

In this paper a National Institute of Standards and Technology (NIST) standard for role based access control was proposed. The authors developed both a RBAC Reference Model and the RBAC Functional Specification. In the Reference Model they described a common vocabulary of RBAC element sets and relations for specifying requirements and the scope of RBAC features included in the standard. The Functional Specification described the requirements for administrative operations for creating and managing RBAC element sets and relations and systems functions for creating and managing RBAC attributes on user sessions and making access control decisions (Ferraiole et al, 2001). This model has organized subsequent RBAC research into the categories enumerated.

Roles are the basis of a RBAC system. Role engineering is focused on the modeling of a concrete instance of a RBAC model. The process of role engineering a/k/a access control realization has two levels: One level includes the development of roles of an information system. The second level is that of the security administrator who defines the association between roles and system users. Significant research has been focused in each area.

4.5.1 Development of Roles in a RBAC

Initial work in this area was done by Coyne. To identify roles, he collected different user activities and described them as verb/object pairs. The activities then were clustered to define candidate roles. In subsequent steps, constraints were defined and role-hierarchies built (Coyne, 1996).

Fernandez and Hawkins constructed security requirements using role rights from use cases. Authorizations and permissions were derived from the preconditions modeled for each use case. The permissions that a particular actor needs would be determined by the use case the actor participates. Shortcoming of this method include that it does not describe when and how constraints are elicited nor does it deal with the defining of role hierarchies. Epstein and Sandhu also used UML diagrams. Using a health care domain they demonstrated how UML can document a RBAC model. However no role engineering process or framework was presented nor did they deal with the defining of constraints, role hierarchies or deriving of permissions (Epstein and Sandhu, 1999).

Roeckle et al concluded that RBAC roles are closely related to core business functions. They suggested a process oriented approach could be used for role finding. Using a case study approach, they distinguished three layers, a process layer where business processes were modeled, a role layer which role candidates were defined from the business processes and a access rights layer which defined the rights of access from the role layer. Roeckle only described the process of role finding on a meta level and did not detail how to derive permissions, or to assign permissions to roles or define role hierarchies or constraints (Roeckle et al, 2000).

Epstein and Sandhu introduced three layers- tasks, work patterns and jobs, between roles and permissions to divide role permission assignment into smaller steps in the effort to make the process more manageable. A task is a specific step of work.

This task is associated with permission necessary to perform the step. Work patterns are the sequences of tasks (Epstein and Sandhu, 2001).

A framework for modeling privacy requirements in role engineering was undertaken by He and Anton in 2003 (He and Anton, 2003). Later Neuman and Strembeck looked at a scenario driven process for functional RBAC roles (Neuman and Strembeck, 2002). Differentiating roles between functional (roles that reflect essential business functions that need to be performed) and organizational (roles corresponding to hierarchical organization of a company), the paper presents a role engineering process for functional roles using scenarios. The authors demonstrate that through scenarios, every possible or actual event sequence can be discovered. From these, possible solutions and reactions can be constructed with permissions, constraints, tasks, work profiles, role hierarchies being modeled through an iterative development process.

Recently Poniszewska-Maranda extended the standard RBAC model by applying Unified Modeling Language (UML) for the purpose of role creation by defining appropriate role permissions using a two stage process: First definitions of the permissions assigned to functions are created. In the second stage the definitions of functions assigned to a particular role are provided (Ponsizewsha-Maranda, 2005).

4.5.2 Administration of RBAC systems

Much work has been focused on the administration of RBAC systems. In two papers working with central administrative non role-based systems role issues were studied. Gavrila studied the administration of user role assignments and the relationships among roles (Gavrila, 1998). A set of administrative rules were proposed

to maintain the consistency of the RBAC system. Using the role graph created by Gavrila and Nyanchama proposed a formalized description for administrative algorithms of the role hierarchy and role permission assignments (Ponsizewsha-Maranda, 2005).

Sandhu developed a role based RBAC administrative model composed of three sub models – user/role assignment, permission/role assignment and role/role assignment which are used to control user and assignments, role permission assignments and role hierocracy(Sandhu, R.S., Bhamidipati, 1996).

This model has been accepted as the most mature model for role based administration but still suffers shortcomings. These shortcomings include no support for the administration of newly introduced relationships, as well as complications from a plethora of constraints for the administration of role hierarchies to maintain the validity of the role range of each administrative role that reduces the flexibility and practicality of the model. This model did not present conflict checking rules to maintain the consistency of the RBAC that administrative activity may introduce conflicts into the system. A final issue is it failed to support the administration of authority constraints (Qui, Jiong, 2005).

Recent work in RBAC has centered on how to construct, implement and administer roles. Roles are viewed as levels of indirection which enable and/or disable access and/or functions on objects. One use of roles is aimed at easing the administrative burden of establishing consistent permissions of access and actions on objects to users in similar circumstance and need. When specifying, constructing and

administering roles a ground up approach is used. The focus of this approach is on the activities of the user, as directed by the needs and purposes of the customer and the rights obligations and duties imposed by law and the social norms. This approach requires brute force: employing great numbers of man-hours to examine each specific instance and scenario, real and imagined, using an implicit, subjective understanding of privacy. Roles created under these systems have the characteristics of being weak and disjunctive. Often they are peculiar to a particular place and time. Despite the great effort taken, frequently roles need to be reworked because of over and under specification and reexamined and redacted as changes occur within and without the business entity. It is for these reasons that NIST has placed reducing the cost of authorization management a focus of it research effort (NIST, 2003).

Using functional specifications provided by a proposed NIST standard for the Core RBAC model administration, Tittinene studied requirements for managing roles, users and permissions using a methodology based upon roles to analyze requirements of individual and organizational users of documents as well as those of organizational needs related to security and access control (Tittinene, 2003).

A RBACAM (Role Based Access Control Administrative Model) was proposed for the purpose of simplifying the description of role hierarchies. The benefit is it would decentralize the administration of RBAC. Each role would have responsibility for role administration in its own domain and enhanced domain. This model provides conflict checking rules to maintain consistency and the administration of authorization constraints as well as administrative algorithms of role hierarchies, user role

assignments, permission role assignments, and authorization constraints (Qui, Jiong, 2005).

In the context of a Financial Enterprise Content Management System, key privacy and access control policies for internal content flow management and external access control for Web portal and institutional programmatic users were developed and demonstrated. Additionally a language was created to specify privacy and access control policies in each part of the system. This system uses EPAL – Enterprise Privacy Authorization Language a technical specification that exchanges privacy policies and makes privacy authorization decisions. It also uses eXtensible rights Markup Language to describe the rights and conditions for owning or distributing digital resources. Using a specification of licenses the XrML agent can determine to grant certain rights on certain resource to a certain principle or not (Chiu and Hung, 2005).

One study involved the design and implementation of an RBAC system based upon the Core RBAC model as defined by the NIST standard. The study concerned the administration of the RBAC based control and authorization facility for the Webocrat system, a European project designed to provide citizens, businesses and governmental agencies with more convenient access to government information and services, to improve the quality of services and provide greater opportunities to participate in democratic institutions and processes. The effort focused on a unit of that project the CSAP whose purpose was to provide practical and consistent security by providing security services for the project such as access control and authorization among other things. This group specified administrative requirements for managing roles, users and

permissions the group specified and presented an administrative console designed to implement these requirements (Dridi, 2004).

4.6 Proposed Demonstration

While the CIA Triad and the additions offered by the Parkerian Hexad have been largely accepted both by government and business alike for providing functional specifications for protecting information, the achievement of the promised secure system has proven elusive as evidenced by news reports of security breaches or organizations and individuals alike, expressing concern that information about them has been accessed or is accessible.

Security policies have been based upon structure (MAC) and upon content (DAC). A security capability based on structure, content, and role (SCR) provides the toolkit for implementing meaningful policies using organization-level terms. Using a MAC system, structure-based access rights (column-level) are enabled that allow clear and concise restrictions to be imposed irrespective of other concerns. Bringing content into the mix such as DAC systems accomplish supports conditional rules based on the range of values, resulting in row-level security. Roles introduce a third conditional dimension based on the context in which a user is manipulating data. The intersection of structure, content, and role supports the dynamic expression of security policies based on both data and users within specific task contexts.

The overarching goal of this project is to create a new method to construct information security. Security and privacy are linked concepts. We employ security measures to enforce privacy and protect private data. Security restrictions depend upon

how privacy and private information are defined. In practice privacy as a concept is not often understood, holds significant subjective meaning and as a result it is often subject to debate. There are implications of not understanding or being able to specify privacy or what data is private in an objective manner. One is the potential for loss when security is breached and private data is exposed and improperly accessed. Additionally there is an increase in cost of construction of the security system. To ensure security by necessity this system must be over developed which results in greater then necessary costs in time and money. This over development also often results in an under functional system that provides less than achievable utility for the system's users.

A new conceptualization of privacy was undertaken to better specify privacy more objectively. This has been completed with the multidimensional, type based system grounded in philosophy, law and social norms. This system enables privacy to be more objectively specified as the basis of this system being grounded in philosophy is embraced to the legal-social framework that the organization operates through norms and laws. From this understanding functional requirements and ramifications of choices are better enabled which assists in creation of more consistent, effective and robust privacy driven information system.

How an individual data item is classified is the first objective in the evaluation. To accomplish this goal a tool has been created. This tool incorporates the strongly typed systems of roles. Through its use the tool enables data to be classified into a privacy type through a review of the data item, the data source and job classification of the accessing party. This tool classifies the data item into a privacy type which in turn

specifies the level of control and access that are permissible to the data item by the job classification.

The privacy classification and the data classification tool enable a new direction to role based security to occur enabling a conceptual designed RBAC system that will provide a theory-based type system of access. Determining privacy through the classification of an item of data together with the role between the data donor and potential user will occur using the conceptualization of privacy proposed in Chapter 3. It will be shown that a theory based system of typed roles that mirrors the real world can be created with the classification system. Through their rich set of theory, rules, laws and directions this theory will be shown to provide a road map of acceptable access and privileges to objects that are meaningful at an organizational level and can be used within the database design process to more efficiently express the complex security policies necessary to meet corporate requirements. The result is a strongly typed system of roles offering robustness capable of handling a wide variety of situations. Finally it will be shown that this new conceptualization of roles enables a global top down approach in establishing access to objects and process upon those objects in the end improving both the design and implementation of database security.

As a proof, interviews have been conducted with stakeholders in a hospital setting to determine the existing security requirements and challenges faced to provision security. Initial interviews will take place of care givers across different hospital settings to determine the privacy needs of the medical profession. Next interviews were conducted with medical caregivers in a midsized hospital using a role

based access system developed by a third party vendor. As part of the interview process it was determined: what roles exist in this setting and how the role is provisioned with data - in particular what data is required by those roles including what operations can be performed on the available data. Next using the identified roles the accessibility and operations to data of various roles in a hospital setting were compared to the predicted accessibility and operations using the new construct and data classification tool of this proposal.

These examples conclusively demonstrate that the conception of privacy proposed in Chapter 3 can be expressed in terms of an artifact in the form of a classification tool. This tool enables data to be classified into relational, privileged, intellectual or secret data using the data value, data source and role. Once classified the functional specifications of the security system are established through applying the protections mandated by that classification of privacy. Finally it is demonstrated that the use of this tool can replicate the classifications used in the building of actual security systems.

Chapter 5: Design, Testing, Results

5.0 Introduction – Evaluation Design Science Framework

In design science it is not enough to propose a new model of privacy. Because the design science paradigm seeks to extend the boundaries of human and organizational capabilities this model needs to be developed into an artifact that can assist information systems to address problems and opportunities faced by the business organization (Hevner et al, 2004). A classification tool will be introduced that takes the conceptualized privacy types and enables the classification of data items into relational, privilege, intellectual and secret privacy [62]through an examination of three elements: the data item itself, the source of the data item and the role of the entity to which data is provided or is accessing data previously provided. The soundness of the tool is evaluated by conducting a field study which compares projected classifications using this tool, with actual classifications employed in a working EMR system built by a commercial manufacturer and modified by the users. Success will be determined by comparing the access and operations on data from existing systems designed without the classification tool and classification system with the access and operations that are predicted by this tool and classification system. These former systems are designed through and instance by instance developmental process that employs many man hours in the design and testing of each. Success will occur should the classification tool provide a similar classification because this classification tool would have

[62] Public privacy was not evaluated in this tool as public privacy is not a privacy type utilized by the organizational entity. Rather, public privacy provides the context in which all data is ultimately classified as private or non private.

accomplished the specification of privacy using far less time and effort that the traditional brute force instance by instance development which is currently deployed in the commercial development of privacy systems.

5.1 Operationalizing the Model

The tool determines a role's access to a data item using a three step process. First it classifies the transaction as a possession or a relational event by looking at the purpose for the exchange or access. Next, using this classification plus the data item, data source and job classification how the data will be used is next reviewed. This will result in an information privacy type classification of relational, privilege, secret or intellectual. The final step determines entitled to access of this role to the data item in question.

