The Role of the Epistemic Community in Influencing Privacy Legislation: The United State and The European Union

George Edward Richie
University of Denver

Follow this and additional works at: https://digitalcommons.du.edu/etd

Part of the Other International and Area Studies Commons

Recommended Citation
https://digitalcommons.du.edu/etd/550

This Dissertation is brought to you for free and open access by the Graduate Studies at Digital Commons @ DU. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons @ DU. For more information, please contact jennifer.cox@du.edu,dig-commons@du.edu.
THE ROLE OF THE EPISTEMIC COMMUNITY IN
INFLUENCING PRIVACY LEGISLATION:
THE UNITED STATES AND THE EUROPEAN UNION

A Dissertation
Presented to
The Faculty of the Josef Korbel School of International Studies
University of Denver

In Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy

by
George E. Richie
November 2010
Advisor: Dr. Joseph Szyliowicz
ABSTRACT

Threats to individual privacy from computer information, database, and surveillance technologies of the mid-20th century prompted the formation of a privacy epistemic community that informed and influenced privacy policy and legislation in the United States and the European Union. Because the United States was more advanced in computer technology than the European nations, awareness of privacy issues, and the privacy epistemic community, emerged first in the United States—and migrated to Europe a generation later. The United States legislated the Privacy Act of 1974, which became the benchmark for individual privacy protection in the United States. While several European nations passed privacy legislation in the 1970s, there was no common privacy policy and law among European nations. In the early 1970s, the Council of Europe (CoE) and the Organization for Economic Cooperation and Development (OECD) created privacy data-protection committees that became important networking organizations for privacy epistemic community experts from the United States, European nations, and other OECD member nations. The influence of the trans-Atlantic privacy data-protection epistemic community can be seen in the similarities among the Fair Information Principles/Practices (FIP) found in privacy studies, guidelines, conventions, and laws in the U.S., the CoE, the OECD, and the European nations.
Two case studies describe the role and influence of the privacy data-protection epistemic community members in influencing privacy studies, policy, and legislation in the United States and Europe. The United States enacted narrow “sectoral” legislation to protect individual privacy from government computers and databases in the Privacy Act of 1974. More than two decades later, the European Union enacted broad “omnibus” data-protection legislation that effectively limits the collection and aggregation of personal data on EU citizens. Why two such dramatically different privacy data-protection laws could have been enacted when influenced by the same privacy data-protection epistemic community leads to analysis of economic, socio-cultural, and political influences on privacy data-protection legislation. Evidence suggests that privacy data-protection epistemic community influence, filtered through different socio-cultural visions of the relationship of the government and the citizen, lead to dramatically different privacy data-protection legislative results.
ACKNOWLEDGEMENTS

To my wife, Linda, and my children, George, Geoffrey, Jessica, and Amanda, who supported and encouraged me in the writing of this dissertation.
# Table of Contents

## List of Tables
- List of Tables ........................................................................................................... viii

## List of Figures
- List of Figures ............................................................................................................ ix

## Chapter One  
**Introduction and Overview** ................................................................. 1
  - Introduction ........................................................................................................... 1
  - Purpose of Study ................................................................................................. 3
  - Limitations, Research Questions, and Approach ........................................... 4
  - Three Research Questions ................................................................................. 5
  - Key Concepts and Definitions ........................................................................... 6
    - Epistemic Community as Independent Variable
    - Intervening Variables
    - Privacy as Dependent Variable
  - Study Overview .................................................................................................. 11
  - Chapter Summary .............................................................................................. 17

## Chapter Two  
**The Concept of Privacy** ............................................................... 22
- Antecedents of American Privacy Concepts .................................................... 24
- Colonial Era Privacy .............................................................................................. 28
- Privacy at the Founding of the Nation .............................................................. 34
- Concept of Privacy in the 19th Century ........................................................... 36
- Growth of Concern Over Newspapers and Privacy ........................................ 41
- The Concept of Privacy From 1890 to 1965 ..................................................... 44
- Privacy After 1965 ................................................................................................. 51
- Chapter Summary .............................................................................................. 55

## Chapter Three  
**The Epistemic Community** ............................................................... 66
- Origins of the Epistemic Community Concept ............................................... 69
- The Nature of the Epistemic Community .......................................................... 73
- Limitations of the Epistemic Community Approach ........................................ 74
- The Influence of the Epistemic Community ..................................................... 78
- The Life-Cycle of Epistemic Communities ...................................................... 82
- Institutionalizing the Epistemic Community ..................................................... 84
- Self-Aware Epistemic Community ..................................................................... 85
- The Global Privacy Epistemic Community ....................................................... 87
- Operationalizing the Identification of the Epistemic Community .................. 88
- Identifying the Privacy Epistemic Community ................................................. 89
- Chapter Summary .............................................................................................. 92
Chapter Four  The Privacy Epistemic Community and the United States
Privacy Act of 1974: A Case Study . ......................... 101
Introduction ......................................................... 101
Genesis of the Privacy Epistemic Community .......... 102
The Path From Security to Privacy
The Nascent Privacy Epistemic Community
Dr. Willis H. Ware and the Rand Corporation .............. 105
Privacy Awareness in the United States ..................... 106
The National Data Bank and Congressional Privacy Hearings
Congressional Hearings and the Privacy Epistemic Community ..... 108
Databanks in a Free Society Project ......................... 113
HEW Secretary’s Advisory Committee on Automated Personal
Data Systems ....................................................... 114
The Privacy Act of 1974 ......................................... 117
Opposition to Privacy Legislation ............................... 118
Privacy Act Expectations ....................................... 121
Chapter Summary ................................................. 125

Chapter Five  The Privacy Epistemic Community and the Legislation of Data
Protection in the European Union: A Case Study  ....... 133
Introduction ......................................................... 133
Response to the Privacy Threat ................................. 135
Germany
Sweden
United Kingdom
The Council of Europe
The Organization for Economic Cooperation and Development
The European Union Data Protection Directive of 1995 ...... 156
Chapter Summary ................................................. 164

Chapter Six  Analysis and Conclusion ......................... 175
Introduction ......................................................... 175
Evidence Addressing the First Research Question .......... 176
Recognized Professional/Technical Expertise in Privacy Issues
Privacy Publications
National and International Organizations with a Privacy
Component
Privacy Websites on the Internet
Privacy Conferences
Participation in Government Hearings, Studies, Testimony
Evidence Addressing the Second Research Question ...... 181
Fair Information Practices ........................................ 183
Evidence Addressing the Third Research Question ............... 185
  A Framework for Analysis
Intervening Variables in the Public Policy Process ............... 186
Evidence of Economic Intervening Variables ....................... 188
  Economic Impact of the U.S. Privacy Act of 1974
  Economic Aspects of EU Data Protection Directive
Evidence of Socio-Cultural Intervening Variables .................. 190
Evidence of Political Intervening Variables ....................... 194
  Evidence of Political Factors in the United States
  Evidence of Political Factors in the European Union
Influence of the Three Intervening Variables ....................... 197
Implications for Further Research ................................. 199
Conclusion ............................................................. 200

Bibliography ........................................................................ 210

Appendices ........................................................................... 254
  Appendix A ................................................................. 254
  Appendix B ................................................................. 277
  Appendix C ................................................................. 280
  Appendix D ................................................................. 283
List of Tables

Table 6.1: Fair Information Practices/Principles (FIP) Sources . . . . . . . . . . . . . . . . . . 184
List of Figures

Figure 1.1: The Theoretical Model ................................. 7
Figure 6.1: A Framework for Analysis ............................... 186
Chapter One

Introduction and Overview

“In reality, a society devoid of individual privacy makes the very basis of democracy---individualism---difficult to attain. An individual who is constantly under surveillance, or one who knows that at any time he may be observed, will limit his external conduct to prescribed standards of safe conformity. Internally, if there is no outlet for one’s own individualistic tendencies, the mind comes to fit into a conformist mold much the same as one’s external actions. An absence of privacy is crucial for totalitarian government to subsist.”

R. H. Clark, *Historical Antecedents of the Constitutional Right of Privacy*

Introduction

Public awareness and concern for “privacy” of the individual have dramatically increased across the developed world over the past century. With each generation, new privacy issues and topics have emerged in response to ever-new dimensions of the creation, accumulation, and distribution of information. Although concerns for privacy can be found in some of civilization’s oldest documents and stories, privacy in law was distinctly a development of late 19th century American society. While several amendments to the Constitution of the United States did enshrine basic common law concepts of individual privacy, it was not until the last half of the 19th century that individual privacy became a public concern and gained permanent stature in law.

Scholars note a direct correlation between the development of new technologies and the growing threat to the privacy of the individual over the past one and one-half
centuries. Initial realization in the United States of the threat of technology to individual privacy came with the newspaper, the telegraph, the box camera, and the telephone. These were the technologies that facilitated the privacy interlopers of which Samuel Warren and Louis Brandeis famously complained in *The Right to Privacy* in 1890. Their *Harvard Law Review* essay created a new area of law, and almost immediately privacy found a new traction in law journals, the courts, and journalism. For the next half-century, privacy law slowly expanded in scope based largely upon the insights of Warren and Brandeis. However, after the early information revolution of the mid-20th century, threats to individual privacy accelerated at an alarming rate.

Creation of automated data processing (ADP) centers by the federal government and large business in the 1950-60s presaged a growing danger to individual privacy by collecting, storing, and integrating small bits of data and information concerning the life and activities of all citizens. Images of universal surveillance and government databases described by Aldus Huxley in *Brave New World*, and George Orwell in *Nineteen Eighty-Four*, were frequently invoked to illustrate the threat to citizens from these new technologies. Government and private organizations, as well as private individuals, recognized the dangers of collection, storage, and manipulation of personal information by ADP centers and initiated studies of the privacy of individuals in the face of ever more capable computer-based information technology.

Initial studies by organizations such as the RAND Corporation, the Association for Computing Machinery (ACM), and the American Federation of Information Processing Societies (AFIPS) produced much of the early technical security-privacy
literature based on their proximity to government and industry main-frame computing
database work prior to the 1970s. What began as concern regarding the security of data
within government and industry quickly evolved into concern for the privacy of the
individual. This technical computer data-processing environment also produced the first
influential members of the privacy epistemic community. Subsequent conceptual
studies based on a proposal from the Social Sciences Research Council in the mid-1960s
regarding the feasibility of a National Data Center created a groundswell of
Congressional, academic, and legal interest in the prospects and problems associated with
the creation of centralized, integrated, government data banks. Initial interest in privacy-
data protection issues and threats based on the proposed government databanks of the
1960s has continuously grown, based on the rapid evolution of digital technologies in the
past half-century and the subsequent multiplication of threats to privacy. As the
technological threats to privacy have grown, the privacy epistemic community has
blossomed as academics, lawyers, business-persons and legislators have been motivated
to investigate and respond to the new privacy problems—and a cascade of privacy-related
literature, organizations, and law have subsequently been created.

**Purpose of Study**

My purpose in this study is to focus on the role of the privacy data-protection
epistemic community in influencing privacy policy and legislation from the mid-1950s to
the mid-1990s. This forty-year period was the era of identification of the privacy-data
protection problem posed by computer, database, and surveillance systems, the
characterization of key issues in individual privacy, and the creation of major privacy
policy and legislation which laid the groundwork for all subsequent privacy discussions. I will define what is meant by the key terms such as privacy and epistemic community and will then employ two case studies to as a means of demonstrating the role of the privacy epistemic community in influencing privacy policy and legislation. Finally, I will evaluate the four intervening variables: 1) privacy epistemic community; 2) economic issues; 3) socio-cultural issues; and 4) political issues, to ascertain influences that resulted in significantly different privacy data-protection policy and legislative outcomes in the United States and the European Union.

Limitations, Research Questions, and Approach

My research efforts focus on the key individuals and organizations that initiated and perpetuated the privacy movement and formed the privacy data-protection epistemic community that has informed, influenced, and motivated the creation of privacy policy and legislation in the United States and the European Union. I have chosen to limit my investigation to the epistemic community approach to policy making because I believe it represents the most compelling construct of the several popular current policy network approaches, that include the advocacy coalition framework,\textsuperscript{14} the multiple stream framework,\textsuperscript{15} and the transnational advocacy network.\textsuperscript{16} As described in Chapter Three, the epistemic community approach has been employed to study decision-making and policy formulation in disciplines ranging from the environment to public administration, business, criminology, and banking. This study is the first to employ the epistemic community approach using comparative case studies of privacy policy formulation and legislation in the United States and the European Union.
Three Research Questions

1) *Does a single privacy data-protection epistemic community exist?*

This is important because the privacy data-protection community must exist before I can show that it had influence on privacy policy and legislation. Six objective criteria are identified in Chapter Three by which I will identify the existence of the privacy data-protection epistemic community.

2) *Did the privacy epistemic community influence privacy data protection in the United States and the European Union?*

Evidence from the case studies in Chapter Four and Chapter Five provide both direct and indirect evidence of the influence of the privacy data-protection epistemic community. This is important because over the past two decades epistemic communities have been identified as playing important roles in educating, organizing, and motivating action on a variety of other local, regional, and global problems. This study will extend epistemic community influence to privacy policy and legislation, laying the groundwork needed to answer the third research question.

3) *Why did the influence of the same privacy data-protection epistemic community result in dramatically different legislation in the United States (The Privacy Act of 1974) and the European Union (directive 95/46/EC on the Protection of Personal Data)?*

If the influence of the same privacy-data-protection community produced different results, then there are other forces at work influencing the policy and legislative decision. Economic, socio-cultural, and political intervening variables are analyzed in to
determine their possible influence on privacy data-protection policy and legislative decision in the United States and the European Union.

**Key Concepts and Definitions**

The following are key concepts that are central to this study need to be defined at the outset before one can discuss the impact of the privacy data-protection epistemic community on privacy policies and legislation in the United State and the European Union.

*Privacy:* The rather broad, social construct, usually seen as a fundamental human right, that is often characterized as: 1) the right “to be let alone;” 2) freedom from unreasonable search, seizure, or intrusion; and, 3) as protection and control of personal information. An expanded definition and discussion of the evolution of the concept of privacy are found in Chapter Two.

*Epistemic community:* “... a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area,” and having 1) a shared set of normative and principled beliefs; 2) shared causal beliefs; 3) shared notions of validity; and, 4) a common policy enterprise. Chapter Three provides a discussion of the evolution of the history of the concept of the epistemic community, limitations of the concept, and objective criteria by which the existence of an epistemic community can be ascertained.

*Privacy data-protection epistemic community:* An epistemic community that focuses on privacy and data-protection as its domain or issue-area. Addition of the
phrase “data-protection” identifies the primary threat, and therefore the primary focus, of most privacy policy and legislation of past several decades. The phrase also differentiates present policy and law from previous periods in U.S. law that historically focused on privacy issues of family, body, or home, or the privacy torts of intrusion, public disclosure, false light, and appropriation.

The Theoretical Model

**Figure 1.1: The Epistemic Community, Intervening Variables, and Privacy Policy/Law.**

- **Independent Variable:** The Privacy Epistemic Community
- **Intervening Variables:**
  - Economic Issues
  - Socio-Cultural Issues
  - Political Issues
- **Dependent Variable:** Privacy Policy & Law
The Epistemic Community as Independent Variable

The independent variable of the privacy epistemic community exerts influence to inform, educate, and advise policy makers and legislators to mollify threats to the dependent variable, privacy. Scholars suggest that the convergence of privacy policy and law over the past half century has been a direct result of the continuing activities and influence of the privacy data-protection epistemic community.\(^{21}\)

Intervening Variables

The intervening variables in this study are the economic issues, socio-cultural issues, and political issues. Comparative policy studies suggest that these intervening variables, characterized as part of the “environment,” “external conditions,” or “socioeconomic variables,” influence priorities, and thus possible choices for any specific privacy problem, and therefore the privacy policy and law that are implemented to resolve the privacy problem.\(^{22}\) This study focuses on the privacy-data protection epistemic community, that network of national and transnational knowledge-based technology and privacy experts with authoritative claim to policy relevant knowledge within the domains of technology and privacy. The privacy-data protection epistemic community gives rise to public awareness of the problem and promotes constructive steps through its ability to educate and influence policymakers and legislators in order to contain, control, or limit the loss of privacy,\(^{23}\) but is subject to the environmental constraints imposed by the intervening variables.\(^{24}\)
Privacy as Dependent Variable

As will be discussed in Chapter Two, the concept of privacy arose in numerous contexts, but not as a unique and stand-alone right until the past half-century. Privacy was normally associated with personal liberty, freedom of association, or property rights and reputation. Aristotle described human beings as “political animals” who needed both public intercourse with other people and privacy for ourselves. He reasoned that the concept of privacy was directly related to society because without the presence of others in society, there would be no need for privacy.\(^25\) John Locke associated the concept of privacy directly with property, considering that the right to property was based on natural law. When added to the Constitution of the United States, the Fourth Amendment also reflected the property aspect of privacy when it stated that: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”\(^26\) The privacy of property was a rather narrowly defined right based on English Common law and the experience of the Constitutional Framers.

Scholars observe that the modern concept of privacy was “invented” by Boston lawyers Samuel Warren and Louis Brandeis as a result of their 1890 arguments for privacy in the *Harvard Law Review*.\(^27\) Warren and Brandeis argued that the right to privacy was separate and apart from the property rights to which privacy had been associated under common law.\(^28\) Of interest to the study of the relationship of privacy
and technology is not only the substance of their legal logic and rationale, but also the environment that produced the Warren and Brandeis article in the first place—the issue of technology (the independent variable) and its effect on privacy (the dependent variable). The proximate motivation to author “The Right to Privacy” mentioned in the early pages of their essay was the fact that “instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”29 The Warrens, a prominent Boston family, were favorite targets of the press gossip. The then recent inventions of the telegraph, the telephone, inexpensive portable cameras (such as the Kodak “Box” Camera), sound recording devices and even improved window glass all made the process of acquiring and processing gossip much easier.30 Based in part on the groundbreaking article by Warren and Brandeis, and stoked by a growing awareness that there was such a thing as “privacy,” the period from 1890 to 1965 was one of continuous but erratic development in the social and legal refinement of the new “right of privacy.”

The burst of technological innovation in computers, databases, and surveillance that followed the Second World War created new threats to individual privacy that galvanized privacy concerns across the nation and promoted the creation of the nascent privacy data-protection epistemic community. The privacy data-protection epistemic community originated with members of the technical computer and database services industry supporting government and industry computers and databases in the late 1950s.
Study Overview

Chapter Two: The Concept of Privacy

To provide background for the two case studies, Chapter Two provides an overview of the evolution of the concept of privacy from antiquity to the post-Civil War era, when technological advances in newspapers, telegraph, telephone, and individual box cameras brought changes in the concept of privacy that resulted in Warren and Brandeis “inventing privacy law” through their essay *The Right to Privacy*. For more than a half-century following Warren and Brandeis’ addition of a new privacy chapter to law, the privacy concepts enunciated by Warren and Brandeis grew, expanded, and were tested in courts across the United States. It was only after the explosion of technological innovation in computers, databases, and surveillance that followed the Second World War had created new threats to individual privacy, and galvanized privacy concerns across the nation, that the nascent privacy data-protection epistemic community coalesced to provide education, guidance, expert advice and policy options to the public and policy-makers.

Chapter Three: The Epistemic Community

Chapter Three reviews antecedents of the epistemic community. This concept can be found embedded in ideas that long predate the work of Peter Haas on epistemic communities in the 1980s. For example, the idea of an invisible college, consisting of a group of scientists with common motivation and purpose, was first introduced in the mid-17th century in London, and is said to be the predecessor of the Royal Society. The idea of the invisible college reappeared in the 1970s in *Invisible Colleges: Diffusion of*
Knowledge in Scientific Communities, and in 2008 in The New Invisible College: Science for Development. The literature of the past two decades has produced numerous journal articles either testing or commenting on the invisible college concept.

Another antecedent of the epistemic community can be found in the work of Arthur Bentley, who in 1908 published the Process of Government: A Study in Social Pressures. Bentley’s contention was that, “All politics and all government are the result of the activities of groups.” In Bentley’s mind, the epistemic community, or knowledge community of experts, would be just one of many groups vying for position and influence in the political process. One might hope that the expert knowledge of the epistemic community provides them an edge in the negotiation for their desired political solution, but Bentley believed that all policies and legislation are the result of constantly competing interests and the groups that represent them.

The role of “experts” in government policy making has been a popular theme ever since the Second World War, when “experts” in many fields were credited with the technical breakthroughs that provided the Allies the edge to win the war. In the early 1960s, Harvey Brooks identified government reliance on “experts” to solve the increasingly complex and technical policy and operational problems that confronted government. Brooks described the technical, (epistemic community) “experts” as taking a larger and larger role in government.