5.1.1 How to Classify Data

Prime Entities are entities that are a source of data. A Prime Entity can be a person, a data store or a record within a data store. A Prime Entity in the hospital setting is the patient as they provide information to the hospital. A second Prime Entity in the hospital setting is the patient medical record data store that is sought by various roles in the hospital that seek access to patient information. Patient information can be any information about the patient such as name, address or it can be patient medical information whether given by the patient to the hospital or obtained by the hospital through testing and conclusions.

Collection Entities can be of two types direct and indirect. A direct Collection Entity has a direct connection to the Prime Entity which provides the data. It can be a

role or an entity within a process or a process or it can be the data store of that information. The second types of Collection Entity have indirect connection. These are the processes or entities authorized to execute those processes that seek access to or control over data which has already been collected by the Collection Entity. These entities are frequently roles that hold permissions to access and control data necessary for them to execute a process or fulfill their role function. What distinguishes this type of Collection Entity is the fact they rely upon an intermediary to have collected the information of the Prime Entity as they do not have direct contact with the Prime Entity supplying the data. An example of such a Collection Entity in the hospital setting are the various caregivers (doctors and nurses) and support personnel (billing, accounting, records clerks) that must access the patient's information but access this information through the hospital record system rather than from the patient direct.

To determine what information is available to a Collection Entity a three step process is used. First the desired information is typed as Confidence or Possession. Next a privacy type is determined. In this step Confidence types can be Relational or Privilege privacy type while Possession type can be Secret or Intellectual privacy types. In the final step it is determined whether access is permitted or denied to the desired data.

The first step types the desired information as Confidence or Possession type. This is determined by the data item to which access is desired and the source (origin) of that item and looking to the motivation of the data recipient when data is exchange or to the motivation of the data accessor when data access is sought. In this step it is not

important that the data is being exchanged between the parties or that it is being accessed after an exchange has taken place. By way of example, a patient can provide information directly to the data store or a patient can have tests done which are reported to the data store through a reporting agency such as a lab which is later accessed by the doctor. In both the data source is the patient.

Figure 18 Desired Information

After identifying the data source and data item the first step is completed when the data is classified as being either a Confidence or Possession. Here we assess is the data sought, exchanged or accessed for the purpose to form, maintain or fulfill a personal relationship. If the information is sought for that purpose it holds the Intermediate classification as Confidence type. If the information is not exchanged or accessed for the purpose to form, maintain or fulfill a personal relationship it is classified as Possession type.

In discriminating between a possession or confidence information relationship the types of questions we could ask could include the following questions:

Confidence – If Yes	Possession – Yes
Is the character of the data provided personal on its face? Is it personal as to its provider?	Is the character of the data provided impersonal as to its provider?
Is it the intention of the Prime Entity that the exchange of information starts or maintains a personal relationship between the Prime and Collection Entity?	Is the intention of the Prime Entity that the relationship is to exchange information starts and maintains no personal relationship
Is the purpose of the Collection Entity in assembling this data one to establish or maintain a relationship	Is the purpose of the Collection Entity in assembling this data one to advance the acquirer's self interest solely?
Is the exchange of data conditioned on the premise that it will only be used to benefit and will be used to harm the Prime Entity?	Does the exchange of data come with no restrictions with the Collection Entity being allowed to do as they wish with the data?

Table 13 Confidence and Posession

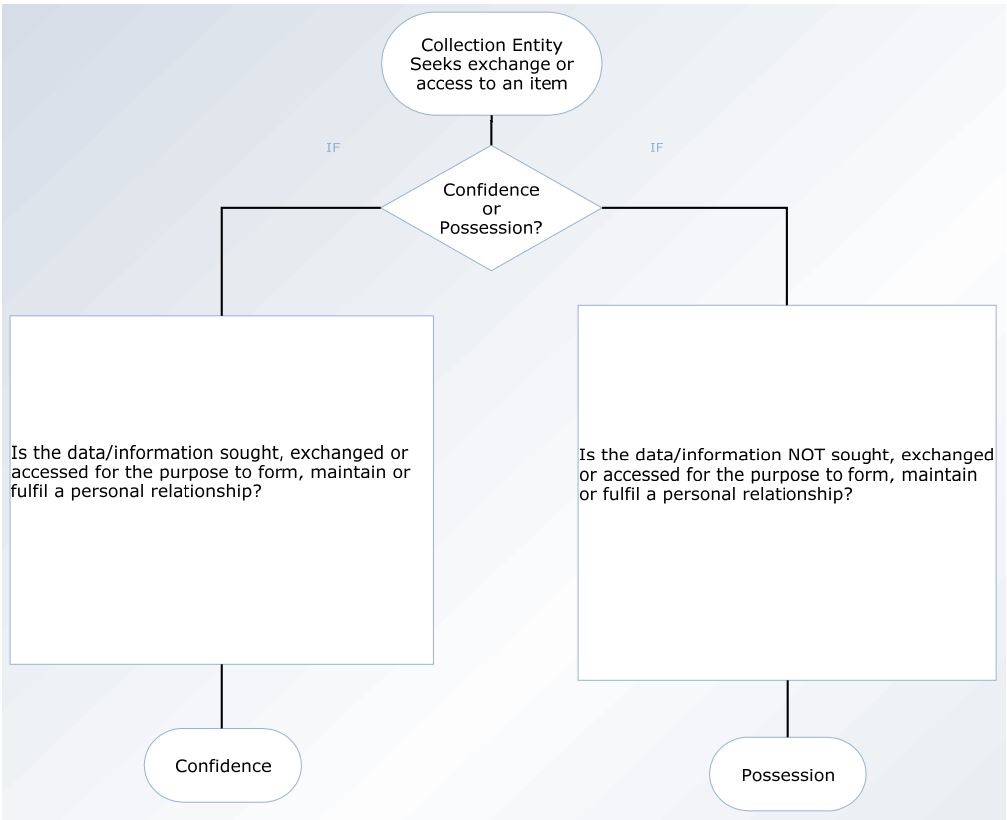

Figure 19 Collection Entity

In the second step a privacy type is determined. In this step Confidence types classify into Relational or Privilege privacy type while Possession type classify into Secret or Intellectual privacy types.

For the Possession type to we ask: Does the information advance or promote the proprietary interest of the organizational/individual entity, serve a purpose in the business pursuit or record the actions of the entity? If the answer is yes the privacy type is Secret privacy. If the answer is no the following question is proffered: Does the Information assist in the development of individual/organization or assist in the development of the organization/individual knowledge, skills or abilities? If the answer is yes the privacy type is Intellectual privacy type. If the answer is no to each type the data has no privacy type.

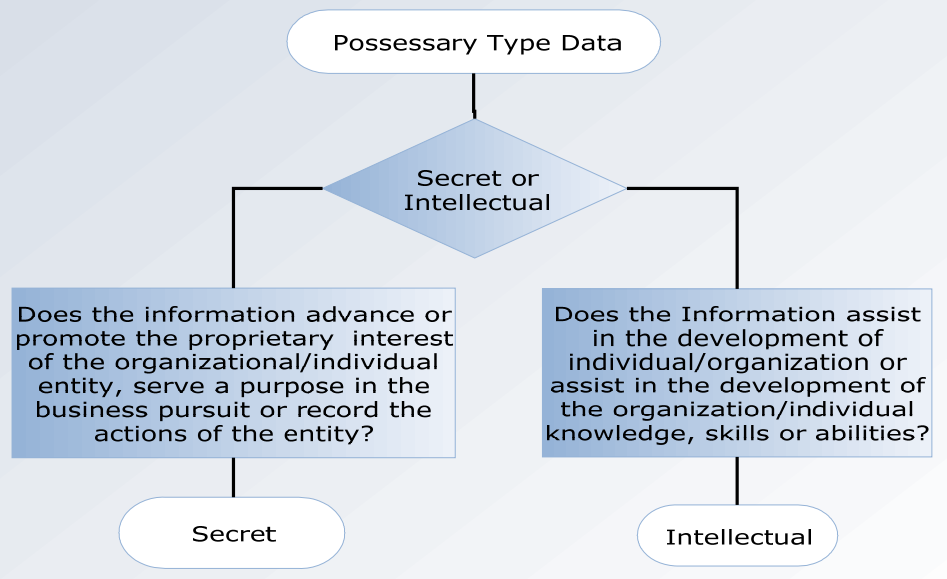

Figure 20 Possessary Type Data

Confidential information relationships can be classified as Privileged or Relational privacy type. The test for each privacy type here uses the same two questions:

1. Does the entity receiving or accessing this information possesses or is in the employment of or employ of person or persons that have professional expertise?
2. In the scope of this professional relationship is this data required as a direct input to perform some task that provides a direct or indirect benefit to the data provider?

If yes to each question, the classification is privilege but should the answer be no to one or both the classification is relational.

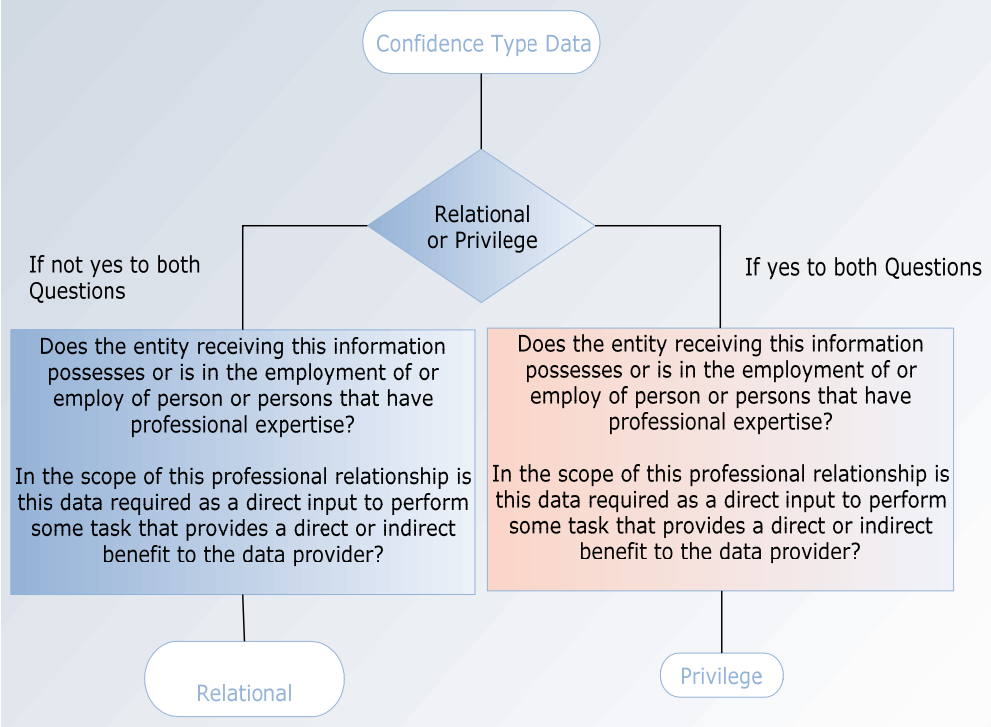

Figure 21 Confidence Type Data

The final step is determining whether access is permitted or denied to the role.

In all privacy types where data is exchanged between the source and accessor access is granted. In the situation where access of the data is sought post-exchange by an entity other than the one who originally received the data the original exchange relationship must be classified into a privacy type and access permitted no greater then that that type would allow or the privacy type of the classification made in step two.