In the late 1960s, Thomas Kuhn popularized the term paradigm, as he described the shared paradigms of scientists conducting “normal” science. In terms very close to
those used by Peter Haas in describing the epistemic community, Kuhn described the shared paradigm of normal science in his *The Structure of Scientific Revolutions*.39

The concept of the epistemic community as popularized by Peter Haas in the late 1980s was thus built on a broad basis of knowledge experts influencing government policy and legislation that spans nearly a century. Over the past two decades numerous other disciplines outside international relations have adopted the term *epistemic community* including public administration, criminology, business, and banking in order to explain the formation and influence of knowledge communities in corporate, public, and government organizations. At the same time, journal articles have addressed the formation of counter-epistemic communities as well as competing epistemic communities, and identified limitations and problems with operationalizing Haas’ definition of the epistemic community.

Recognizing the inherent limitations of the subjective attributions that Haas assigns to members of the epistemic community (such as shared normative and principled beliefs, shared causal beliefs, shred notions of validity and intersubjective, internally defined criteria),40 I identify six objective and observable criteria by which I will identify the epistemic community in this study.

**Chapter Four: United States Privacy Case Study**

The United States Case Study focuses on the origin of the privacy epistemic community in the late 1950s, its growth in the 1960s and 1970s, and its influence on the U.S. Privacy Act of 1974. The origins of the privacy epistemic community can be traced from early technical papers authored by the computer scientists who worked for large
companies that provided mainframe computer and database services to the Federal Government, the Department of Defense, and defense-related industries in the 1950s and 1960s. By the mid-1960s, the early privacy epistemic community members had begun to transition from writing about problems of security to writing about problems of privacy, and often wrote about both in the same paper. Most of these security-privacy papers were authored for the frequent conferences that were conducted by the electronic-computer technical societies. Societies such as the Association for Computing Machinery (ACM), and others, sponsored several regional conferences each year at which technical special interest groups conducted break-out sessions, several of which focused on issues of data and information security, information privacy, and the impact of computers on society.

By the mid-1960s, academics and lawyers had joined computer scientists in the privacy epistemic community and were authoring popular books on the threat to privacy posed by technology such as computers, data processing, and databanks. Proposals for a National Data Center that would collect, store, and process data from all government agencies drew attention from Congress, and privacy-data protection hearings were initiated in 1965.

The congressional hearings provided a natural networking, educational, and indoctrination venue for the privacy epistemic community from which dozens of key privacy protection epistemic community members emerged over the next decade. Several major privacy studies were conducted in the early 1970s, each of which was directed by members of the privacy epistemic community. These studies produced
recommendations that were ultimately folded into the Privacy Act of 1974. Heightened awareness by the American public and Congress of privacy threats following the Watergate Scandal created a window of privacy policy opportunity into which the Privacy Act legislation conveniently fell. Political concerns led to a negotiated compromise in the creation of the Privacy Act such that it applied only to the federal government and did not create a privacy oversight body. The privacy policy window of opportunity had closed by the time that the privacy epistemic community was next able to make substantive recommendation to Congress in 1977 regarding amendments of the Privacy Act of 1974. Thus, the American people are left with narrow, sectoral, privacy protection that applies only to federal agencies and not private sector organizations.

Chapter Five: The European Union Case Study

The European Union Case Study focuses on the origin of privacy awareness and the growth of the privacy epistemic community that influenced privacy legislation, not only in key national data-protection legislation, but also in the crafting of the European Data Protection Directive 95/46/EC. Prominent European privacy data-protection epistemic community members, including Spiros Simitis, Frits Hondius, and Hans Peter Bull from Germany; Jan Freese from Sweden, and Paul Sieghart from the UK, addressed privacy issues in Europe that were the same as those in the United States. Europeans observed the congressional privacy hearings of the mid-to-late 1960s and became aware of the threat posed to individual privacy by automatic data processing and databanks. Key academics, lawyers, and bureaucrats from Europe joined the privacy data-protection
epistemic community in publishing privacy literature, participating in conferences and
testifying in government hearings and meetings.

The Committees of Experts in the Council of Europe (CoE) and the Organization
for Economic Cooperation and Development (OECD) played important roles by creating
trans-Atlantic networking opportunities for members of the privacy data-protection
epistemic community. These committees drafted fair information practices/principles
resolutions, guidelines, and covenants, which shaped the privacy data-protection debates
in the U.S. and the EU.

Finally, the role of the privacy-data protection epistemic community is identified
in the five-year long process by which the European Union Data Protection Directive
95/46/EC was ultimately passed in 1995.

**Chapter Six: Analysis and Conclusions**

In Chapter Six I draw upon my criteria for identifying an epistemic community
and the evidence presented in the two case studies to respond to the three research
questions posed in Chapter One:

1) *Does a single privacy data-protection epistemic community exist?*

The six criteria identified in Chapter Three will be employed to identify the
privacy data-protection epistemic community.

2) *Did the privacy epistemic community influence privacy data protection in the
United States and the European Union?*
Evidence from the case studies in Chapter Four and Chapter Five will be presented to provide both direct and indirect indication of the influence of the privacy data-protection epistemic community.

3) Why did the influence of the privacy data-protection epistemic community result in dramatically different legislation in the United States (The Privacy Act of 1974) and the European Union (directive 95/46/EC on the Protection of Personal Data)?

In answering the third research question, I analyze evidence for economic, socio-cultural, and political intervening variables that may be responsible for differences in privacy policy and legislation in the United States and the European Union in the context of comparative policy studies and empirical evidence.

**Chapter Summary**

This first chapter has introduced key issues and described the purpose of the study, identified the hypotheses and theoretical model, outlined the primary research questions, and provided the framework for the remaining chapters. This study is meant to break new ground in employing comparative case study analysis of the influence of the privacy data-protection epistemic community on policy and legislation in the United States and the European Union.

I will now proceed to Chapter Two with a review of the background of the concept of privacy as a basis for introduction of the epistemic community approach in Chapter Three.
Chapter One Notes


8 George Orwell, *Nineteen Eighty-Four* (New York, NY: Knopf, 1992), 325. References to the dystopias described by Huxley and Orwell posed by computer technologies can be found in the works of early privacy authors such as Westin, *Privacy and Freedom*, 487 and Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, 333.


Ibid.


Prosser, Privacy, 389-407.


Thomas Y. Davies, "Recovering the Original Fourth Amendment," *Michigan Law Review* 98, no. 3 (Dec., 1999), 547. In this extensive essay Davies analyzes the original environment and context of the Fourth Amendment and the many judicial interpretations to which it has been subject over the past two centuries.


33 See: [http://www-history.mcs.st-and.ac.uk/Societies/RS.html](http://www-history.mcs.st-and.ac.uk/Societies/RS.html) regarding the use of the phrase invisible college in London circa 1645.


40 Haas, *Introduction: Epistemic Communities and International Policy Coordination*, 3.
Chapter Two

The Concept of Privacy

I do not have even an every-day definition of “privacy,” or of the “right of privacy.” Some may define “privacy” as the sum of all “private rights.” Many, however, obviously contemplate a discrete private right of privacy, though they may differ widely as to its character and content. So we find innumerable references to the “right to be let alone”; some contemplate a right to be alone, to be free from unwanted intrusion, to be secreted and secretive; a right to be unknown (“incognito”), free from unwanted information about oneself in the hands of others, unwanted scrutiny, unwanted “publicity”; a right of “intimacy” and a freedom to do intimate things. Some offer another kind of definition, a right to be free from physical, mental, or spiritual violation, a right to the “integrity” of one’s “personality.” 1

Louis Henkin
Privacy and Autonomy (1974)

Over the past century, public awareness and concern for “privacy” have dramatically increased—not only in the United States—but also across the developed world. New privacy issues and topics have periodically emerged in response to ever-new technological means of creating and distributing data and information about individuals while the dimensions, role, and importance of privacy have simultaneously evolved within the public consciousness.

The concept of “privacy” is not a new, or even a relatively recent, phenomena. Privacy has been an inherent human concern that has been valued for thousands of years. Yet while the concept of privacy has deep historical roots, personal physical and psychological privacy expectations and attributes have varied widely across societies and
cultures. In the past century and one-half, the concept of privacy has expanded dramatically in the United States as the result of several simultaneous movements:

1) technological innovation that has permitted intrusion, collection, maintenance and integration of ever smaller pieces of more disparate data on the activities and characteristics of individual citizens; 2) the growing awareness of the concept of privacy as a fundamental individual right; and, 3) the legal privacy response in courts and legislatures which have had the effect of structuring, expanding and explicating the right of individual privacy.

As the quotation by Louis Henkin at the beginning of this chapter reflects, even today a concise definition of “privacy” has proven remarkably elusive. This is because the concept of privacy has had no common definition, no agreed upon parameters, and the many facets of privacy are deeply embedded in temporal, social, and cultural contexts. At some times, and in some cultures, privacy has even been viewed as an antisocial characteristic and a negative value because it conflicted with the public values and cohesiveness of society. The very concept of privacy has varied over time and across cultures and has grown to reflect an evolving variety of new perceived threats and incursions into the “privacy” of the individual over the past century. Up until the end of the nineteenth century, privacy was primarily a physical concept having to do with intimacy, concealment of the person and possessions, or the retreat of the individual relative to the outside, or public dimension. Within the past century, the concept of privacy has flourished and blossomed to encompass not only the physical domain, but also the unseen psychological and information-data domains.
This chapter provides an overview of the origins of the concept of privacy and the evolution of the concept of privacy in the United States in order to provide the basis for further discussion of the role of the privacy epistemic community in influencing privacy legislation in the last half of the twentieth century. It will trace the evolution of the concept of privacy in the United States over the past two centuries as privacy has grown from a loose common-law concept, to a constitutional property-based concept, and finally to a constitutionally derived right of the individual.