Attached as Exhibit are Data Access Pattern of Control Hospital (Notes on CMH) and the predicted Data Access Pattern (Determining Level of Access)

Questions for the Classification of Data Type of an individual data item	
For Question 1: If data is being exchanged: Review the data item, data source and entity to which data is provided If data is post exchange and access is sought: Review data item, data source and entity which seeks access to data.	
Question 1a	Question 1a Is the data/information sought, exchanged or accessed is for the purpose to form, maintain or fulfill a personal relationship (Are we attempting the mutual exchange of personal information to form/maintain or fulfill a personal relationship?) If Yes Result = Confidence
Question 1b	Question 1b Is the data/information sought or exchanged NOT for the purpose to form, maintain or fulfill a personal relationship If Yes Result = Possession
For question 2: Look at the classification determined in Question One plus the data item, data source and job classification and ask:	
For all Confidence type ask:	Question 2a Does the entity receiving or accessing this information possesses or is in the employment of or employ of person or persons that have professional expertise? Question 2b Is this data required as a direct input to perform some task that requires professional expertise and provides a direct or indirect benefit to the data provider? If yes to Questions 2a and 2b the classification is privilege If no to one or both Questions 2a and 2b the classification is relational

For all Possession type ask:	Question 2e Does the information advance or promote the proprietary interest of the organizational/individual entity, serve a purpose in the business pursuit or record the actions of the entity? If Yes the classification is Secret Else: Question 2f Does the Information assist in the development of individual/organization or assist in the development of the organization/individual knowledge, skills or abilities? If Yes, Intellectual
Question 3 If Privilege	If privilege Question 2 c (1)Did this information originate in a relational privacy relationship? If Yes Is the disclosure of such information a compelling necessity that access should be granted? If yes ask Is access to this information minimally necessary to perform this job function for this entity/process If Yes to question 2 and 3 grant access but deny access if either or both question two or three are no. (2)Did this information originate in privilege privacy relationship? Is it with in the scope of the privilege to access and use this information? If yes ask Is information minimally necessary to perform this job function? If yes to both grant access if No to either or both deny access (3) Did this information originate in a secret privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. (4) Did this information originate in a intellectual privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. If no does the failure to disclose threaten or harm others or society in an unacceptable way. If yes access granted. If No Access denied.
Question 3 If Relational	If relational Question 2d (1)Did this information originate in a relational privacy relationship? If Yes Is the disclosure of such information a compelling necessity that access should be granted? If yes ask Is access to this information minimally necessary to perform this job function for this entity/process If Yes to question 2 and 3 grant access but deny access if either or both question two or three are no. (2)Did this information originate in privilege privacy relationship? Is it with in the scope of the privilege to access and use this information? If yes ask Is information minimally necessary to perform this job function? If yes to both grant access if No to either or both deny access (3) Did this information originate in a secret privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. (4) Did this information originate in a intellectual privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. If no does the failure to disclose threaten or harm

	others or society in an unacceptable way. If yes access granted. If No Access denied.
Question 3 If Secret	If Secret 2g (1)Did this information originate in a relational privacy relationship? If Yes Is the disclosure of such information a compelling necessity that access should be granted? If yes ask Is access to this information minimally necessary to perform this job function for this entity/process If Yes to question 2 and 3 grant access but deny access if either or both question two or three are no. (2)Did this information originate in privilege privacy relationship? Is it with in the scope of the privilege to access and use this information? If yes ask Is information minimally necessary to perform this job function? If yes to both grant access if No to either or both deny access (3) Did this information originate in a secret privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. (4) Did this information originate in a intellectual privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. If no does the failure to disclose threaten or harm others or society in an unacceptable way. If yes access granted. If No Access denied.
Question 3 If Intellectual	If Intellectual 2h (1)Did this information originate in a relational privacy relationship? If Yes Is the disclosure of such information a compelling necessity that access should be granted? If yes ask Is access to this information minimally necessary to perform this job function for this entity/process If Yes to question 2 and 3 grant access but deny access if either or both question two or three are no. (2)Did this information originate in privilege privacy relationship? Is it with in the scope of the privilege to access and use this information? If yes ask Is information minimally necessary to perform this job function? If yes to both grant access if No to either or both deny access (3) Did this information originate in a secret privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. (4) Did this information originate in a intellectual privacy relationship? If yes is this an appropriate entity or process to provide access? If yes grant access. If no access denied. If no does the failure to disclose threaten or harm others or society in an unacceptable way. If yes access granted. If No Access denied.

Table 14 Questions for Classification of Data

5.2 Empirical Study

As a proof, interviews have been conducted with stakeholders in a hospital setting to determine the existing security requirements and challenges faced to provision security.

The choice of the hospital was made as it would demonstrate the privacy types and would generalize well to other business entities. The hospital is constructed to bring together patient and caregiver to provide the highest level of care possible while maintaining the privacy of the patient. A hospital performs services that require very high levels of accurate, relevant data from multiple sources and locations to be provided in a timely manner to enable mission critical decisions. This information is also required in varying levels by all areas of the hospital entity to support the primary function of patient care. Primarily its actions are predicated upon information from its clients and the tests preformed on the clients. Through its systems and functions the hospital brings together the patient information with the requisite knowledge skills and ability of its physicians and staff to provide for these high levels of care while at the same time safeguarding the information about the patient and the actions of the hospital in serving the patient. Significant information flows come in and out of the hospital to provide for these services. In recent years actions to protect patient privacy have been enacted by the federal government due to patient information leakage to outside third parties.

Additionally hospitals are highly regulated by a variety of federal and local governmental agencies on a wide variety of areas including but not limited to having to meet reporting requirements for a wide variety of the activities and services it performs. All businesses have laws and regulations that impose both privacy and reporting requirements to some degree. While not every firm has the same requirements as a hospital to safeguard others information, financial firms (banks, accountants, brokerage houses, lawyers) have much the same requirements to safeguard client information yet report certain types of account activity. Increasingly the Federal Trade Commission is imposing requirements on the safeguard and use of client information by retailers. Homeland Security Act has imposed similar requirements on telephone, power and transportation companies. Aside from the mission critical decisions made in the hospital and the needs to safeguard patient information, many of these concerns are similar to the concerns faced by all businesses.

The goal of the study is to gather information from this type of entity. From this data a determination will be made whether organizational data can be classified into the privacy types of relational, privilege, intellectual and secret privacy types and that these types can be specified using a classification tool that determines existing access and operations on data. This field study would be accomplished through interviews of employees working in two hospitals. These interviews would determine the data needs of the organization and then examines individual data items with a view of how this data is made accessible to its members. Success will be determined by comparing the access and operations on data from existing systems designed without the classification

tool and classification system with the access and operations that are predicted by this tool and classification system If these sets are similar it would show that classifications hold and the tool could construct these types of privacy in a way that was useful to that business entity.

5.2.1 Interview Strategy

.A single interviewer conducted all rounds of face to face interviews. A script was used in each interview to ensure that the questioning was complete[63]. At every juncture effort was made to make the interviewee comfortable in order to get them to provide anecdotal information that would lead to new information and other sources of information. At each interview written notes were taken. Follow up was done on after all interviews. At times the notes taken were not clear or follow up questions presented themselves during the transcription process. Follow up was used in these cases to clarify points and to ask new questions. A second follow up was done with each interviewee where they were presented with the transcript of the notes taken and then given the opportunity to make changes or add anything they deemed noteworthy. Once the notes were all taken the interviews were compared for similarities and differences. Where differences were apparent, inquiry again was made in the attempt to gain clarification. Where differences persisted, the reasons for the differences were examined and noted. To deal with possible bias and guard against reporter error where ever possible multiple interviews were conducted across job functions having differing

[63] See appendix for the script

stakes in the data.[64] This data was then transcribed into tables indicating the job, data item and operations that could be performed on the data.

The first round of interviews was conducted at two hospitals both doctor driven but having differing approaches in how they classified, stored and made data available. The purpose of the first round was to determine the degree of sameness in approach to data and operations on data in particular common requirements, needs and challenges that hospitals faced with their data and information gathering, storage and dissemination. The second round of interview focuses on one hospital using an EMR. Particular attention was paid in these interviews as to the specific instances of regularly occurring access to the medical record and operations that can preformed on that item by the various roles enabled. This would provide a baseline for testing the model developed.

The same procedures were followed in each interview. Unless the interviewer was the hospital administrator themselves, the interviewee was instructed by his immediate supervisor that he had the permission from the hospital administrator to cooperate fully in the interview process. A private location was provided for the interview to take place on hospital premises during the interviewee's regular work schedule. With the initial exception of the interview with the IT staff during the second round, and the interview with one hospital administrator and his chief security officer, every interview was a one on one interview. With the IT Staff, it was the suggestion of

[64] When Risk Management was consulted only a single interview was permitted with its Director. The interview was very limited with the Director providing he has access to everything and every body at any time.

the IT administrator to meet initially with the whole staff to discuss the issues and for the interviewer to get a more global perspective of the hospital's strategy. A four hour interview of the entire staff took place using open ended questions and following up on their discussion of the question presented. At the conclusion of that interview, each staff member was made available for individual follow up questions.

During the entire interview process a variety of roles were interviewed including the Hospital Administrator, Assistant Hospital Administer, IT director, Chief Security Officer, HIPAA Compliance Officer, DBA, Chief of Software Support, the entire IT department and the various users throughout the hospital including nurses from all levels, doctors, clerical, laboratory staff and supervisors, department heads and their staff. A significant amount of the interview time was centered on three positions: the Chief Security Officer, the HIPAA Compliance Officer, and the Chief of Software Support.

In the first round the interviews were conducted with two different hospitals and two different people from each hospital. Prior to the interview a meeting took place between the interviewer and the Hospital Administrator. During this meeting the administrator was informed that the thrust of the interview was concerning the data of the hospital, how it was generated, stored, made accessible and protected. The administrator then provided people with the requisite knowledge and expertise to answer these types of questions. From each hospital the Assistant Hospital Administrator who supervised the data and privacy protection aspect of the hospital was made available to provide answers to these questions. Additionally the each

hospital provided one additional person. One hospital provided their Chief Security Officer. The other hospital provided their HIPAA Compliance Director. Interviews with the hospital providing the Chief Security Officer took place with the assigned Hospital Director present and participating. This interview was conducted over a four hour time period with breaks taken every 45 to 60 minutes. . The majority of the information did come from the Chief Security Officer because he was more familiar with the information sought. It should be noted that during this interview both provided information to each question when they had differing viewpoints or additional information. In the interviews with the other hospital, separate interviews were conducted with the Assistant Administrator and the HIPAA Compliance Officer. Like the previous set of interviews, the HIPAA Compliance Officer possessed the majority of the information with the Administrator referring often to the HIPAA Officer as having the more informed answer. The interview with the HIPAA Compliance Officer took place over three separate days approximating 2 hours each day. The interview with the Assistant Hospital Administrator took place one day for approximately one hour.

In the second round the roles interviewed were expanded to admission, unit secretary, unit nurses, unit supervisors, nurse managers, director of nursing, chief nurse, doctors, various laboratory units, and research.In this round while every role contributed strong information, the Chief Software Support provided the vast amount of information. In part it was due to the design of the work system at the hospital and in part this was due to security concerns of the interviewee. The Hospital Administrator and HIPAA Compliance Officer were very concerned that any role be aware only of the

access patterns of the areas with in their control. Enabling an open inquiry beyond the Chief Software Support was a concern that this would be compromised. To accommodate the hospital when interviews were conducted with personnel other then the Chief Software Support, while conducted in private, the inquiries were very limited in the terms of open ended questions of asking what data was accessible to them and what operations could be performed. Additionally through agreement with the interviewing entity, all access patterns disclosed regardless of source were only reviewed by the Chief of Software support.

Additionally it should be noted that the hospital in the second round of interviews had three access systems: patient care, risk management, research. The Chief of Software Support by design was the chief officer in the hospital over the data access of the EMR only. The other two information access systems, one for hospital research and the other for risk management were separate access systems with different individuals in control over these schemas. The risk management and research systems are not a part of the study.[65]

5.2.2 Distinctions between the two hospitals

Both hospitals are doctor driven and held a commitment to patient care. The privacy of patient information was a vital concern as well for similar reasons: preservation of the traditional doctor patient relationship, a condition for high quality care and the threat of a law suit and financial loss should this duty become breached.

[65] It should be noted that a select group has access to all systems. By design the Chief administrator of the hospital, the chief of risk management and the chief resident were the only roles that had global access to all three systems. No interviews of substance were conducted with any of these individuals.

Each hospital was distinctive in how they approached these issues. One hospital was in the early stage of conversion to an EMR system. From interviews with the IT director, Chief Security Officer and its HIPAA Compliance Officer it was learned that this hospital was using a paper based medical record that was powered by people. In this system the entire staff was trained in the rudimentary issues of privacy. Certain key people were targeted and provided extensive training to enable them to protect and enforce the privacy policy of the hospital with respect to its medical records. This group each performed a job function of a record custodian of some type or could provide gatekeeper functions to the patient record. At the other hospital interviews were conducted with the Assistant Hospital Administrator and the HIPAA Compliance Officer. From these interviews it was learned that they had purchased an EMR from a commercial vendor and implemented the system approximately two and half years earlier. This EMR was a semi customized system that permitted further customization after delivery. At this hospital it was disclosed the customization of this system was still on going with the IT staff still in the process of producing changes to the system.

These interviews were summarized and reviewed by the author. Next interviews were undertaken with the hospital using the EMR where efforts were undertaken to determine which roles had access to data. From this information the privacy model would be compared.

5.2.3 Conclusions of the First Interviews

Interviews from both hospitals provided evidence that both were concerned with privacy protection. In both hospitals privacy types were not used. Instead private data

was treated as either being patient health information or not patient health information. While each had similar access policies to the medical record both differed when access concerned non PHI data. This is particularly true in the cases of employee records and benefits and hospital administration. However despite these differences, the hospital users using the paper based system experienced greater satisfaction in having access to needed medical information despite the expression of concerns of time delays in getting the information. Users of the EMR based system expressed satisfaction with the speed they received records but were frustrated with the system. The basis of concern was due to two factors: “black holes” that prevented access to needed information and “white holes” that lead unauthorized people to protected data.

The administrators of hospital using a people powered- paper based system felt to a degree they had some risk exposure as the entire record was potentially exposed. They openly acknowledged there was no real simple way to restrict access to the file once it was out of the record custodian possession. They believed however the commitment of their people to patient privacy reduced that risk to acceptable levels.

Despite the differences between the hospitals neither was distinctive in its information needs. Each faced the same issues of making available data to appropriate persons and processes while maintaining the privacy of the data. Each has high concerns that this data be safeguarded as patient data carries with it an obligation of protection. This is interpreted by each to require that once patient data was within their grasp, they must judiciously control that data. Secondly each viewed access as given

only to necessary persons and processes in an amount reasonably necessary for a defined task to be performed.