**Antecedents of American Privacy Concepts**

American concepts of privacy have been influenced and informed by religious tradition and historical experience of more than two thousand years. Perhaps the earliest documentation of the concern for privacy comes from Hebrew history found in the Pentateuch, part of the Torah, which later became the foundation of the Old Testament in the Christian Bible. In the Book of Genesis are several stories that exhibit awareness and concern for privacy in the earliest of times. The first recounting of concern for privacy occurs when Adam and Eve ate the forbidden fruit and “Then the eyes of both of them were opened, and they realized they were naked; so they sewed fig leaves together and made coverings for themselves.” This earliest awareness of the need for physical or body privacy was reinforced shortly thereafter, when, in recognition of their need for personal privacy, “The Lord God made garments of skin for Adam and his wife and clothed them.” Similarly, later in the Book of Genesis, privacy of the person was again the subject in the story of Noah’s nakedness and the response of his sons:
When (Noah) drank some of the wine, he became drunk and lay uncovered inside his tent. Ham, the father of Canaan, saw his father’s nakedness and told his two brothers outside. And Shem and Japheth took a garment and laid it across their shoulders; then they walked in backward and covered their father’s nakedness. Their faces were turned the other way so that they would not see their father’s nakedness.⁵

With these several examples of the concern for physical or body privacy coming so early in the Old Testament, one would expect that the ancient Hebrews would have been highly sensitive to privacy issues, however, as with many biblical sources, the scholar finds conflicting evidence of the concept of privacy in the Old Testament. In his study of Privacy, Barrington Moore describes a distinct lack of the concept of individual privacy, or even a clear conflict between the “public” and the “private,” in early Hebrew history.⁶ Because the central character of early Judaism as both religion and social organizing authority is the single, monolithic Yahweh, from whom no secrets can be hid, Moore finds “the very notion of an area of social and individual life marked off as private and immune to divine interference would be an impossible absurdity . . .”⁷ By the time of Moses, Yahweh had become exclusive to the Hebrews and intolerant of all deviation from his commandments within the Hebrew population. The Hebrew people became the agents of Yahweh in punishing errant attitudes and activities within their families and their tribes. Prophets such as Isaiah and Jeremiah spoke in the name of Yahweh and admonished the people to have no secrets because privacy from God could only serve evil purposes. Thus, “Secrecy from God was equated with wickedness,”⁸ and as Isaiah said, “Woe to those who hide deep from the Lord their counsel, whose deeds are in the
The closeness of the family, the tribe, and the overarching religious community created an environment without discernable privacy. Moore says of the relationship between private and public in ancient Hebrew society:

“It was public in the sense of constituting a system of shared ritual and doctrine, and as the external source of morality and social obligation. As such, it confronted the individual in all the decisions of daily life. It was also a public from whom no secrets were hid and which left little or no autonomous area for private existence.”

Thus, for the ancient Hebrews there was little if any distinction between private and public, for what the modern world would consider to be in the “private” realm was an integral part of Hebrew law and society tightly bound by strict religious norms. Moore does note that the Tenth Commandment, “You shall not covet your neighbor’s house; you shall not covet your neighbor’s wife, or male or female slave, or ox, or donkey, or anything that belongs to your neighbor,” established a de facto right of private property which was invoked by prophets such as Nathan and Elijah against the authority of the kings to have subjects killed and take their property. However, this limitation on the taking of private property by the kings was exceptional because it was communicated directly to the kings by the Lord through the prophets, and did not establish a privacy precedent for all of Jewish society beyond the coveting property prohibition found in the commandments.

In the world of the 5th century BCE Greeks, the concept of individual privacy received mixed reviews. For Plato, the ideal society had no need for privacy, and this was reflected in Plato’s major political treatises. In the model society Plato described in
The Republic, the private sphere would be subordinated in the common community of wives, children, and education. Likewise, for the soldiers who would be housed in common facilities that “have nothing private for anybody but are common for all.”

Barrington Moore observed that although ancient Athens Greece acknowledged the public and the private domain, “Privacy cannot be the dominant value in any society. Man has to live in society, and social concerns have to take precedence.” Moore notes that “the words employed for private convey(ed) some hint of the antisocial in their meaning.”

The esteem with which public life was held in Greece leads to the observation that: “In ancient Athens . . . private life was generally seen as a manifestation of antisocial behavior, although . . . (the) culture recognized the private as well as the public realm.”

Perhaps the most important influence on the American concept of privacy came from the English philosopher John Locke (1632-1704). To John Locke, “. . . privacy was one of the presocietal or “natural rights” which was preserved when individuals, by social contract, agreed to form a society. Furthermore, when society, by a second social contract, agreed to form a government, privacy was one of the rights the government was expected to preserve and protect.” However, Locke recognized the tension between the private and the public of the individual and believed that: “The person is the source of privacy, but the person is also a public figure, a social being.” Thus, Locke recognized the same tension between the public and the private that was displayed in early Hebrew and Greek thought.

Westin credits the philosophy of John Locke with guiding the crafting of the Constitution of the United States and the establishment of a republican form of
The rudimentary concept of privacy, that is, the separation of the individual from society, was understood through tradition and custom in the early American colonies, and privacy was expected and generally observed in daily activities. When privacy was
violated, measures were usually immediately taken to redress and punish its breach at the local or community level. Recourse to formal law was rarely invoked for violations of privacy, in part because privacy law was rather thin—if it existed at all—but more importantly because the formal mechanisms of the law were generally not available in the early colonies.

The concept of privacy in the early American colonies is illustrated by one of the earliest documented cases of what we would today consider an “invasion of privacy.” In 1624, when Plimoth Plantation was only four years old, Governor William Bradford suspected two relative newcomers to the colony (Lyford and Oldham) of undermining his leadership and the future welfare of the Plimoth Plantation. Bradford intercepted numerous incriminating letters written by Lyford and Oldham and addressed to friends in England on board the ship *Charity* just before the ship sailed. “So the Governor called a court and summoned the whole company to appear. And then charged Lyford and Oldham with such things as they were guilty of; but they were stiff and stood resolutely upon the denial of most things, and required proof.” Then Governor Bradford had several of the intercepted letters of Lyford and Oldham read to the assembled court. While Lyford was mute following the reading, “Oldham began to rage furiously because they had intercepted and opened his letters, threatening them in very high language . . .” Following Oldham’s outburst, Governor Bradford turned to Lyford and “asked him if he thought they had done evil to open his letters; but he was silent, and would not say a word . . .” Lyford’s lack of response when asked about the “evil” of reading of his letters is explained by colonial historian Thomas O’Connor who says that:
At least one of the reasons why the defendants could say nothing was that the concept of privacy as a legal entity in the seventeenth century simply did not exist—either for the administration of justice or for the defendant who found himself before the bench. The concept was not to be found either in English common law or in the Biblical law of the Puritans—nor in the curious mixture of both traditions, which became common during the colonial period in Massachusetts.  

The society, environment, and technology of the colonies made privacy expectations significantly different than in later centuries. For most colonists, a small, simple house and a large family made for limited psychological and physical privacy of the individual within the dwelling. For the average family, “Crowded and noisy living conditions and poverty, which subordinate privacy to basic family needs, forced readjustments in the balance of privacy that individual colonists sought.” Having a refuge of privacy in one’s own room or place of escape was for the relatively few wealthy colonists. Settlements were densely built to provide security in the wilderness of the New World with the result that the density of homes within the community allowed for only limited privacy among families. Flaherty points out that: “The colonial concept of privacy, like so many rights and privileges, was essentially a negative one. The colonists expected to be left alone in their homes and families.” Even within their homes and with their families,

Privacy was a luxury undreamed of in that day, and you had little of it. From childbirth to deathbed one’s life was shockingly open to one’s family, friends, relatives, neighbors, enemies, clergymen, and the curious. It was not a matter of social position. At Buckingham, the young King of England, George III, had little more privacy than
a Boston artisan. Nor Louis XV at Versailles. They seemed to have had no more conception of privacy as a desirable thing than they had of electricity, and did not miss either.29

The lack of concern over privacy, *qua* privacy, in the seventeenth century colonies has been echoed by other scholars who note that the concept of privacy was not found in English common law of the time, was not found in the Biblical law of the Puritans, or even in the founding documents of the United States except for what passed as personal property protection in the Fourth Amendment. If the concept of privacy existed at all it was simply accepted as a “given” because the homogeneity and rural nature of American society offered little opportunity for invasions of privacy.30

Privacy was, however, always available within an environment consisting of great stretches of fields surrounding towns and wilderness between settlements---providing nearly unlimited individual privacy in great open spaces.31 An individual could easily step away from the community and find both physical and psychological privacy in the vast solitude of forests and fields. Thus, the balance of individual privacy for many colonists was often achieved outside the home and away from the family and community.

Unlike centuries later, the limited technology of the seventeenth and eighteenth centuries meant that seeing, hearing, and saying were the key privacy issues for most colonists. The spy (or peeper), the eavesdropper, and the gossip were the central threats to privacy. Spying or peeping constituted intrusion by voyeurism; eavesdropping (literally standing under the eaves of the house in order to listen) constituted interception of the spoken word; and gossip constituted divulging that was heard to others.32 Because
opportunities to be seen and heard varied greatly within the community, individual privacy could only be ensured by acting or speaking beyond the sight or ear-shout of others.

The written letter and the printed book or pamphlet were rare, cherished, and closely guarded by the owner. This level of security and privacy was in direct contrast with conditions regarding the transport and delivery of mail and parcels. Because there was no regular postal service in the seventeenth and early eighteenth centuries, when letters and parcels were sent, they were usually carried by friends, itinerant peddlers, ships captains, or people hired for the specific purpose of delivering items. The security and privacy of letters and parcels was always in question. The sending, transport, and delivery of mail was often haphazard for there were no generally accepted rules regarding the mails until the early eighteenth century. The Post Office Act of 1710, enacted in the Reign of Queen Anne, finally sought to ensure the security, privacy, and timeliness of the mails by declaring that: “No person or Persons shall presume wittingly, willingly, or knowingly, to open detain, or delay, or cause, procure, permit, or suffer to be opened, detained or delayed, any Letter or Letters, Packet or Packets.” Under the leadership of Benjamin Franklin, who was Postmaster-General from 1753 to the Revolution, security and privacy of the American mail became a central issue. All persons who worked in the post office or had anything to do with the receipt, transport, or delivery of the mail were required to take the “Oath required by the Act of the Ninth of Queen Anne” which bound the individual to the Act of 1710. The only exception to this oath was a Warrant in Writing signed by a Secretary of State, under which the mails could be opened and inspected.
When privacy was violated, the offense was usually dealt with at the scene, or the community employed sanctions and public chastisement to punish the offender. Only rarely were legal measures invoked in cases involving privacy, “for privacy as a part of English common law did not exist in the seventeenth century. Neither was the concept to be found in the Biblical law of the Puritans, nor in the mixture of both traditions that was prevalent in colonial Massachusetts.” Recourse to the law for issues of privacy were based on extensions of property rights that individuals have in themselves such as intrusion and material wrongs, such as damage to reputation (property).