The following observations were made from the interviews of both hospitals:

It is well accepted that high quality healthcare is delivered when appropriately trained personnel are coupled with timely information necessary to meet the health challenge. The challenge to provide this information is the high volume of data, information and knowledge that emanates from a wide variety of sources both within and without the treatment facility and which continues to grow exponentially. This data is required to drive the various functions of the hospital – from patient care, to billing, to research to compliance with governmental regulations – each which can change circumstantially. Often to accomplish these purposes a piece of data passes through many individuals, departments, organizations and governmental agencies many of which have conflicting agendas and goals. Unless safeguards are imposed the privacy expectations that surround that data can be easily compromised. All of this requires the highest efforts be undertaken to enforce the privacy expectations of the patient and his health care providers. Yet even providing this and imposing the best safeguards privacy expectations of the patient and health care providers are often compromised.

In recent years new challenges have emerged. An increased coupling between medical care and insurance together with the emergence of medicine emerging as a business has increased the portability of medical information outside the hospital most notably to insurers and medical reviewers. To counter act the portability, new laws and regulations regarding patient medical information are being proposed and enacted. It is

imperative to keep up with these changes particularly as patients and their significant others are more willing today to seek financial remuneration when disclosures of patient information is improperly made or high standards of patient care is not achieved. Oftentimes these actions become coupled with additional financial repercussions in the form of increased insurance premiums, loss of key personnel, the inability to attract talent, loss of funding or sources of funding or loss of trust and standing in the community the hospital serves. As a result there is a push to provide greater managerial control over the hospital operations to minimize risk and the risk of loss. To accomplish this objective will require greater access to patient information by non treating personnel which will further drive this cycle.

Automation of data access is the most viable way to address the above stated concerns. While these systems generally work well they are not a panacea. First they are expensive to roll out largely due to the complexity necessary to meet the tasks at hand and not possessing the expertise and knowledge needed both technically and legally. Second many times functionality must be sacrificed at the expense of development and the risk of failure. Finally, after roll out an almost endless stream of maintenance must be done in part to correct issues that were inherent with the rolled out system and in part to implement changes necessary to keep up with the ever changing social, business and legal environment that the hospital functions.

5.2.4 Conclusions from the Second Round of Interviews

Before purchasing an EMR system many alternatives were considered including staying with the old paper based system, the costs of in house development and the

attractiveness of obtaining a customized system. Factors including the risks inherent with the paper based people automated system, the need for faster access to information, the size and expertise of the IT staff, and the large volume of information and access patterns to be analyzed and determined were prime factors that motivated the decision to obtain an semi customized EMR through a vendor.

Since the system has been delivered the results obtained have been disappointing. In the months following the installation the system lacks the desired and specified functionality. In particular, access to data is inconsistent among caregivers similarly situated. Often when access is provided it is seldom optimum and is usually either under or over established. Existing work patterns in the hospital had to be altered to fit the acquired system because it could not be easily altered to support the desired work flow pattern without substantial rework. In some cases the staff have initiated work-a-rounds that subterfuge the security of the system. Even when rework is possible before a project is reworked it must higher priority over all other projects before it is initiated. Even when change is initiated frequently the change is an iterative process until the desired level of functionality is received or the project is abandoned. In any rework of access, before the project is finalized months are taken waiting for supervisors and legal to approve the changes while they examine the exposure of risk and consider other alternatives.

Daily changes must be made to the EMR. A person’s absence due to vacation, illness, relocation, or firings often lead to vast areas of needed information either becoming inaccessible for day to day operations (including routine patient care) or the

checks that ensured control over information and limited information access becoming disabled. In many cases the reassignment of the absent person's role permits too great of access or eliminates the required people controls that supplement the controls imposed by the EMR. Under these circumstances when assigning information access, traditional access patterns are generally applied to determine what data is needed to carryout the job by that level of employee. All too frequently ad hoc emergency measures are implemented that provide or stop the flow of data without a proper examination of the risk. Increasingly classifications are becoming less clear with new job classifications emerging, new uses of information that require access to be expanded, changes in laws and regulations that dictate changes in access, and heightened concerns over privacy which forces a rethinking of the traditional access patterns.

Change in the external environment will initiate required changes in the EMR. Proposed and actual changes in regulations and laws require access patterns be reviewed almost continuously. Often this results in a substantial reworking of system access across the hospital subject to examination by the administration and legalHi. While laws and regulations provide performance directives they provide no guidance on how these directives translate into required system changes. These changes are initially implemented using the best practice of limiting access while the redesigning process constructs alternative access patterns. This often limits functionality and utility to levels below that which is both required and desired by users for many months while measures are designed and tested.

5.3 Evaluation

A review was taken of the data collected by the hospital entity and the access patterns permitted through the commercial system. It was decided to take a patient record as it was built through the system and see how the model compares with the specifications of the commercial system. The chart of questions in Section 5.1.2 were asked and applied by job description to each pair of information/source of information. The following chart records those results and makes posting of results less unwieldy.

Data Item	Source	Question asked/Result	Second Question asked/Result

Table 15 Results

5.3.1 Admissions Clerk

In the interviewed hospital, one method a patient enters the hospital is through a referral from a physician. On the assigned date and time, the patient presents themselves to the admission clerk. In addition to the patient's name address and telephone, information about the method of payment, insurance, various consents and the doctor's orders are disclosed to this clerk. When the procedure is completed the patient is admitted to the hospital and assigned a bed by the clerk. In the commercial system, after admission this clerk has access to each of these items but is unable to see previous visits or the medical record of those visits. Neither is the clerk able to access the patient record as it accumulates during this visit.

The following table contains the results and predicted access for the Admission Clerk:

*Where tool and hospital access are identical the final column value will be **bold.***

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name Patient address	Patient	1a/Confidence	2a yes/2b no Relationship	2d(1)Access Granted
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	2d/(1)Access Granted
Bed Assigned	Hospital	1b/Possession	2e/Secret	2g (3) Yes Access Permitted
Dr Order	Doctor	1a/Confidence	2a yes/2b yes Privilege	2c(2)/Access Granted

Table 16 Tool and Hospital Access

Discussion of results for admissions clerk

The tool classifies access identically to that used by the hospital.

Patient name and address classified as relational. Relational privacy requires control and access be maintained. The level of control is respect which requires that the obtained information must be controlled for the benefit of the information provider. The control further protects the control over information by collecting only information reasonably necessary for the relationship. Here the clerk collects only that minimal information necessary to create a relationship between the hospital and patient and that this information is controlled for the information provider's benefit. Access to this type of information is limited to a compelling necessity. The compelling necessity in this case is the need to ascertain the correctness of the name and address.

Insurance information was also classified as relational. The purpose of learning about a patient's insurance information on part of the hospital has many functions including do we offer services to them and at what level is service provided. The call between relational and privilege was tougher to make. A good argument can be made that whether insurance is available or not is a direct input to perform medical treatment. The decision to classify this as relational was made because it appears this question is more germane to the relationship formation rather than the treatment given after the relationship is formed.

This item can be assessed in two ways. One, insurance determines whether the relationship is even entered into. Two, insurance determines the type of care given during the relationship. Some hospitals will not take private pay patients. Others take patients who don't have insurance but the care given follows a different protocol from that of the insured patient. A third class of hospital would accept the patient regardless of having insurance and would not differentiate in care given. Does a better operational definition need to be made for the tool or do the facts of the hospital govern the classification?

Bed Assigned classifies as possession/secret. It is possession at it is non personal information. It is secret as it is a record of the actions of the entity. This is unique as it is a permitted operation on data rather than an access operation to data. Additionally this assignment is based upon the operations of the entity and as a result is promoting the proprietary interest of the hospital.

Dr. Order is confidence/privilege. It is confidence because it is personal information necessary to form a relationship. It is privilege as the clerk is in employ of person's who have professional expertise and it is a direct input into the task of providing care to the patient. This type of information requires this information be safeguarded and access be that of minimally necessary. Here out of necessity the clerk must have access to this information as they are the interface between the hospital and patient and this information enables the clerk to perform the functions of that position.

Note there is not any example to demonstrate intellectual privacy for this job description. This is likely to the low level of importance that this job has in the hospital.

5.3.2 Unit Secretary

Unit secretaries function as the clerical staff for the hospital. A unit secretary is assigned to a specific unit in the hospital for her shift. This assignment can change daily. They report to all nurses assigned to the unit as well as all doctors who have patients in the unit. Generally a unit secretary has full access to general patient information and limited access to patient care information. The general rule is the unit secretary can only access and update information for a patient in their assigned unit however; the EMR can see and write to any patient in the hospital. General information is considered to include the ability to read and update patient demographics, church affiliation, opt them out of general census, place staff alerts, and identify next of kin. Additionally they can pull a current visit history (when admitted, how admitted, bed assignments and transfers, account number) but cannot look at past stays in the hospital. Cannot change phone number

Patient care information to which this position can read and write includes the current care given to the patient both from the nurse and the doctor but they are not supposed to have access to any lab test results.[66]

[66] Because this hospital employs a redundant system of faxing results to the unit as well as placing the results in the EMR, the unit secretary does in fact have access although it is not desired that they have access to these lab results.

The following table contains the results and predicted access for the Unit Secretary:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	2d (1) Access Permitted
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	2d (1) Access Denied
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	2d (1) Access Denied
Patient bed assignment	Hospital	1b/Possession	2e Secret	2g (3) Access Permitted
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	2d (1) Access Permitted
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	2c (2) Access Denied
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	2c (2) Access Denied
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	2c (2) Access Denied
Doctors order of a patient not in unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	2c (2) Access Denied

Table 17 Unit Secretary Results

Discussion of results for unit secretary

The tool classifies access for patient demographics, patient bed assignment, next of kin, nursing notes, doctors' orders and lab tests identically to that used by the hospital in all cases. However in two cases – Lab tests and doctors orders of a patient not with in a unit, while the tool classifies the information as privilege, the business rule

of the hospital forbids access by the unit secretary because the patient is not in the care of that unit. Privilege privacy requires that before access is provided it must be assessed whether this is an appropriate individual/organization to provide access to information taking into account that access must be limited to that minimally necessary to carryout a job function. While the tool asks this question it fails to predict this access and demonstrates one of the limitations of the tool – before final classification can be made it is imperative that the business rules of the organization, conventions of the industry and even common sense be looked at when making this final determination.

5.3.3 Unit Nurse

Unit nurses provide care for patients in a specific care unit of the hospital. Some care units are specialized such as CCU, ICU, EMR and Cardiac Care. The majority of care units handle the general population of the hospital.

Distinction is made in the hospital between general and patient care information. General care information includes staff alerts, gender, date of birth, admit date, medical record number and account number all of which is accessible to a unit nurse. Patient care information includes diagnosis, nursing notes and doctor orders for care. The nurse cannot access the results of any lab tests but can see if a lab results have come in. An interesting side bar is the unit nurses only see patients assigned to the unit unless they are assigned to the EMR where can see the whole house.

The following table contains the results and predicted access for the Unit Nurse:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	Source	First Question asked/result	Second Question Asked/Result	Third Question Asked/Result
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Denied**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Denied**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders of patient within the unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors order of a patient not in unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Denied**
Patient care information after patient is discharged or removed from unit	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) No access Denied**
Other employee work schedule	Hospital	1a/Confidence	2a Yes 2b No Relational	**2(3) No Access Denied**
Other employee vacation benefits	Hospital	1a/Confidence	2a Yes 2b No Relational	**2d (3) Access Denied**
Information on how scheduling must take place	Hospital	1b/Possession	2e Yes Secret	**2g (3) Access Denied**

Table 18 Unit Nurse

For the general and personal care information the tool classifies access identical to the hospital examined with the exception of lab tests. The hospital examined did not permit the nurse access to the result of the test but did permit them access to information that the lab test results were in. This aberration appears to be in the business rules of the hospital where they want to keep information the nurse receives to the minimum necessary to do the job and it is believed that this is not necessary to do the job.

Another area of interest is the work schedule and vacation benefits. Hospital forms the relationship with the other employee. That relationship is confidence. In a confidential relationship the hospital must exercise a high level of control over that information type of information. When the employee seeks information concerning another employee work schedule or vacation benefits, this type of a relationship is a confidence type because this information is not for the purpose of forming, maintaining or fulfilling a personal relationship. This in turn classifies into relational privacy type. Because of the requirements of instituting a high level of control, unless a compelling necessity is shown, no access can be provided. When looking at how scheduling must take place the information is of possession type as it does is sought not to form, maintain or fulfill a personal relationship. This in turn is the type of information that would promote or advance the proprietary interest which translates into a secret privacy relationship.

5.3.4 Unit Supervisor

Unit Supervisors have access to all the general and patient information that a unit nurse has with this exception: A unit supervisor in general can see only their own patients information after the patient leaves the unit for so long as they remain a in the hospital for this visit. The one notable exception is the of the EMR supervisor who can see any patient in the hospital. When a patient is discharged the ability of all these supervisors to view the patient's general and patient information ends.

The following table contains the results and predicted access for the Unit Supervisor:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Permitted**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Permitted**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes	**2c (2)**

			Privilege	**Access Denied**
Doctors order of a patient not in unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Denied**
Patient care information after patient is discharged	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Denied**
Patient care information after patient removed from unit but remains in the hospital	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2)Access Permitted**
Employee work schedule	Hospital	1b/Possession	2e Yes Secret	**2g Access Permitted**
Employee vacation benefits	Hospital	1b/Possession	2e Yes Secret	**2g Access Permitted**
Information on how scheduling must take place	Hospital	1b/Possession	2e Yes Secret	**2g (3) Access Permitted**

Table 19 Unit Supervisor

The Unit Supervisor has greater access to patient's general and care information over the unit nurse in that they can view the patient throughout the hospital provided they once resided on the floor. Looking at work schedules and vacation benefits of other employees this information is relational from the viewpoint of the employee but secret from the viewpoint of the supervisor. The unit supervisor requires this information in order to enable the management of personnel. Still the disclosure of information must be limited in part because of the 'secret nature' of the information but also because of the interest of the employee in not having this detail of his work known

by others. Finally information on how to schedule is available to the supervisor as they require this guidance on how to set forth coverage on the unit. This is an element of know how which requires protection.

In all ways the access patterns of the tool are consistent with the developed system.

Except for the lab test the tool classifies access identical to the hospital examined. As stated before the hospital examined did not permit the nurse access to the result of the test but did permit them access to information that the lab test results were in. This aberration appears to be in the business rules of the hospital where they want to keep information the nurse receives to the minimum necessary to do the job and it is believed that this is not necessary to do the job.

5.3.5 Nurse Manager

Nurse Managers have specific areas of authority. In the hospital interviewed there were six nurse managers one each over the following areas: ICU, CCU, EMR, Operating Room, Recovery Room and Same Day Surgery. These individuals require a greater global picture of the hospital in order to fulfill their supervisory duties.

The Nurse Manager has access to general and patient information of any patient who has ever been in their unit even after the discharge of the patient from the hospital. The one exception is the EMR supervisor who can see any patient in the hospital as it is deemed imperative they have global access to all patients in order to provide requisite levels of care. Because nurse managers are involved in quality control, nurse managers have access to the entire health record of the patient. Additionally this position has

expanded capabilities in the management of personnel. They can see the time records, job history, supervisor comments and actions and work schedules current and past. Additionally they have limited access to benefits such as seeing taken vacation days, sick days but they cannot view the total sick days and vacation days an employee has in their benefit package. As to the personnel record the only item that is accessible is the employee phone number.

The following table contains the results and predicted access for the Nurse Manager:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Permitted**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Permitted**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2)Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Denied**

Doctors order of a patient not in unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) provided patient was in their unit at some point**
Patient care information after patient is discharged or removed from unit	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Patient care information of a patient not ever in supervisor's unit (Still in hospital)	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (1) Depends if patient was ever in the supervisors unit. However EMR supervisor can see this information regardless**
Employee work schedule (Own)	Hospital	1a/Confidence	2a Yes 2b Relational	**2d (1) Access Permitted**
Employee vacation benefits (Own)	Hospital/Employee	1a/Confidence	2a Yes 2b Relational	**2d (1) Access Permitted**
Employee total vacation benefit (own)	Hospital/Employee	1a/Confidence	2a Yes 2b Relational	**2d (1) Access Denied**
Employee vacation taken	Hospital/Employee	1b/Possession	2e Yes Secret	**2d (1)Access Permitted**
Employee total vacation benefit (not own)	Hospital/Employee	1b/Possession	2e Yes Secret	**2d (1) Access Denied**

Pay level of employee with in unit	Hospital/Employee	1b/Possession	2e Secret	**2g (1)Access Permitted**
Pay rates associated with pay level	Hospital	1b/Possession	2e Secret	**2g (3) Access Denied**

Table 20 Nurse Manager

Discussion of the results of Nurse Manager

The tool produces access patterns identical to that of the commercial system. Looking at the relationship of the Nurse Manager to the vacation, pay level and rate of pay produces a good example of how the tool approaches the sensitive area of employee benefits and pay. While the information exchanged between the hospital and employee in this area would classify as confidence/relational as to those individuals when looking at the Nurse Manager accessing this information it becomes apparent in this relationship that this data holds a different privacy relation. To the Hospital/Nurse Manager relation this information is a possession type which translates into secret data as it promotes its proprietary interest and serves a purpose in the business pursuit of the hospital. Because the information sought to be accessed is relational information a constraint is placed upon the Hospital providing ready access to this data. Instead the hospital must exercise the level of control over the data and permit access no greater then the level permitted at the relationship level. Relationship data is accessible to others only upon compelling necessity and then this must be examined from the stand point of is this an entity to which access should be allowed. The compelling necessity is provided by the need to supervise employee's benefits and pay. The difference in

access comes from the question is this an entity to which access of this information is appropriate. Business rules, industry conventions and common sense will dictate the appropriate access. However these same rules and conventions will be testable through the performance requirements for each type of privacy. For the vacation days taken and the pay level it is appropriate to allow access. For the days left and the rate of pay this level of employee is not appropriate to have access to this information.

5.3.6 Director of Nursing

The Director of Nursing has the same access to general and patient care information as does the Nursing Manager – they can see any patient who has been in any unit they have supervision over even after the patient leaves the unit or is discharged from the hospital and they have have access to the entire health record of the patient because they are involved in quality control. The director in charge of the EMR still has access to all patients regardless where they are resident in the hospital. The second difference here with the Director of Nursing and the Nursing Manager is what employees they can see and do reports on. This level has access to the entire nursing staff including all supervisors in their department but they cannot see pay rates, benefits, unused sick or vacation time.

The following table contains the results and predicted access for the Director of Nursing

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Permitted**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Permitted**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors order of a patient not in unit	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) provided patient was in their unit at some point**
Patient care information after patient is discharged or removed from unit	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Patient care information	Patient	1a/Confidence	2a Yes 2b Yes	**2c (2) Depends if**

of a patient not ever in supervisor's unit (Still in hospital)			Privilege	**patient was ever in the supervisors unit. However EMR supervisor can see this information regardless**
Employee work schedule (Own Employee)	Hospital	1a/Possession	2e Yes Secret	**2g (1) Access Permitted**
Employee vacation benefits (Own)	Hospital/Employee	1b/Possession	2e Secret	**2g (3) Access Permitted**
Employee total vacation benefit (own)	Hospital/Employee	1b/Possession	2e Secret	**2g (3) Access Permitted**
Employee vacation taken	Hospital/Employee	1b/Possession	2e Yes Secret	**2d (3) Access Permitted**
Employee total vacation benefit (not own)	Hospital/Employee	1b/Possession	2e Yes Secret	**2d (1) Access Denied**
Pay level of employee with in unit	Hospital/Employee	1b/Possession	2e Secret	**2g (1) Access Permitted**
Pay rates associated with pay level	Hospital	1b/Possession	2e Secret	**2g (3) Access Denied**

Table 21 Director of Nursing

The classification tool largely follows the classification schemes of the other job functions with the exception of employee vacation taken, remaining vacation time pay level of employee and pay rates associated with pay level. Vacation taken, vacation remaining, pay rate and pay classification present a challenge in classification. From the vantage of the employee, this can appear to be a relational type of privacy. Yet from the vantage of the hospital entity this can be a form of secret privacy as it can demonstrate the strategy of the hospital entity in the way of staffing and cost that must be expended. How to approach this is not as straight forward as many other determinations. The decision was made to classify this as a secret and allow access to reflect the relational aspect between the hospital and employee to that of not revealing this unless compelling necessity was demonstrated. Here again the tools classification is 100% agreement with the hospital system.

5.3.7 Chief Nursing Officer

The Chief Nursing Officer is the highest nursing position in the hospital and is considered on level with the executive suite. As a result a chief nursing officer has access to every piece of information related to the patient both past and present and full access to all employee records with the exception of other executives records. Additionally due to their involvement in the financial aspects of the hospital, the CNO has access.

The following table contains the results and predicted access for the Chief Nursing Officer:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Permitted**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Granted**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Permitted**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors order of a patient not in unit of direct supervision	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Patient care information after patient is discharged or removed from unit	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Patient care information of	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access**

a patient not ever in the hospital during this employees tenure				**Permitted**
Employee work schedule	Hospital	1b/Possession	2e Yes Secret	**2g (1) Access Permitted**
Employee total vacation benefit	Hospital	1b/Possession	2a Yes Secret	**2d (1) Access Denied**
Pay classification of employees non executive	Hospital	1b/Possession	2e Yes Secret	**2g (1) Access Permitted**
Pay rates of employees (non executive)	Hospital	1b/Possession	2e Yes Secret	**2g (3) Access Permitted**

Table 22 Chief Nursing Officer

Chief Nursing officers have broad duties that require access to information throughout the hospital. Because of their high status as supervisors they are entitled to access to almost every bit of information in the hospital.

Work schedule pay rate and pay classification present a challenge in classification. From the vantage of the employee, this can appear to be a relational type of privacy. Yet from the vantage of the hospital entity this can be a form of secret privacy as it can demonstrate the strategy of the hospital entity in the way of staffing and cost that must be expended. How to approach this is not as straight forward as many other determinations. The decision was made to classify this as a secret and allow access to reflect the relational aspect between the hospital and employee to that of not revealing this unless compelling necessity was demonstrated. Using this type analysis

permitted agreement between the tool and the hospital. Agreement for this role was identical to the commercially developed system.

5.3.8 Doctor accessing Patients

Doctors have complete access to all medical records of their own patients but when viewing other information, it is restricted. In the hospital studied a doctor could not view another doctor's patient unless he was provided permission by the patient's doctor.

The following table contains the results and predicted access for the Doctor:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Permitted**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Permitted**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Lab tests	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**
Others Doctors' patient not this doctor's patient and no permission	Patient	1a/Possession	2e Yes 2f Yes Privilege	**2c (2) No access permitted**
Patient care information after patient is discharged or removed from unit	Patient	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted**

Table 23 Doctor-accessing Patients

For the most part the tool predicts access identical to that permitted. From interviews of both hospitals and interviews of various doctors, there appears to be no set way in which doctor's access to a patient not their own is covered. Each hospital was adamant that post HIPAA unless permission was given no doctor saw another doctor's patient record without permission. However when carefully looking at the access mechanisms these permissions are often loosely handled. In other cases the business rules of the hospital favored access to all patients by a doctor with precaution taken of accounting for access and actions. This laxness is often to account for how doctors will cover for one another. Another reason for the laxity are two reasons: the great amount of trust a hospital has that the doctor will not abuse his authority in this area and the power the doctors wield over the hospital often makes the hospital provide to the doctor mechanisms that potentially expose the hospital to loss.

5.3.9 Lab

Lab personnel have very limited access to general patient information – this is limited to patient name, account number, date of birth and gender. As to patient care information, it receives only what the doctor directly sends the lab in the form of a doctor's order for a particular test.

The following table contains the results and predicted access for the Lab:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1a/Confidence	2a yes/2b No Relationship	**2c (1) Access Permitted**
Patient Address	Patient	1a/Confidence	2a Yes/2b No Relationship	**2d (1) Access Denied**
Insurance Information	Patient	1a/Confidence	2a yes/2b no Relationship	**2d (1) Access Denied**
Patient bed assignment	Hospital	1b/Possession	2e Secret	**2g (3) Access Permitted**
Next of kin	Patient	1a/Confidence	2a Yes 2b No Relational	**2d (1) Access Denied**
Nurses notes	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Denied**
Doctors orders	Hospital	1a/Confidence	2a Yes 2b Yes Privilege	**2c (2) Access Permitted only for test order all other is denied**

Table 24 Lab

Doctor's orders are not always accessible to the lab. In the interviews taken in most cases the only doctor order the lab sees are the orders for the test. However in interviews with the lab supervisors and the doctors both stated that at times the lab personnel want more in the way of a history on the patient than is contained in the doctor order. In this situation (which is rare) the lab and the doctor will consult and the doctor will provide to the lab the precise medical history or patient medical information that the lab seeks in order to provide the lab sufficient background to effectively

administer the testing. The tool in this scenario classifies data in ways identical to the commercially developed system but does not account for the work around devised by the hospital staff.

5.3.10 Risk Management Team

The risk management team is a separate function inside the hospital whose purpose is to identify potential risks and then eliminate or limit the risk exposure. Because risk can appear in any department and in many different forms the members of the risk management department have broad reaching powers that approximate or even exceed that of the executive management in the hospital.