In additional to the lack of privacy-specific law, the vagaries of formal common law in the colonies made the law and the expected outcome questionable:

The conditions of settlement and of development within each colony meant that each evolved its own individual legal system, just as each evolved its individual social and political system. Geographical isolation, the date and character of the several settlements, the degree of absence of outside supervision or control---all had their effect in ultimately developing thirteen different legal systems. The law of each colony was thus unique to that colony, and generally consisted of an agglomeration of three sources: 1) remembered elements of English law; 2) law based on special problems and issues that the settlers came upon in their new home, and which were not part of their previous law experience; and 3) the ideological aspect of law based on who they were—for example the Puritans who were guided by a strict set of religious beliefs that influenced their law. The vagaries of law among the 13 colonies thus ensured differences in the observation and enforcement of privacy infractions at law. But “(b)ecause privacy was not seriously threatened, it was taken for granted---recognized and revered by custom and circumstances.”
Pamphlets, and later newspapers, found only in the few largest communities in the seventeenth and eighteenth centuries, did not generally intrude upon the privacy of colonists until well after the founding of the nation because: “Until the 1830s, a newspaper provided a service to political parties and men of commerce . . . .”\(^42\) It was only in the 1830s, when papers expanded in numbers, content, readers, and competition that a revolution in newspapers took place. “That revolution led to the triumph of “news” over the editorial and “facts” over opinion, a change which was shaped by the expansion of democracy and the market . . . .”\(^43\) That change generated great changes in the concept of privacy in the United States.

**Privacy at the Founding of the Nation**

Although the word “privacy” is not found in any “founding documents” of the United States, protections for property, and thus for some dimension of privacy of the individual, were incorporated as an afterthought to the constitution. In fact, many of the issues surrounding privacy that were experienced in the American Colonies under British rule prior to the Revolution were addressed in the Bill of Rights in 1791. Over the past century legal scholars have argued that numerous “privacy” protections are embedded or implied in the First, Third, Fourth, Fifth, and Ninth Amendments to the Constitution of the United States.\(^44\)

*Amendment I*  
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. \(^45\)

*Amendment III*  
No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.\(^46\)
Amendment IV  The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

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

Amendment IX  The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people. 47

Today, it is generally acknowledged that privacy was implied in these several amendments to the Constitution. But in the nineteenth century courts routinely found that the Fourth Amendment with its guarantee of “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” was the only constitutionally guaranteed privacy for the individual. Recognition of implied privacy rights inherent in amendments beyond the Fourth Amendment were identified and developed only in the late twentieth century by privacy scholars. With the exception of the Fourth Amendment, there is no indication that these amendments were ever thought to grant any specific right of “privacy” outside the context of “property” to individual citizens prior to the Warren and Brandeis “creation” of the right of privacy in
1890. In fact, as one legal scholar observed, “The Constitution does not confer private
rights; they are antecedent to and independent of the Constitution. The Constitution does
not even command that government grant, promote or extend private rights; it only places
limits on the infringement of private rights by government, both the rights specified and
all others “retained by the people”.\textsuperscript{48}

The Concept of Privacy in the 19\textsuperscript{th} Century

Following the founding of the United States, privacy remained a vague concept
for citizens of the new United States---an extension of colonial privacy concepts based on
custom and common law property rights such as trespass or intrusion---and not associated
with a distinct legal doctrine. The Constitution of the United States had been modified in
1791 to add ten amendments called the Bill of Rights.\textsuperscript{49} As noted previously, one of
these, the Fourth Amendment, did explicitly guarantee “The right of the people to be
secure in their persons, houses, papers, and effects, against unreasonable searches and
seizures,”\textsuperscript{50} but there was no explicit right of privacy that legal scholars could draw upon.
It’s true that scholars could point to the influence of John Lock and the implicit privacy
nuances incorporated in the First Amendment, protecting the privacy of not having to
speak, the privacy of opinion, the privacy inherent in freedom of association, and the
privacy right of anonymous or pseudonymous expression. The Third Amendment
guaranteed the privacy of the home from troops being quartered without the
homeowner’s consent during peacetime but quartering of troops in private homes ceased
to be an issue in the new United States. The Fourth Amendment explicitly guaranteed
security, and implicitly privacy, against unwarranted searches and seizures of “persons,
houses, papers, and effects,” which were effectively the technology of the era. The Fifth
Amendment carried the implied privacy right inherent in the privilege against self-incrimination. Between the establishment of the nation and the Civil War one noted privacy scholar, Alan Westin, wrote that American society: “had a thorough and effective set of rules with which to protect individual and group privacy from the means of compulsory disclosure and physical surveillance known in that era.” Working within the construct of the Fourth Amendment, cases with privacy implications did occasionally appear on court dockets, and the dimensions of the property-related right of privacy were occasionally explored by the judiciary. The technology of the eighteenth and early nineteenth centuries essentially limited privacy issues to the written word, direct speech, and direct sight. The only means for physical surveillance was by use of the eyes and the ears, the only means of extracting information from the mind was by use of torture, and there was little documentation or record keeping about individuals.

Additionally, in the decades following the founding of the United States, the population was relatively sparsely distributed across the nation’s land, and the same factors of wilderness and open space that provided individual privacy for the early American colonists continued to provide a great degree of privacy for the population into the early nineteenth century. The expansion of the western frontier echoed in Greeley’s advice to “Go west, young man, and grow up with the country,” was as much an admonition to distribute the population and ensure privacy as for economic reasons of exploiting the new wilderness of the west. O’Connor notes that the “element of distance” was an important factor in securing privacy on the American frontier saying that: “privacy in early America was in many ways much more of a geographical fact than a constitutional theory.” In the early nineteenth century America was a rural, agrarian,
nation with its population sparsely distributed on homesteads, farms, and many small towns, but the dynamics of immigration and large families quickly changed population numbers and concentrations.

At the time George Washington became President there were just under 4 million inhabitants in the country. By 1810 this population had grown steadily to 7 million. But between 1810 and 1850, the American population leaped to 23 million—a three-fold increase of the entire population in only 40 years; and by the turn of the century the population had risen to 76 million—more than tripling the population once again!\(^\text{54}\)

These dramatic increases in population decreased the physical distances between and among them and impinged upon their privacy, even on the frontiers. Other factors were also at work that influenced privacy perceptions. As the population of the United States increased in the nineteenth century, the concentrations of population changed too. The rise of industry and manufacturing, improvements in agriculture, and the creation of improved road, rail, and water infrastructure conspired to initiate the transition from a rural, agrarian society to an urban, industrial society in the United States. The urbanization of the country is illustrated by recognizing that:

Even as late as 1820 there were only 13 communities in the United States which could boast of more than 8,000 inhabitants; but the widespread appearance of manufacturing, the building of roads, and the advent of the railroad brought about such a rapid growth in large cities that by 1860 there were over 140 urban communities in the nation, and by 1900 the figure had risen to 547—with one out of every three Americans already living in crowded urban conditions.\(^\text{55}\)

A concept of privacy based on a sparse population, widely distributed in small rural, agrarian settlements in the early nineteen century slowly evolved and produced a cognitive dissonance of privacy perception within society that reached its height in the
last decades of the century. Wilderness and geographical separation, constitutional protections, and statutory laws worked well to protect the privacy of citizens into the first half of the nineteenth century. However that rapidly changed as population, technology, urbanization and concomitant social changes conspired to create new threats to individual privacy. As O’Connor observed:

Even at the very moment when individual liberties and the undefined by substantially real sense of personal privacy seems to have reached an historical climax, the physical and philosophical conditions which created such a climate of opinion were already swiftly disappearing. From the middle of the nineteenth century on, the entire political, social, economic, and cultural structure of the United States underwent a complete and significant change.\(^56\)

The first major change in the landscape of privacy in the early nineteenth century was brought about by the growth and popularity of newspapers. The decade of the 1830s is generally identified as when the revolution in American journalism began. In that decade the American newspapers transformed themselves from small, expensive, commercial and political party papers that were read by only business and political elites, to larger distribution “penny press” papers that sought out not only commercial and political information to print, but also local and social news that appealed to an increasingly varied middle-class urban population.\(^57\)

Technological developments were also important to the increasing number, reach, and circulation of the penny press newspapers. The first of many advances in printing took place in the first decade of the nineteenth century. Wood hand presses were replaced with iron presses that were easier to operate and produced higher quality impressions.\(^58\) In 1814, the steam powered cylinder press was introduced, which
produced about ten times the imprints per hour as the hand operated pressed. By mid-century the double cylinder “Hoe Type Revolving Machine” had revolutionized the speed, output, and cost of printing, making it possible to sell newspapers cheaply. 59

Breakthroughs in the production of paper and improvements in railroad and canal transportation also facilitated the expansion and reach of newspapers in the first half of the nineteenth century.

For the first time, the new penny press newspapers sought out “news” as the mainstay of their appeal to their readers. They hired reporters who reported on local events even though “The institution of paid reporters was not only novel but, to some, shocking.” 60 The penny press actively sought out “news,” and often actively compromised the privacy of those about whom they wrote, and in so doing, “. . . ushered in a shared social universe in which “public” and “private” would be redefined.” 61

By the middle of the nineteenth century new technologies augmented the newspaper ability to capture, publish, and distribute information. The entire landscape of privacy changed once again with the invention of new technologies such as long-distance telegraph and telephone communications, 62 fast, portable Kodak photography, 63 faster high-quality newspaper printing, 64 and sound-voice recording capability. 65 These new technologies suddenly exposed individuals to numerous new threats to their privacy because of the ability to intercept, “capture,” and preserve the spoken word and the exact photographic image of a person or event, and then print them in a relatively permanent form and widely distribute them to distant places in the newspaper. One legal scholar noted that the concept of privacy in modern law is directly linked to the technology of printing, saying, “Privacy, like copyright and obscenity, had no direct legal ancestor in
the preprint era. As a legal concept, privacy is something new, a field of law whose origin is linked to printing, although the relationship is more complex . . . ”66 Because there was no clear legal doctrine that addressed the publication of personal information by media empowered by First Amendment “freedom of the press,” there was little to restrain newspapers from printing all “news,” whether fit to print or not.67

**Growth of Concern Over Newspapers and Privacy**

Concern for the proliferation of newspapers and changes in their news focus alarmed many social observers because of the advent of new issues of invasion of privacy by the press. One of the first to recognize the threat posed by the rise of the penny press newspapers was the author James Fenimore Cooper. Cooper had left the United States to write in Europe for seven years (1826-1833). When he returned to the United States, he was struck by the changes in American journalism that had occurred during his absence. Cooper attacked the new penny press newspapers for creating a “press-o-cracy” by seeking their own ends and not those of the community. He vilified the press in books such as *Homeward Bound* (1838), *Home as Found* (1838), and *The American Democrat* (1838).68 In *The American Democrat* Cooper wrote:

> If newspapers are useful in overthrowing tyrants, it is only to establish a tyranny of their own. The press tyrannizes over publick men, letters, the arts, the stage, and even over private life. Under the pretence of protecting publick morals, it is corrupting them to the core, and under the semblance of maintaining liberty, it is gradually establishing a despotism as ruthless, as grasping, and one that is quite as vulgar as that of any Christian state known. With loud professions of freedom of opinion, there is no tolerance; with a parade of patriotism, no sacrifice of interests; and with fulsome panegyrics on property, too frequently, no decency.69
Cooper was one of the first to identify the threat that new newspaper business ethics posed to individuals and to society. Although press tyranny over “private life” was listed as one of several domains into which newspapers intruded, Cooper was responding more generally to the new power of the penny press and the influence it wielded in society. “The new journals reflected political, social, and technological changes that a thoughtful man might well have been alarmed about.”