The following table contains the results and predicted access for Risk Management:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1b/Possession	2e/Secret	**2g(1) Access Permitted**
Patient Address	Patient	1b/Possession	2e/Secret	**2g(1) Access Permitted**
Insurance Information	Patient	1b/Possession	2e/Secret	**2g(1) Access Permitted**
Patient bed assignment	Hospital	1b/Possession	2e/Secret	**2g(3) Access Permitted**
Next of kin	Patient	1b/Possession	2e/Secret	**2g(1) Access Permitted**
Nurses notes	Hospital	1b/Possession	2e/Secret	**2g(2) Access Permitted**
Doctors orders	Hospital	1b/Possession	2e/Secret	**2g(2) Access Permitted**
Lab tests	Hospital	1b/Possession	2e/Secret	**2g(2) Access Permitted**
Doctors order of a patient not in unit	Hospital	1b/Possession	2e/Secret	**2g(2) Access Permitted**
Patient care information after patient is discharged or removed from unit	Patient	1b/Possession	2e/Secret	**2g(2) Access Permitted**

Table 25 Risk Management Team

Risk management seeks data not to form a personal relationship but to protect the hospital entity from real or potential loss. Using any data but particularly personal

data that is classified as relational or privileged becomes an important basis of their work as they assess the risk that the hospital faces. Often it is this same data the reveals the risk the hospital seeks to identify. In each case the proprietary need of the hospital is so very high that they trump all interests of relational or privilege privacy and enable risk management to have access to all data in the hospital regardless of its source and category and value. The tool enables classification of data in this area to in ways identical (100% agreement) to the way the commercial system functions.

5.3.11 Research Team

Research wing of the hospital seeks to develop understandings and capabilities that will assist the hospital in it meeting the challenges of its unique environment. Research will draw its data from many areas of the hospital but will not have the carte blanche access that the risk management posses.

The following table contains the results and predicted access for Research:

*Where tool and hospital access are identical the final column value will be **bold**.*

Data Item	**Source**	**First Question asked/result**	**Second Question Asked/Result**	**Third Question Asked/Result**
Patient name	Patient	1b/Possession	2f Yes Intellectual	**2h(1) No Access Denied**
Patient Address	Patient	1b/Possession	2f Yes Intellectual	**2h(1) No Access Denied**
Insurance Information	Patient	1b/Possession	2f Intellectual	**2h(1) No Access Denied**
Patient bed assignment	Hospital	1b/Possession	2f Intellectual	**2h(3) Access Permitted**
Next of kin	Patient	1b/Possession	2f Intellectual	**2h(2) Access Denied**
Nurses notes	Hospital	1b/Possession	2f Intellectual	**2h(2) Access Permitted**
Doctors orders	Hospital	1b/Possession	2f Intellectual	**2h(2) Access Permitted**
Lab tests	Hospital	1b/Possession	2f Intellectual	**2h(2) Access Permitted**

Table 26 Research Team

As demonstrated from the table certain items of data are accessible to the researcher while other items are not. This access pattern corresponds nicely (100% agreement) to that of the hospital for most studies. In general personal identifying information is not available in any study.

However the pattern of access can change depending on the nature and purpose of the study conducted where personal identifiable information is not a permissible data item.

5.4. Conclusion

The review of the results of classifying hospital data using the privacy classification tool demonstrates a number of points. The tool classified 116 data items and compared the tool classification with that classification used by the hospital. The tool mirrored the hospital classification 95.6% of the time. In the incorrect classification, the classification for the unit secretary (access to doctor orders and access to lab tests), Unit Nurse (access to lab tests) and lab (access to doctor orders) could be explained as the result of a debatable perspectives on who should have access to this information. Each of these items had ways to which these roles easily could gain access outside the information system and had this been classified as an access (these items were classified as no access and the tool classified them as access) the fit would have been over 99%.

Comparison of Tool Classification with Hospital Classification			
Position	Number of Data Items	Frequency of match with Hospital Classification	Percent of Agreement
Unit Secretary	9	7	77.78%
Unit Nurse	13	12	92.31%
Unit Supervisor	14	14	100.00%
Nurse Manager	18	18	100.00%
Director of Nursing	18	18	100.00%
Chief Nursing Officer	10	10	100.00%
Doctor	10	9	90.00%
Lab	6	5	83.33%
Risk Management	10	10	100.00%
Research	8	8	100.00%
Total	116	111	95.69%

Table 27 Tool and Hospital Classification

The tool also handles two situations that are regularly confronted with data access. The first situation is when the role/privacy type accessing the data is identical to the role/privacy type that initially procured the data. Here the determination of access is very simple – the predicted access was always identical to the access provided by the hospital. The second access pattern occurs when there is a difference between the role/privacy types accessing with the role/privacy type that initially procured the data. In this situation it is imperative to check to see if access is permitted that is in line with that of the initial relation. In each of the cases using the control and access rules it was possible to construct the appropriate limitations of access.

This study demonstrates that privacy while traditionally treated as a single dimensional construct can be classified into four distinct privacy types of privacy: relational, privilege, secret and intellectual. It has been shown that each of the classifications has a unique signature of control and access that has a basis in philosophy and law. It has been shown that this model can be instantiated in a tool that enables data to be classified. It has also been shown that this tool produced a data model that closely resembled that of an acceptable, commercially developed information system that did not use this tool in its development of its access patterns.

The commercial system developed data classifications and access using and instance by instance classification. As there is no consensus on what is privacy objective functional specifications are not available for system development. Instead subjective notions of privacy are used. With use of this tool that has its basis in law and philosophy some objective notion of privacy is available. This objectivity enables the tool to act as a top down development tool enabling development to proceed both from a top down and bottom up development approach rather than the bottom up approach that has been the traditional development method.

Additionally the unique signature of the various types of privacy can be used to produce fine grained controls and access to data that the business organization requires. The fine grained approach enables access to be best specified to meet the needs for access and control over each privacy type data enabling the user to receive relevant, quality data in amounts necessary but not exceeding that required to perform their task.

Chapter 6: Contributions, Limitations and Future Research

6.0 Introduction

This chapter will discuss the contributions of the study, together with its limitations It will conclude with the anticipated future research.

6.1 Contributions

This study proposed and demonstrated a new privacy model. This model is based not upon subjective understandings of privacy but being grounded in law and philosophy produced an objective standard. This privacy model proposed not one but five distinct types of privacy, relational, privilege, intellectual, transitory and secret privacy. Each of these privacy types have a distinguishing signature of control and access. Each of these privacy types have differing philosophical backgrounds which were supported in through laws and social norms. This model also differs from the four prong classification proposed by Prosser. As previously stated, Prosser's taxonomy of privacy posited that a person has a right to be protected from intrusion, a right to control the disclosure of private facts, a right to protect the commercial value of one's name or likeness, and a right to protect against "false light" disclosures. Prosser did not go beyond this classification other than providing support for the classification itself. The taxonomy proposed here, while having a basis in right theory goes beyond Prosser and identifies relationships that embody the rights Prosser speaks of by looking upon the character of the information and the relationship between the information donor and information recipient and providing a classification that defines the degree of control and access that should be afforded to the target information.

This study addressed the call for better understanding of privacy and for new paradigms of privacy. It provided an explicit, objective standard to specify privacy. This standard captured the social and legal requirements for privacy. It has as it base law and philosophy and is expressed in relationships that are defined through a mixture of control and access. The end result produced a multidimensional type based construct which is capable of acting as both a goal and method of development that provides guidelines to all types of privacy as well as specific guidelines unique to each particular type of privacy. Through these developments privacy is not able to be constructed in a bottom up manner but it can now proceed to be constructed from a top down method.

It was demonstrated this model could be constructed into a data classification tool. This tool would initially classify a data item and source into a confidence or possession type. From this classification an intermediary classification ensued which was followed by a final step which determined whether a given role was denied or given access to the data.

Finally it was time to determine if the model would actually classify data in a real life setting. Applying the model to a data classification schema determined by a commercially developed RBAC system the model was able to recreate the access scheme with a 95.69% agreement. When work-a-rounds constructed by the hospital staff was taken into account, the model actually replicated the system plus work-a-round at with an over 99% agreement.

A number of objectives were not met. No evidence was produced that this system produces a better specified construct of privacy. Despite the fact the existing system specifications were replicated in hours this is insufficient evidence to demonstrate that systems could be proposed, selected, implemented more effectively and efficiently and understood more completely using this specification. No proof was demonstrated that would show that less time and effort will be spent on reworking systems to add unanticipated functionality or in designing into systems the requirements to meet mandated functionality for both the present and the future. Finally nothing was shown that would demonstrate this system will provide a better way to exploit technological change and preserve status quo or at least reconcile status quo with technological changes

This study however gives business the promise of a new tool to address problems and opportunities presented by privacy – once further work is done on testing the tool. Before this occurs it is incumbent to take this tool and apply it out of this context across the business community, not just a hospital.

6.2 Limitations

This study has a number of limitations. The test was done only on two medium sized hospitals. In order to see if the model holds future research should include information from additional hospitals of varying sizes. Additionally this was tested only in the hospital setting. Taking this into a non medical setting particularly one which heavily relied upon secret type privacy or which had a significant numbers of test cases in intellectual privacy would produce interesting results.

The model was not thoroughly tested. On question three of the model there were test cases that originated from relational, privilege and secret privacy. However no test cases originated as an intellectual privacy classification. Information which originates as intellectual privacy that is later accessed will need to be procured in order to fully test the model. Additionally no testing was done showing that Public Privacy is a distinct privacy type.

A final limitation comes from how the test was conducted. During the study the notes were coded by the taker of the notes. In the future the verified notes need be coded and summarized by two coders who are blind to the privacy taxonomy.

6.3 Future Research

There are many areas that present ripe vistas for future research. Because this model was applied in a medium sized hospital, we must ask will it hold in hospitals of all sizes. Having accomplished this then effort should be addressed to apply this in other commercial areas where privacy is important. Looking at businesses that deal with finances, intellectual property or rely upon creativity would be interesting areas to apply this model.

The question should be asked: Is this model better than competing models of privacy for explaining and understanding privacy? Does the model promote a better understanding of the functional specifications of a privacy driven project? Does it assist in the construction of a better security design? As a tool is it easier to use than traditional developmental tools? Is the privacy tool an improvement over the ways in which privacy is presently incorporated into systems?

What are model's relative strengths and weaknesses when compared with the competing models when the model is applied to development of systems? Here measuring time and cost of development and comparing development with and without the tool would be an interesting test of the model. Another area of research would address the question of whether this tool can lower the cost to build a system in terms of time and money. Does the tool enable modules to be created that can be used on different systems eliminating cost of development? Does the tool enable benchmarking of like existing systems where systems can be more directly compared, lessons learned and understandings incorporated in new systems?

References

Agre, P. (1998) *Surveillance and capture: The two models of privacy, technology and privacy: A new landscape*. The MIT Press.

Allen, A. (1988) *Uneasy access: Privacy for women in a free society*. Rowman and Littlefield, Totowa, NJ.

American Library Association (ALA). (2002) *Privacy: An interpretation of the library bill of rights.* Article IV. Retrieved February 20, 2006, from http://www.ala.org/ala/oif/statementspols/statementsif/interpretations/privacy.cfm.

American Philosophical Association, Proceedings and Addresses. *v70, No. 2, pp. 119-121.* Retrieved July 30, 2006, from http://www.apaonline.org/apa/governance/statements/research.html.

Annesley v. Anglesea (1743) 17 St Tr. 1139/

Audi, Robert, American Philosophical Association's Committee on the Status and Future of the Profession (Jaegwon Kim, Chair, 1976–1981; Robert Sleigh, Chair, 1981–1986), and Committee on Career Opportunities (Robert Audi, Chair, 1980–1985) at http://www.apa.udel.edu/apa/publications/texts/briefgd.html.

Austin, L. (2003) *Privacy and the question of technology*. Law and Philosophy Kluwer. Academic Publishers, Netherlands. p.22, 119-166.

Afyouni, H. (2006) *Database security and auditing: Protecting data integrity and accessibility.* Thompson Course Technology, Boston, Massachusetts.

Bellotti, V. (1998) *Design for privacy in multimedia computing and communications environments.* Technology and Privacy: The New Landscape, Philip Agre and Marc Rotenberg eds., MIT Press, Cambridge.

Benn, S. (1975) *Privacy, freedom, and respect for persons in Nomos* XIII: Privacy, J.R. Pennock and J.W. Chapman eds. New York, Atherton Press p. 1-26.

Bezanson, R. (1991) *Privacy, Personality and social norms*, Case Western Reserve Law Review, v41 p.681-87.

Blair, M. (Nov. 13, 2000) *New Ways Needed to Assess New Economy*. Brookings Institution, Nonresident Senior Fellow, Economic Studies, The Los Angeles Times.

Bloustein, E. (1962) *Privacy as an aspect of human dignity: An answer to Dean Prosser*. *N.Y.U.L.R.* 39. p. 1003.

Bowers v. Hardwick (1986) Dissenting opinion, section III. 478 U.S. 486.

Brandeis and Warren, (1890) *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

Britt v. Naval Investigative Service, 886 F2d. 544 (3d Cir. 1989).

Buris, G. (1995) Book Review, 16 J Legal Med. 447, 449.

California Health Care Foundation and Consumers Union. (January 1999) *Promoting health: protecting privacy*, p.12.

Carey v. Population Services International. (1977) 431 U.S. 678,685.