The issue of individual privacy attracted the attention of Judge Thomas McIntyre Cooley on the Michigan Supreme Court, who wrote in his *Treatise on Constitutional Limitations* in 1868 that: “It is sometimes better that crime should go unpunished than that the citizen should be liable to have his premises invaded, his desks broken open, his private books, letters, and papers exposed to prying curiosity, and to the misconstructions of ignorant and suspicious persons.” Later, in his *Treatise on the Law of Torts* (1888) Judge Cooley insisted that: “The right to one’s person may be said to be a right of complete immunity: to be let alone.” Cooley’s phrase was subsequently made immortal in the privacy literature by Warren and Brandeis in *The Right to Privacy* when they characterized their concept of privacy as the right “to be let alone.”

The journalist, editor, and founder of *The Nation*, E. L. Godkin, was particularly sensitive to the issue of individual privacy and authored an article entitled *The Rights of the Citizen. IV. To His Own Reputation* in the July 1890 issue of Scribner’s Magazine. Just five months before Warren and Brandeis published *The Right to Privacy* Godkin provided his readers a summary of the threats posed by the press to the privacy of individuals. Godkin declared that, “Privacy is a distinctly modern product, one of the luxuries of civilization, which is not only unsought but unknown in primitive or
barbarous societies.” Although the awareness and need for privacy varied among individuals, it was integral to personal dignity, and had to be protected. Godkin suggested that: “The chief enemy of privacy in modern life is that interest in other people and their affairs known as curiosity, which in the days before newspapers created personal gossip.” The worst thing about gossip published in newspapers was that what would have been between neighbors in the past was now broadcast to the world. As Godkin characterized it:

In other words, gossip about private individual is now printed, and makes its victim, with all his imperfections on his head, known hundreds or thousands of miles away from his place of abode; and what is worst of all, brings to his knowledge exactly what is said about him, with all its details. It thus inflicts what is, to many men, the great pain of believing that everybody he meets in the street is perfectly familiar with some folly, or misfortune, or indiscretion, or weakness, which he had previously supposed had never got beyond his domestic circle.

Godkin did not believe that the law could protect the individual against invasion of privacy and suggested that the only remedy was “. . . to be found in attaching social discredit to invasions of (privacy) on the part of conductors of the press.” He immediately realized, however, that such discredit would often be nullified by the fact that newspapers often greatly profit from invasions of privacy. When Godkin summarized the threats to privacy in July 1890 he could not have know that only five months later Warren and Brandeis would publish The Right to Privacy, citing Godkin’s Scribner’s Magazine article, and suggesting legal remedies to just the invasions of privacy of which Godkin wrote.
The Concept of Privacy From 1890 to 1965

The first major turning point in the development of the concept of privacy took place following the publication of an article in the Harvard Law Review entitled The Right to Privacy in 1890. Two Boston law partners, Samuel D. Warren and Louis D. Brandeis, both recent graduates of Harvard Law School, authored what various legal scholars have called “the most influential law review article of all,” an unquestioned “classic,” and an “outstanding example of the influence of legal periodicals upon the American law.” Warren and Brandeis are credited with “inventing” the right to privacy by authoring “a pearl of common-law reasoning” in an essay “that single-handedly created a tort.” The long-term impact of The Right to Privacy on the evolution of privacy theory and jurisprudence would be hard to overestimate. Within two decades of its publication, an article in the American Law Review called it “one of the most brilliant excursions in the field of theoretical jurisprudence which the recent literature of the law discloses.” Shortly thereafter, the Columbia Law Review noted that The Right to Privacy “enjoys the unique distinction of having initiated and theoretically outlined a new field of jurisprudence.”

The invention of the right to privacy, initiation of a new field of jurisprudence, and creation of a new tort was based on Warren and Brandeis’ extension of previous privacy rights, based on property law, to encompass the damage to the individual’s feelings, personality and private life based on intrusion and exposure of personal information. Warren and Brandeis cited Godkin’s then recent article on privacy, and borrowed Judge Cooley’s now famous definition of privacy as the right “to be let alone.”
Warren and Brandeis elegantly articulated an argument that had been nascent in American society for several decades---that the privacy of the individual was being compromised by new technologies and innovations---and Warren and Brandeis suggested that a solution rested with a new law of privacy. Many legal scholars have suggested that the proximate cause of Warren and Brandeis’ concern over privacy was the result of intrusions into the Samuel Warren’s personal life by Boston newspapers, because Warren and Brandeis wrote that:

The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.88

While the proximate subject of Warren and Brandeis’ treatise was the newspapers that intruded upon, or invaded the privacy of prominent citizens such as Samuel Warren, they acknowledged that the culprits that allowed the newspapers this invasion of privacy were really the underlying and enabling technologies that had been created in the second half of the nineteenth century. Warren and Brandeis openly identified these technologies and then blended them with the act of newspaper reporting, in The Right to Privacy when they said that: “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”89 Thus, Warren and Brandeis responded to the results of the employment of these recent technologies by newspapers---the publication of alleged
personal information in the form of “gossip” for the “prurient tastes” of newspaper readers---and outlined a new facet of privacy law that would rest on injury to the feelings and injury to one’s “inviolate personality,” suggesting that there is “a general right to privacy for thoughts, emotions, and sensations, (and) these should receive the same protection (at law), whether expressed or in writing, or in conduct, in conversation, in attitudes, or in facial expression.”

The new legal right of privacy advanced by Warren and Brandeis in *The Right to Privacy* did not meet with universal accolades. Some argued from a practical standpoint that the right of privacy did not exist as a specific legal right, and that the arguments in favor of a right of privacy were based on a misunderstanding of the authorities that Warren and Brandeis had cited. They believed that inconvenience or injury that persons might suffer connected with the enjoyment of possession of property was the only basis for redress, and that there was no equity concern for the feelings of the individual or with considerations of moral fitness as expressed by Warren and Brandeis.

The privacy discussion initiated by Warren and Brandeis began almost immediately in the courts and then entered the law journals as the privacy theory debate quickened. One of the first significant challenges to the Warren and Brandeis new right to privacy came in 1902 from the Court of Appeals of New York in the case of *Roberson v. Rochester Folding Box Co.* Without the consent of the plaintiff, the defendant used a picture of the young girl to advertise their flour with the tag-line “The Flour of the Family.” In a three-to-four decision the court declared that a right to privacy in this case did not exist, thus rejecting the privacy arguments of Warren and Brandeis. The court based its decision on “the lack of precedent, the purely mental character of the injury, the
“vast amount of litigation” that might be expected to ensue, the difficulty of drawing a line between public and private figures, and the fear of undue restriction of the freedom of the press." Following the Roberson v. Rochester Folding Box Co. decision the storm of negative public reaction motivated one of the concurring judges, Judge Denis O’Brien, to take the unusual step of defending the court’s decision by publishing a law review article in the Columbia Law Review. O’Brien concluded his defense of the court’s decision by noting New York did not have a positive law that applied to the unauthorized use of Roberson’s picture. In response to the public clamor regarding the Roberson decision, the New York Legislature enacted the nation’s first statutory right to privacy.

Just three years later, in 1905, a similar case was considered by the Supreme Court of Georgia in Pavesich v. New England Life Insurance Co. The defendant employed not only the plaintiff’s picture but also a specious testimonial, allegedly from the defendant, in praise of the New England Life Insurance Company. Even though Paolo Pavesich was a well-known artist, and a public figure, the court said that, “It is not necessary to hold that the mere fact that a man has become what is called a public character, either by aspiring to a public office, or by exercising a profession which places him before the public, gives to every one the right to print and circulate his picture." In a unanimous decision, the Supreme Court of Georgia rejected the Roberson case, endorsed the views of Warren and Brandeis, recognized the existence of a right of privacy, and established a precedent case in support of the recognition of expanded privacy rights. “For the next thirty years there was a continued dispute as to whether the right of privacy existed at all, as the courts elected to follow the Roberson or the Pavesich
case. Along in the thirties, with the benediction of the *Restatement of Torts*, the tide set in strongly in favor of recognition, and the rejecting decisions began to be overruled.\(^{100}\)

The next milestone in the dispute over whether a right to privacy existed, and in what form, came in 1928 in the case of *Olmstead v. United States*.\(^{101}\) *Olmstead* is considered to be a pivotal privacy case of the early twentieth century not only because the U.S. Supreme Court rejected the idea that privacy was a separate constitutional right that was protected by the “unreasonable search and seizure” clause of the Fourth Amendment, but because of the elegant dissenting arguments made by Associate Justice Louis Brandeis. Roy Olmstead, and more than 50 others were convicted of violating the National Prohibition Act, challenged his conviction claiming that the evidence of wiretapped private telephone conversations was a violation of the Fourth Amendment.\(^{102}\)

Chief Justice Taft, writing for the court, reasoned that privacy protection of the Fourth Amendment did not apply to telegraphic and telephonic messages as it did to sealed letters in the mail. Taft reasoned that there was no searching or seizing and no entry into personal or private places to secure evidence. The evidence had been obtained in public places that were not part of petitioner’s houses or offices, and were therefore not protected under the Fourth Amendment.\(^{103}\)

Associate Justice Louis Brandeis authored an elegant dissenting opinion to the majority (5-4) in which he argued that technological advances had made it possible for the government to invade privacy in more ways, and by more subtle means, than the limited physical search and seizure activities imagined by the authors of the Fourth Amendment. Additionally, the use of transcribed telephone conversations without the speaker’s consent violated the self-incrimination clause of the Fifth Amendment. Just as
the mail was a public service provided under the authority of the government, the telephone was also a public service provided under the authority of government. Brandeis therefore reasoned that there was no difference between a private telephone conversation and a sealed letter in the mails. “The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails,” Brandeis declared.104 The Fourth and Fifth Amendment protections are broad in scope and the framers:

“...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. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.”105

Brandeis thus laid the philosophical groundwork for an understanding of constitutional privacy that was in keeping with the rapidly advancing technology of the twentieth century and presaged the expansion of the Fourth Amendment privacy law to include wiretapping that would occur nearly four decades later in *Katz v. United States* (1967).

In 1967, the Supreme Court reversed the *Olmstead v. United States* (1928) decision in *Katz v. United States*. Charles Katz was convicted in California of illegal gambling based on the FBI electronically recording his conversations in a public pay telephone booth. In a 7-1 decision the Supreme Court held that so long as an individual can justifiably expect his conversation to remain private, his conversation is protected by
the Fourth Amendment “unreasonable search and seizure” clause. Additionally the court for the first time said that the Fourth Amendment protects people, not places, and the rights of the individual are therefore protected in the absence of physical intrusion. Justice Potter Stewart wrote: “No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment.”

This ruling was important for two reasons: 1) the court enunciated privacy protection based on the individual’s “reasonable expectation” of privacy; and 2) the Fourth Amendment was declared to protect people, not places, extending privacy protections beyond the physical home or office. As an adjunct, Justice John Harlan authored a two-part test which subsequently became the most common formulation cited by the courts for determining whether police activity constituted a search within the meaning of the Fourth Amendment: “ . . . first that a person have exhibited an actual (subjective) expectation of privacy and, second that the expectation be one that society is prepared to recognize as “reasonable”.”

While Supreme Court decisions acted to expand and define the concept of privacy, academic legal analysis played an important part in expanding the recognition of privacy protections in other arenas. In 1960, William Prosser, Dean of the University of California School of Law, authored “what is considered to be the second most important tract on privacy,” after that of Warren and Brandeis. Prosser analyzed more than three hundred privacy cases, noting that, “It is only in recent years, and largely through legal writers, that there has been any attempt to inquire what interests are we protecting, and
against what conduct,"109 and then went on to identify and explicate the following four privacy torts:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which placed the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.110

Prosser noted that a careful reading of Warren and Brandeis’ The Right to Privacy reveals that they were primarily concerned only with the second form of tort, having to do with public disclosure of embarrassing private facts by the newspapers.111 Yet in a period of only 65 years, this single article by Warren and Brandeis---focusing on only a single privacy tort---had ramified into several privacy torts and a growing number of ever more specific privacy rights. Prosser’s scholarly discussion of privacy torts was written at the beginning of what became an explosion in privacy concerns in the following several decades as science and technology provided the means for privacy to be compromised by government, business, and individuals in an information, biological, and physical technology explosion.

Privacy After 1965

Wars generate technological change, and World War II engendered more technological change than any previous conflict. Following World War II, the momentum of scientific discovery and technological innovation generated during the war was harnessed to produce new breakthroughs in all dimensions of American life.112 Although much of the work in fields such as biology, medicine, and information technology took place in prior decades, the impacts of new knowledge and technology on
privacy had matured, and began to be felt in society, by the 1960s. Thus, the 1960s saw a plethora of social and legal discussions regarding privacy issues as new technologies from contraceptives and advanced medical procedures to computers and databases changed the privacy landscape in the United States.

Laws in the United States are created in one of two ways, by federal or state legislative action or by Supreme Court decisions—thus privacy law in the United States consists of an admixture of legislated law and court-decision created law. While the threat to privacy posed by computers and databases was recognized early by some in the information technology field, the legal profession, and academia, the first, and most significant changes in the evolving concept of privacy took place as a result of issues surrounding individual reproductive rights or reproductive choice. Three high-profile cases, *Griswold v. Connecticut* (1965), *Eisenstadt v. Baird* (1972), and *Roe v. Wade* (1973) changed the concept and scope of privacy and are generally credited with not only finally establishing a definitive constitutional right of personal physical or privacy of the body, but also creating a solid consciousness or awareness of “privacy” in the minds of the American people.

In 1965, the *Griswold v. Connecticut* decision by the Supreme Court suddenly brought the issue of privacy to the consciousness of the American public and is credited with finally establishing a general constitutional right to privacy. *Griswold v. Connecticut* addressed a Connecticut law that prohibited the use of “any drug, medicinal article or instrument for the purpose of preventing conception . . . ” by married couples. In a 7-2 decision the Supreme Court ruled that the Connecticut law was unconstitutional and violated the “right to marital privacy.” Justice William O. Douglas
authored a majority opinion in which he wrote that the right to privacy was found in “penumbras” and “emanations” of other constitutional protections found in the First, Fourth, and Fifth Amendments. Three additional justices wrote concurring opinions, Justice Goldberg basing his decision on the Ninth Amendment, while Justices Harlan and White based their decision on the due process clause of the Fourteenth Amendment. Together they identified “a composite right to privacy, drawing its substance from a number of the Bill of Rights’ guarantees in language which appeared to indicate a strong constitutional presumption against any manner of governmental infringement.”

With the *Griswold v. Connecticut* decision a broad right to personal privacy was recognized for the first time based on “penumbras” and “emanations” of five amendments. Justice Douglas established the pedigree of the right to privacy by saying that, “We deal with a right of privacy older than the Bill of Rights.” *Griswold v. Connecticut* represents one of the major turning points in privacy law and has subsequently been cited as a benchmark in cases that have further expanded the bounds of privacy in the United States.

In 1972, *Eisenstadt v. Baird* expanded the concept of individual privacy when it established the right of unmarried couples to have and use contraception the same as married couples. In a 6-1 decision, the Court recognized the rights of single people to procreate *vel non* (or not), and by implication sanctioned the ability of unmarried couples to engage in sexual relations. Writing for the majority, Justice Brennan held that the right of privacy established by *Griswold v. Connecticut* extended to unmarried couples, saying, “If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted government intrusion into matters so fundamentally
affecting a person as the decision whether to bear or beget a child.”

The effect of *Eisenstadt v. Baird* was to extend the right of privacy enunciated in *Griswold v. Connecticut* to the individual, and, “A person could carry this right anywhere; it was a freedom that would no longer be confined to one’s bedroom or house.”

In 1973, the Supreme Court, in a decision that has since proven to be one of its most contentious, expanded the right of privacy by striking down bans on abortion in *Roe v. Wade*. Basing its decision on the constitutional right to privacy emanating from the Due Process Clause of the Fourteenth Amendment, the Court held that a woman could abort her pregnancy for any reason, up to the point at which the fetus became viable, which was defined as the ability to live outside the womb. Justice Blackmun, writing for the majority, declared:

> This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.

The Court’s *Roe v. Wade* decision elicited a national debate that continues to the present day regarding the right of abortion in the United States. Although the debate has at times been acrimonious, it has been one of the principal generators of privacy awareness for the American public and catapulted the issue of privacy into the spotlight, as it had never been before.

At the same time that issues of personal body privacy issues were being adjudicated, parallel privacy issues were being recognized in the realm of information and data privacy as it affected the privacy of the individual. Beginning with the *Title III*
of the Omnibus Crime Control and Safe Streets Act of 1968,\textsuperscript{123} the Freedom of
Information Act of 1966,\textsuperscript{124} the Fair Credit Reporting Act of 1970,\textsuperscript{125} the Family
Educational Rights and Privacy Act of 1974,\textsuperscript{126} and the Privacy Act of 1974, the United
States Congress created laws to protect information and data privacy of individuals. The
evolution of the concept of privacy, and the growth and influence of the privacy
epistemic community in creating privacy legislation in the two decades prior to the
passage of the Privacy Act of 1974 is the subject of the Chapter Four case study.

Chapter Summary

Privacy in the United States can trace its conceptual lineage to some of the earliest
peoples in Western Civilization, to include the Hebrews and the Greeks. However, it was
the English philosopher John Locke who had the greatest influence in associating the
right of property to the liberty of the individual. Locke’s philosophy regarding liberty of
property and person influenced the Founders to include specific property and person
protections in the Fourth and Fifth Amendments, although the word “privacy” was not
used in any of the founding documents.

In 1890, Warren and Brandeis elegantly argued that technological and social
changes had severely compromised the privacy of individuals and they outlined common
law arguments for the right “to be let alone.” Their article ignited philosophical and legal
debates in the United States that continue to rage today regarding the definition,
characteristics, types, and contexts of individual privacy. Supreme Court decisions in the
six decades following Warren and Brandeis’ article were often contradictory, but, in
general, the concept of privacy implicit in the Fourth and Fifth Amendments was
expanded and clarified.
In the 1960s, the issue of privacy once again became a major topic of philosophical and legal interest in the United States because of technological changes that dramatically impacted the reproductive and informational domains. In 1965, the Supreme Court finally established a general constitutional right to privacy in their *Griswold v. Connecticut* decision. Subsequent Supreme Court decisions have significantly expanded the personal and physical privacy bounds created in *Griswold v. Connecticut*. Supreme Court expansion of Fourth Amendment “search and seizure” privacy protections in decisions such as *Katz v. United States* (1967), were expanded and clarified by Congress in legislation such as *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*.

In Chapter Three, I will introduce the concept of the epistemic community as an intervening variable in influencing legislative outcomes. I will identify the characteristics of the epistemic community, limitations of the epistemic community, and provide the criteria by which the presence and influence of an epistemic community can be measured.
Chapter Two Notes


2 Barrington Moore Jr., *Privacy: Studies in Social and Cultural History* (Armonk, NY: Pantheon, 1984), 328. Moore identifies this public-private tension in the three major case studies he investigates, Athenian, Hebrew, and Chinese. In each case there was a requirement to be a public citizen that mitigated against, and precluded, the right of a private existence.


6 Moore, *Privacy: Studies in Social and Cultural History*, 328. See Chapter Three, Privacy, Prophecy, and Politics in the Old Testament for a detailed overview of the inherent lack of privacy predicated on an all-knowing, all-seeing, Deity from whom the individual can withhold no actions or thoughts.

7 Ibid., 169.

8 Ibid., 172.


11 Ibid., 182.


13 Ibid., 2 Samuel 11-12. The prophet Nathan rebuked King David over the death of Uriah the Hittite and the taking of his widow, Bathsheba, as David’s wife. At 1 Kings 21, find the story of how Elijah rebuked King Ahab and his Queen Jezebel over the death of Naboth and the taking of Naboth’s vineyards. In both cases it was the coveting and taking of private property by the monarch that motivated the wrath of the Lord. Moore
suggests that these events served to create and sharpen the bounds between the public authority of the monarch and the private lives and property of the subjects.


15 Ibid., 123.

16 Ibid.


21 Ibid.


24 Ibid., 152.

25 Ibid.


28 Ibid., 245.


Quoted in Ibid. Flaherty devotes Chapter Four to the evolution of security and privacy for the mail in Colonial New England.

Ibid., 121.


Ibid., 35.