Cavoukian, A., Information and Privacy Commissioner of Ontario (June 1997) *Identity theft: Who's using your name?* Retrieved March 28, 2005, from http://www.ipc.on.ca/english/pubpres/sum_pap/papers/ident-e.htm.

Chiu, D. and Hung, P. (2005) *Privacy and access control issues in financial enterprise content management,* Proceedings of the 30th Hawaii International Conference on Systems Science.

Clarke, R. (1994) *The digital persona and its application to data surveillance,* Information Society, v10. No. 2. p. 77-92.

Clark, D.D., and Wilson, D.R. (April 1987) *A comparison of commercial and military security policies,* .IEEE Symposium on Computer Security and Privacy.

Coase, R. (1960) The Problem of Social Cost" in Journal of Law and Economics, v. 3, pp. 1-44. Cohen, J. (Spring 2003) *Symposium: The law and technology of digital rights management: DRM and privacy,* 18 Berkeley Technology Law Journal.

Cohen, J. (Spring 2003) *Symposium: The law and technology of digital rights management: DRM and privacy,* 18 Berkeley Technology Law Journal.

5 Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604).

Committee on National Security Systems (CNSS). (2003) *National information assurance (IA) glossary*. CNSS Instruction No. 4009.

Coyne, E.J. (1996) *Role engineering*, Proceedings of ACM Workshop on Role-Based Access Control.

Cruft, R. (2004) *Rights: Beyond interest and will theory*. Law and Philosophy 23, p.347-397.

Danzig, R. (1978) *The capability problem in contract law: Further readings on well-known cases*. Foundation Press Mineola, NY.

Danzig, R. and Watson, G. (2004) *The capability problem in contract law: Further readings on well-known cases*. 2d ed.

Davison, R.M. R, Clark, H.J. Smith, D Langford, and F-Y Kuo. (2005) *Information privacy in a globally networked society: Implications for information systems research*, Communications of the Association for Information Systems, v12, p.341-365.

DeCew, J. (Summer 2002) *Privacy.* The Stanford Encyclopedia of Philosophy. Edward N. Zalta (ed.). Retrieved July 26, 2006, from http://plato.stanford.edu/archives/sum2002/entries/privacy/.

DeCew, J. (1997) *In pursuit of privacy: Law, ethics and the rise of technology.* Cornell University Press, Ithica N.Y.p.10.

Department of Health Education and Welfare. (1973) *Records, Computers and the Right of Citizens.*

Dratler, J. (1991) *Intellectual property law: Commerical creative, and industrial property*. v1, 4.03[3][b].

Dridi, F., Muschall, B., and Pernul, G. (2004) *Administration of an RBAC system,* Proceeding of the 37th Hawaii International Conference on Systems Sciences IEEE.

Eddy, C. (2000) *A critical analysis of health and human services' proposed health privacy regulations in light of the Health Insurance Privacy and Accountability Act of 1996,* Loyola University Chicago Institute for Health Law Annuals of Health Law 2000 9 Ann. Health L. 1

Edelman, L, and Suchman, M. (1997) *The legal environments of organizations,* Annual Review of Sociology, v23 p.479-515.

Efinger, J., Maldonado, J., & McArdle, G. (2004) *PhD students' perceptions of the relationship between philosophy and research: A qualitative investigation.* The Qualitative Report, 9(4), 732-759. Retrieved July 26, 2006, from http://www.nova.edu/ssss/QR/QR9-4/efinger.pdf.

Electronic Privacy Information Center. (2003). *The privacy act of 1974.* Retrieved November 19, 2005, from http://www.epic.org/privacy/1974act.

Elias, S. (1998) *Trade secret law: An overview,* Nolo Press.

Emerson, T. (1979) *The right of privacy and freedom of the press.* Harvard Civil Rights-Civil Liberties Law Review, v14 p.339.

Epstein, L. and King, G. (2002) *The rules of inference*. 69 U. Chi. L. Rev. 1, 9.

Epstein, P. and Sandhu, R. (1999) Toward a UML based approach to role engineering. Proceeding of ACM Workshop on Role-Based Access Control.

Erlanger, H., Garth, B., Larson, J., Mertz, E., Nourse, V. and Wilkins, D. (2005) *New legal realism symposium: is it time for a new legal realism?: Foreword: Is it time for a new legal realism.* 2005 Wis. L. Rev. 335.

Federal Communications Commission (FCC), Consumer and Governmental Affairs Bureau. (2006) *Children's Internet protection act*. Retrieved March 23, 2006, from http://www.fcc.gov/cgb/consumerfacts/cipa.html.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. and Chandramouli, R. (August 2001) *Proposed NIST standard for role based access control,* ACM Transactions for Information and System Security, v4, no.3. p. 224-274 @ pg. 233.

Federal Register. (December 28, 2000) Volume 65, Number 250 p. 82759-82468.

Field. (September 1994) *Computerized medical records create new legal and business confidentiality problems*. 11 Healthspan 3, 4. Retrieved January 30, 2008, from http://www.aarc.org/resources/position_statements/ethics_detailed.html

First American Labor Case, (1931) 41 Yale L.J. 165, (describing the historical context of the 1806 case, Commonwealth v. Pullis (The Philadelphia Cordwainers' Case)

Forester Research. (2005) National Consumer Health Privacy Survey2005. Retrieved November 1, 2005 from http://www.chcf.org/topics/view.cfm?itemid=115694.

Fried, C. (1968) *Privacy*. 77 Yale Law Journal p. 475-483.

Froomkin, A. M. (2000) *The death of privacy?* 52 Stanford Law Review, 1461 p. 1463.

Froomkin, A. M. (1996) *Regulation and computing and information technology: flood control on the information ocean: living with anonymity, digital cash and distributed databases* 15 L.J. and Comm. 395, 493

Fuller, R. (1992) *Cosmography: A Posthumous Scenario For The Future Of Humanity*: With Kiyoshi Kuromiya, adjuvant. Macmillan Publishing Company, New York.

Garrett, R. (1974) *The Nature of Privacy*, Philosophy Today 18. p. 264.

Gavison, R. (1980) *Privacy and the limits of the law*, Yale Law Journal p. 89, 421-471.

Gavrila, S.I., and Barkley J.F. (1998) *Formal specification for role based access control user/role and role/role relationship management,* Proceeding of Third ACM Workshop on Role Based Access Control, Fairfax, VA, p. 81-90.

Geertz, C. (1983) *Local knowledge.* Basic Book, New York.

Gerety, T. (1977) *Redefining Privacy*. Harvard Civil Rights-Civil Liberties Law Review 12(2) p. 234

Glaser, B. and Strauss, A. (1967) T*he discovery of grounded theory: Strategies for qualitative research.* Aldine, New York. p. 15

Goffman, E. (1957) *The presentation of self in everyday life,* Anchor (1957).

Graham, J. (1987) *Privacy, Computers, and the commercial dissemination of personal information*. 65 Texas Law Review 1395.

Greenaway, K. and Chan, Y. (June 2005) *Theoretical explanations for firms information privacy behaviors,* Journal of the Association for Information Systems, v6, no.6, p. 171-198.

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

Gross, H. (1971) *Privacy and Autonomy in Nomos*XIII: Privacy. J Roland Pennock and John W. Chapman, Eds. p. 169, 170

Hadley v. Baxendale (1975) *A study in the industrialization of the law,* 4 J. Legal Stud. 249, 249-84.

Harris Equifax. (1993) *Health information privacy study.* Retrieved November 1, 2005, from http://www.epic.org/privacy/medical/polls.html.

Hevner, A., March, S. and Park, J. (March 2004) *Design science in information systems research,* MIS Quarterly, v28, No. 1, p. 75- 105.

He, Q. and Anton, A. (2003) *A framework for modeling privacy requirements in role engineering.* Proceedings of the 9th International Workshop REFSQ, Austria.

Hines, N.W. (2005) *Empirical scholarship: What should we study and how should we study it?* Aals Newsl. (Ass'n of Am. Law Sch.) Washington, D.C. p. 1, 1-7.

Hoekendorf, (Nov 20, 1996) *How electronic data interchange improves communications between payers and providers*. Information Management Week.

Hohfeld, W. (1964) *Fundamental legal conceptions as applied in judicial reasoning*, New Haven, Connecticut, Yale University Press.

Holloway, J. (Spring 2005) *A Primer on the Theory, Practice and Pedagogy Underpinning a School of Thought on Law and Business,* 38 University of Michigan Journal of Legal Reform 587.

Inglehart, R. (1977) *The silent revolution: Changing values and political sty.les among western publics*. Princeton University Press, Princeton, N.J.

Inness, J. (1992) *Privacy, intimacy and isolation*. Oxford University Press, New York.

Italia,M. (2003) *The history of legal professional privilege and its role in tax advice by tax professionals,* Accounting History International Conference Siena.

Izaki, K., Tanaka, K., and Takizawa, M. (2001) *Information flow control in role-based model for distributed objects* Proceedings of the 8th International Conference in Parallel and Distributed Systems. p. 363-370.

James, S. (2003) *Rights as enforceable claims*, Proceedings of the Aristotelian society 103/2. p. 133-147.

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

Kayworth, T., Brocato, L., and Whitten, D. (2005) *What is a chief privacy officer? An analysis based on Mmintzberg's taxonomy of managerial roles*. Communications of the Association for Information Systems. v16 110-126.

Kennedy, E. (Mar. 10, 1999) *Statement on the introduction of the medical information privacy and security act*.

Kramer, M. (1998) *Rights without trimmings,* in Mathew H. Kramer, N.E. Simmonds and Hillel Steiner, *A debate over rights: Philosophical enquiries,* Oxford, Clarendon Press. p. 8.

Krasner, S. (1988) *Sovereignty: An institutional perspective.* Comparative Political Studies. v21, p. 66-94.

Krattenmaker, T. (1973) *Testimonial privileges in federal courts: An alternative to the proposed federal rules of evidence* 62:61. The Georgetown Law Journal 61 p. 89.

Lessig, L. (1999) *Code and other laws of cyberspace.* Basic Books, New York.

Lemley, M (1999) *Law and Economics of Internet Norms* http://repositories.cdlib.org/blewp/art132/.

Locke, J. (1988) *The second treatise on government* 4. Thomas P. Peardon, ed.

Long, E. (1967) *The intruders*, New York: Frederick A. Praeger, Inc. p. viii. 55.

Lowrance, W. (May 1997) *Privacy and health research: A report to the secretary of health and human services.* Department of Health and Human Services, 6.

Mason, R. O. (March 1986) *Four ethical issues of the information age*. MIS Quarterly (10:1) p. 4-12.

Masten S. (no year) *A Legal basis for the firm* in *the nature of the firm: Origins, evolution and development.* OE Williamson, ed. Oxford University Press: New York, p. 199-212.

Maute, J. (2000) *Response: The values of legal archaeology*. Utah L. Rev. 223, 224. p. 234-235.

McAdams, R. and Ulen, T. (2002) *Introduction: Symposium: Empirical and experimental methods in law,* University of Illinois Law Review, p. 791.

Meyer, J., Boli, J. and Thomas, J. (1987) *Ontology and rationalization in the Western cultural account.* Institutional Structure, Constituting State, Society. Sage: Newbury Park, CA. p. 12-37.

Meyrowitz, J. (1985) *No sense of place: The impact of electronic media on social behavior,* Oxford University Press, New York.

Milgrim, R. (2002) *Milgrim on Trade Secrets* § 1.07.

Miller, M., Yee, K., and Shapiro, J. (no year) *Capability myths demolished.* Retrieved Oct. 16, 2006, from http://zesty.ca/capmyths/.

Milne, G.R. and Culnan, M. (2002) *A longitudinal analysis of the privacy web sweep data: using marketing research to inform public policy.* The Information Society (18), p. 345- 359.

Ministry of Economic Affairs - Taiwan, ROC, Intellectual Property Office. (2005) *Trade secrets Act*.

Nagel, T. (1998) *Concealment and exposure*. Phil. & Pubic Affairs. 27. p. 3–20.

National Association for the Advancement of Colored People V. Alabama ex Rel. Patterson, Attorney General 357 U.S. 449 (1958)

National Institute of Standards and Technology (NIST). (2003) *Cyber security activities,* National Institute of Standards and Technology.

Neuman, G. and Strembeck, M. (2002) *A scenario-driven role engineering process for functional RBAC roles,* Proceedings of the 7th ACM Symposium SACMAT, Monterey.

Newhard, J. (30 Dec 2004) *Life, liberty, property and privacy,* The Sentinel.

Nissenbaum, H. (1998) *Protecting privacy in an information age: The problem of privacy in public, law and philosophy* 17 p. 559-596.

Nozick, R. (1974) *Anarchy, State and Utopia*, New York, Basic Books 1974 p. 29

Nyanchama M. and Osborn, S. (1999) *The role graph model and conflict of interest*, ACM Transaction on Information and System Security TISSEC Vol 2 Issue 1, p. 105-135.

Nyanchama, M. and Osborn, S. (1994) *Access rights in role-based security system.* Database Security VIII: Status and Prospects p. 37-56.

O'Neill, O. (1985) *Between Consenting Adults.* Philosophy and Public Affairs 14 p. 252-277.

Olmstead v. United States, 277 U.S. 438, 478 (1928).

Organization for the Prevention of Chemical Weapons (OPCW). (no year) *Privileges and immunities agreements*. Retrieved April 26, 2005, from http://www.opcw.org/html/db/legal/la_pi_intro.html.

Osborn, S., Sandhu, R., Munnwer, Q. (2000) *Configuring role-based access control to enforce mandatory and discretionary access control policies,* ACM Transactions on Information and System Security, v3 No. 2 p. 85-106.

Parent, W.A., (Autumn 1983) *Privacy, morality and the law,* Philosophy and Public Affairs. v12., No. 4, p. 269- 289.

Parker, D. (2002) *Toward a new framework, for information society*, The Complete Security Handbook, 4th Edition, Symour Bosworth and M.E. Kabay, New York.

Plone, The (2000) *Federal_Data_Reference_Model.htm: Glossary of terms for federal data reference model (DRM)*. Retrieved need date, from http://proptax.mdor.state.mn.us/mdr/glossaries/Federal_Data_Reference_Model.htm.

Ponsizewsha-Maranda, A. (2005) *Role engineering of information systems using extended RBAC model,* Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE '05), 0-76952362-5/05.

Pooley, J. (1975) *Trade secrets* § 2.03[1] (1997) note 49, § 4.04[2]a see also Tri-Tron Int'l v. Velto, 525 F.2d 432, 435 (9th Cir. 1975).

Posner, R. (1998) *Economic analysis of the law*, Fifth Edition, Aspen Law and Business, New York. p. 281.

Prince Albert v. Strange, 2 DeGex and Sm. 652 (1849).

Privacy Protection Commission (1977) *Personal privacy in an information society.*

Public Law 104-66, the *Federal reports elimination and Sunset Act of 1995.*

Qui, Jiong, Ma Chen-hua, Yin, Jian-wei, Dong Jin-xiang. (2005) *Research and implementation of role-based RBAC administration model,* Proceedings of the 2005 The Fifth International Conference on Computer and Information Technology, IEEE Computer Society.

Rachels, J. (2006) *The elements of moral philosophy* McGraw-Hill Humanities/Social Sciences/Languages; 5th ed. p.326.

Rachels, J. (Summer 1975) *Why privacy is important,* Philosophy and Public Affairs, 4, p. 323-333.

Radin, M.J. (1990) *The pragmatist and the feminist.* 63 S. Cal. L. Rev. 1699, 1707.

Rainbolt, G. (1993) *Rights as normative constraints on others,* Philosophy and Phenomenological Research 53/1 pp 133-147.

Rao, Radhika, (2003) *A veil of genetic ignorance? Protecting privacy as a mechanism to ensure equality.* Hastings Center Report Vol 33. No. 3, Hastings Center.

Reiman, J. (1976) *Privacy, intimacy and personhood, philosophy and public affairs* 6(1) p. 26-44.

Reiman, J. (1995) *Driving to the Panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future.* Santa Clara Computer & High Tech. L. J. 11. p.42.

Revesz, R. (2002) *A defense of empirical legal scholarship,* 69 University of Chicago Law Review. p. 169.

Roberts v. United States Jaycees, 468 U.S. 609 (1984).

Roeckle, H., Schimpf, G. and Weidinger, R. (2000) *Process-oriented approach to role finding to implement role-based security administration in a large industrial organization*: Proceeding of ACM Workshop on Role-Based Access Control.

Rosen, J. (2000) *The unwanted gaze: the destruction of privacy in America.* Random House. p.60-61

Rotenberg, M. (1994) *Privacy and Security for Medical Information Systems, Seizing the Opportunity: The Power of Health Information*. AHIMA National Convention (1994), Las Vegas, Nevada.

Rubenfeld, J. (1989) *The right of privacy*. 102 Harv. L. Rev. 737, 752-54.

Saltzburg, S. (1980) *Privileges and professionals: Lawyers and psychiatrists,* Virginia Law Review. v.66, p.597 @ 600.

Samarajiva , R. (1998) *Interactivity as though privacy mattered,* in Technology and Privacy: The New Landscape, Phillip E. Agre and Marc Rotenberg, eds. MIT Press Cambridge MA.

Samuelson, P. (2000) *Privacy as intellectual property?* 52 STAN. L. REV. 1125 note 148.

Sandeen, S. (Fall 2006) *Relative Privacy: What privacy advocates can learn from trade secret law,* Law Review of Michigan State University, Detroit College of Law, Michigan State Law Review, Michigan State Law Review.

Sandhu, R.S. and Bhamidipati, V. (1996) *The ARBAC97 Model for Role Based Administration of Roles,* ACM Transactions on Information and System Security Vol 2 Issue 1, pg. 105-135.

Scanlon, T. (1975) *Thompson on privacy,* Philosophy and Public Affairs, Vol. 4 No. 4, Summer, p. 315-322.

Schauer F. (2000) *The social construction of privacy*, discussion draft 10 (unpublished manuscript, at http://www.ksg.harvard.edu/presspol/publications/pdfs/schauer1.PDF) p.8.

Schneier, B. (4 Oct 2004) *Bigger Brother.* The Baltimore Sun

Schoeman, F. (1984) *Privacy: Philosophical dimensions in the literature.* Philosophical Dimensions of Privacy. Ferdinand Schoeman ed., Cambridge University Press, Cambridge. p.4.

Slife, B. D., and Williams, R. N. (1995). *What's behind the research? Discovering hidden assumptions in the behavioral sciences*. Thousand Oaks, CA: Sage.

Slobogin, C. (Fall 2002) *Public privacy: camera surveillance of public places and the right to anonymity*, 72 Miss. L.J. 213.

Smith, H., Milberg, S., Burke, S. (June 1996) *Information privacy: Measuring individual's concerns about organizational practices,* MIS Quarterly.

Solove, D. (2002) *Conceptualizing privacy.* 90 CAL. L. REV. 1087, 1152.

Spencer, S. (Summer 2002) *Reasonable expectations and the erosion of privacy.* 39 San Diego Law Review p. 843.

Stedman, J. (1962) *Trade secrets*. 23 OHIO ST. L.J. 4, 6. p.7.

Stone, J. and Merrion, S. (April 2004) *Instant Messaging or instant headache,* ACM Queue Vol.2, No. 2.

Thomson, J. (Summer 1975) *The right to privacy*. Philosophy and Public Affairs. no.4 p.313.

Threedy, D. (2006) *AALS section on contracts symposium empirical scholarship: what should we study and how should we study it?* Legal Archaeology: Excavating Cases, Reconstructing Context 80 Tulane Law Review p.1197.

Tittinene, P. (2003) *User Roles in Document Analysis*, CAISE '03 Forum Short Paper Proceedings University of Maribor Pres., p. 205-208.

Tracey, G. (Winter 2006) Symposium: *The next generation of law school rankings: Ranking methodologies: An empirical study of empirical legal scholarship: The top law schools*, 81 Ind. L.J. 14.

Tsai, V. (1993) *Cheaper and better:The congressional administrative simplification mandate facilitates the transition to electronic medical records*. Taylor & Francis. The Journal of Legal Medicine 19:4 @ 10.

Turkington, R. (1997) *Medical record confidentiality, law, scientific research and data collection in the information age*, 25 J.L. Med. & Ethics 113, 115.

Ulen, T. (2004) *Symposium: Law and economics and legal scholarship: The unexpected guest: Law and economics and other cognate disciplines and the future of legal scholarship*, 79 Chicago Kent Law Review p.403.

Video Privacy Act 18 USC 2710

Warren, L. and Brandeis, S. (1890) *The Right to Privacy*, 4 Harv. L. Rev. 193.

Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum. p. 7.

Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

Williamson. O. (no year) *Comparative economic organizations: The analysis of discrete structures alternatives.* Administration Science Quarterly. v36, p.269-296.

Yin, R. (2003) *Case study research: design and methods* Sage 3d ed.

Zweig, D. and Webster, J. (2002) *Where is the line between benign and invasive?:An examination of psychological barriers to the acceptance of awareness monitoring systems*. Journal of Organizational Behavior. p.605-633.

Appendices

Appendix A

Questions For first round administrative interviews

Name

Position

Responsibility and Tasks performed

Tell me about the hospital

- Size
- Functions performed and who performs
- Organizational chart
- Resources
- Data Management
- How does data get into the system and eventually to the hands of the person or function that requires it?
- What are the standards used for this? Where did they come from? What are the competing standards? Why did you chose the one you did?
  What should I know about hospital information systems in general/specifically?

- What is unique to the hospital setting when compared to industry in general and other medical providers?
- How are your regulated?
- Who regulates you?
- What must you do to fulfill your regulation requirements?
- What are the potential penalties?
- What data must you provide to whom as part of your regulation requirement?
  Who are your stakeholders?

- Strengths and weaknesses of each stakeholder?
- The needs and requirements of each stakeholder?
- How do you provide for them?
- Who must you provide information to?
- Who must you cordon information from?
  What are your challenges with information management?

What departments depend upon what information?

How do you enforce separation of authority?

How do you manage security?

- Setting goal
- Implementing
- SOA issues
- Stakeholder issues
  How do you manage your information and information flow?

- How does this impact security?
-

Who are the people/department that perform what function for you?

What other things should I know about this area?

If unaware of any questions answer ask: Who knows, how can I reach them?

For Second Round Interviews (For Interviews with each job function)

Name

Position

Responsibility and tasks performed

Length of time at job

Other jobs held in past

For each responsibility and task (past and present)

- What information do you require to do your job function?
- How do you access this information?
- What is the source of that information?
- How you access that source?
- Nature and character of that information
- Responsibility you must exercise once you obtain the information
  If unaware of any questions answer ask Who knows, how can I reach them?

For Interviews with IT Personnel

Name

Position

Responsibility and task performed

Length of time at job

How does your job impact the data management/data access schema?

Do you have access to the data access/data classification portion of system?

- If yes what access
- What can you perform

What are the policies of access?

Who sets the policy?

Who has access to what type of data in what amount?

If unaware of any questions answer ask Who knows, how can I reach them?

Appendix B

Types of Privacy

Name	Characteristics	Limitations on Acquistion, Use and Disclosure	Control	Access to Entity and Information about the Entity	
Relationship	Personal Information that forms impressions and relationships Representative relationships include friend to friend Husband and wife employer employee	The disclosee should only obtain information reasonable and necessary for the relationship to form and be maintained Regardless of whether the relationship is professional or intimate information personal to the discloser is provided to the disclosee	Respect A high level of control is provided over this type of information by the owner of this type of information In general this information is voluntarily released Once obtained the information must be controlled for the benefit of the information p	Necessity Access only on a compelling necessity Low access to individual/individual and individual/organization relationships Low access to information contained in those relationships	Confidentiality
Secret	Information of the organization Representative relationships include Employer-Employee Employer-Independent Contractor Consultant-Consultee Secret information is any information maintained by an individual or an	The organization or individual discloses this information to employees contractors or other organizations in order to do business more efficiently or effectively Once given access the disclosee can only use this information to futher the interests of t	Selective Lockdown Control the use and dissemination of the information of the individual/organization in order to protect and advance the Individual/Organization's goal's and Interest	Selective Access To the appropriate individual/organization provide high access to the information of the individual/organization To the appropriate individual/organization provide and/or hi	
Privilege	Highly Important information of another person or organization that in the hands of an appropriately trained professional can greatly assist that person or organization in its goals or problems Sharing this information with appropriately trained individua	To acheive this value an incentive is provided to the disclosed to use this information only for the benefit of the discloser and to safeguard further disclosure all information obtained	Safeguard Collect all information reasonable and necessary to accomplish the task at hand Control the use and dissemination of the information collected or generated inorder to protect the interest of the information donor	Minimum Necessary Acess only to those appropriate trained and then only in amounts reasonably necessary to do their task Low access to individual/organization Low access to information	Confidentiality
Intellectual	Information being digested by individuals or the organization This information is input into the organization or the individual Representative relationships Library - Patron Information provider - information consumer Representative information includ	Only those obtaining and using this information are entitled to know the source content of this information and any tests using this information	Unavowed Control everything including what data is collected how it is used and who is using the data In controling what data is collected it is not only what data and/or information has been collected but that data and/or information is being colle	Safeguard Unless others are threatened or harmed in socially unacceptable ways there is no access to this data Low access to individual/organization Low access to information	Confidentiality
Transitory	Information available in public or public places that can compromise a reasonable person's privacy expectations	Traditional values of data collection and use of data found in public spaces need to be respected	On all information collected in a public place be certain it does not violate relationship secret privilge or intellectual privacy or affect these types of privacy adversely in absence of a compelling reason	High access to individual/organization High access to information	

About the Author

Gary Poe graduated from the Stetson College of Law in St. Petersburg, Florida, in 1980. He has been a successful trial lawyer for 18 years previous to pursuing his doctoral degree in Management Information Systems at the University of South Florida. The author has resided in Florida since 1975 and currently makes his home in Inverness where he has resided on Lake Henderson for the last 15 years with his wife Laura, and his children Sarah, Gary Jr. and Gillian.