Ibid., 14.


Ibid.

Ibid.
48 Henkin, Privacy and Autonomy, 1412.

49 Ibid.

50 See generally, Thomas Y. Davies, "Recovering the Original Fourth Amendment," Michigan Law Review 98, no. 3 (Dec., 1999), 547. Davies recounts the pre- Constitution history surrounding the creation of the rights formally enunciated in the Fourth Amendment and what those rights meant to the Founders.

51 Westin, Privacy and Freedom, 337-338.

52 Hixson, Privacy in a Public Society: Human Rights in Conflict, 18.

53 O'Connor, The Right to Privacy in Historical Perspective, 103-104.

54 Ibid., 109.

55 Ibid., 107.

56 Ibid., 105.


58 Ibid., 31.

59 Ibid., 33.

60 Ibid., 24.

61 Ibid., 30.

62 Inventors at http://inventors.about.com/library/inventors. The telegraph, first demonstrated by Morse in 1838, was in use by Western Union coast-to-coast by 1861; the telephone was successfully demonstrated by Bell in 1876 and immediately began to eclipse the telegraph.

63 The Kodak Camera. Insight: Collections & Research Centre. www.nmsi.ac.uk/nmpfrt/insight/onehib_TheKodakCamera.asp. After several “box” cameras were developed in the mid-to-late 19th century, George Eastman developed the first Kodak in 1888, which rapidly became the technological standard of the early 20th century.

65 The History of Sound Recording Technology. http://www.recording-history.org/html/musictech2.html . Edison demonstrated his first functional phonograph in 1877 and had improved his design as the Graphophone within the decade.


68 Ibid., 12-13.


74 Edwin Lawrence Godkin, "The Rights of the Citizen-IV: To His Own Reputation," Scribner’s Magazine 8, no. 1 (July, 1890), 58.

75 Ibid., 65.

76 Ibid., 66.

77 Ibid.
78 Ibid., 67.


84 Ruth Gavison, "Too Early for a Requiem: Warren and Brandeis were Right on Privacy vs. Free Speech," *South Carolina Law Review* 43, no. 3 (Spring 1992), 438.


88 Ibid., 196.

89 Ibid., 195.

90 Ibid., 205.

91 Ibid., 206.


"In this series of events we can see political evolution at work. We can see the effect of public opinion upon law and institutions in the making. For all these things appeal to the decent and unsophisticated human mind as outrages. And the highest legal authority in the greatest State in the Union assures us that they are outrages for which the law provides no remedy. So much the worse for the law say all the decent people. If there be, as Judge Parker says there is, no law now to cover these savage and horrible practices, practices incompatible with the claims of the community in which they are allowed to be committed with impunity to be called a civilized community, then the decent people will say that it is high time that there were such a law. In some way they will see to it that there is such a law, and the Court of Appeals will not be left to shadowy analogies and precedents for its conclusion that these outrages are legally unpreventable and unpunishable. It will have the advantage of a clear and explicit statute to construe."

Lawrence Edward Savell, "Right of Privacy-Appropriation of a Person's Name, Portrait, Or Picture for Advertising Or Trade Purposes without Prior Written Consent: History and Scope in New York," *Albany Law Review* 48, no. 1 (Fall 1983), 1. The New York Legislature responded by enacting the Nation's first statutory right to privacy (Law 1903, Ch. 132), now codified as sections 50 and 51 of the Civil Rights Law. Section 50 prohibits the use of a living person's name, portrait or picture for “advertising” or “trade” purposes without prior written consent (Civil Rights Law § 50). Section 50 provides criminal penalties and section 51 provides a private right of action for damages and injunctive relief.


Ibid., 217-218.


Prosser, *Privacy*, 386.


Ibid., 455-457.

Ibid., 458-471.
104 Ibid., 475.

105 Ibid., 478.


107 Ibid., 361.


109 Prosser, Privacy, 388.

110 Ibid., 389.

111 Ibid., 392.


113 The information technology field, consisting of digital computers, databases, storage, and retrieval systems is the basis for the case study found in Chapter Five, as the threat to privacy posed by information technology was the impetus for the Privacy Act of 1974.


115 See R. H. Clark, "Constitutional Sources of the Penumbral Right to Privacy," Villanova Law Review 19 (1974), 833. Clark carefully analyzes those aspects of the five amendments that the court relied upon to declare a composite right to privacy based upon “penumbras” and “emanations.”

116 Ibid., 833.


119 Ibid., 453.


123 See *Title III of the Omnibus Crime Control and Safe Streets Act of 1968* (as amended) at:

124 See *Freedom on Information Act of 1966* (as amended) at:

125 See the *Fair Credit Reporting Act* (as amended) at the FTC site:

126 See the *Family Educational Rights and Privacy Act of 1974* at:
Chapter Three

“Never doubt that a small group of thoughtful, committed citizens can change the world.
Indeed, it is the only thing that ever has.”
Margaret Mead

The Epistemic Community

The definition, characteristics, and criteria for identifying the existence or presence of an epistemic community are the subjects of this chapter. In this chapter, I trace the lineage of earlier “cognitive” or “expert” groups or communities whose contributions to knowledge and decision-making made them valuable to policy makers and legislators of the past. I then employ Peter Haas’ conceptualization of the epistemic community as my starting point, noting subsequent scholarship that identifies weaknesses or limitations in his epistemic community concept. Finally, I identify criteria by which I can operationalize the epistemic community concept and objectively identify the presence of an epistemic community in the subsequent United States and European Union Privacy Case Studies.

The term “epistemic community” is less than a half-century old, having been invented by Michel Foucault. Because the phrase “epistemic community” is relatively new, it is important to understand that the epistemic community has had a number of antecedents---and although not termed epistemic communities, they have often behaved in the manner, and with the characteristics attributed to, the epistemic community.
Elements of the epistemic community concept can be found in the idea of an *invisible college*, consisting of a group of networked scientists with common motivation, purpose, or common policy enterprise. The concept of the invisible college was first introduced in the mid-seventeenth century in London, and said by some to be the predecessor of the Royal Society. The idea of the invisible college reappeared in the 1970s in *Invisible Colleges: Diffusion of Knowledge in Scientific Communities*, and in 2008 in *The New Invisible College: Science for Development*. The literature of the past two decades has produced significant research either building on, or testing, the epistemic community organized in the form of invisible colleges. Ernst Haas, in *When Knowledge is Power* for example, describes epistemic communities that “take the form of “invisible colleges,” networks of the like-minded not employed in the same university, laboratory, or think tank.” These distributed, networked, like-minded scientists and scholars develop a common enterprise or purpose and influencing decision-makers and legislators through their knowledge expertise.

More than a century ago, one of the most influential books on government of the twentieth century drove home the idea that, “All politics and all government are the result of the activities of groups.” Arthur F. Bentley’s voluminous book, *The Process of Government: A Study of Social Pressures*, focused on the role of interest groups and the importance of ideas that motivated the group, as well as the conflict among groups within society and government, that results in government policy and law. For Bentley, the interaction and conflict of interest groups constituted politics. There was no “public opinion” because there was no “public”---there were only many different kinds of groups,
each of which had its own interests. To Bentley’s mind, the epistemic community, or knowledge community of experts, would be just one of many groups vying for position and influence in the political process. One might hope that the expert knowledge of the epistemic community provides them an edge in the negotiation for their desired political solution, but Bentley believed that all policies and legislation are the result of constantly competing interests and the groups that represent those interests.

Nearly half a century after the appearance of “The Process of Government,” Harvey Brooks described the important role that technical experts played in the increasingly complex machinery of government. The role of “experts” in government policy making has been a popular theme ever since the Second World War, when “experts” in many fields were credited with the technical breakthroughs that provided the Allies the edge to win the war. In the early 1960s, Harvey Brooks identified government reliance on “experts” to solve the increasingly complex and technical policy and operational problems that confronted government. Brooks described the trend toward technical, (epistemic community) “experts” taking a larger and larger role in government, saying:

In most of the western world the first instinct of statesmanship is to turn intransigent problems over to “experts” or to “study groups.” There appear to be an almost naïve faith that if big problems can be broken down sufficiently and be dealt with by experts and technicians, the big problems will tend to disappear or at least lose much of their urgency.

Brooks noted that: “Much of the history of social progress in the twentieth century can be described in terms of the transfer of wider and wider areas of public policy
from politics to expertise.” The trend toward depending upon the knowledge of experts was not just confined to the United States, Brooks said, but even more pronounced in Europe. “The trend towards the acceptance of expertise has been especially striking in Europe where both ideology and the apolitical professional bureaucracy have been stronger than in the United States.”

Origins of the Epistemic Community Concept

As previously noted, Michel Foucault is credited with inventing the term “epistemic community,” in his book *The Order of Things* in 1971. Foucault’s original use of the term is considered by some to be indistinguishable from “ideological communities.” In the past four decades, Foucault’s original term has been adopted, and its definition significantly expanded, by a multitude of scholars. For example, in *Knowledge Application: the Knowledge System in Society*, Holzner and Marx say that an epistemic community:

. . . thus designates those knowledge-oriented work communities in which cultural standards and social arrangements interpenetrate around a primary commitment to epistemic criteria in knowledge production and application. In these terms, science is not the only epistemic community. Any special way of knowing, whose development and elaboration requires the establishment of an autonomous social space, will tend toward the structure of an epistemic community. In fact, certain esoteric knowledge traditions associated with various groups of serious astrologers must be considered epistemic communities, just as much as the officially recognized and discipline-based modern professions.

Holzner and Marx go on to say that: “The establishment of a common frame of reference with shared epistemic criteria provides all members of such a community access to a consensually validated perspective for the construction of reality.” Thus, the
epistemic community serves to socialize new members into the knowledge, identity, and worldview of the community.

Ernst Haas, in *When Knowledge is Power*, builds upon Holzner and Marx’s definition of the epistemic community, saying that their definition does not go far enough. Ernst Haas says:

> For me, an epistemic community is composed of professionals (usually recruited from several disciplines) who share a commitment to a common causal model and a common set of political values. They are united by a belief in the truth of their model and by a commitment to translate this truth into public policy, in the conviction that human welfare will be enhanced as a result.  

In the late 1960s, Thomas Kuhn popularized the term *paradigm*, as he described the shared paradigms of scientists conducting “normal” science. In terms very close to those used by Peter Haas in describing the epistemic community, Kuhn described the shared paradigm of normal science in his book, *The Structure of Scientific Revolutions*. Peter Haas acknowledged this relationship when he said of his own definition of an epistemic community:

> It also somewhat resembles Kuhn’s broader sociological definition of a paradigm which is “an entire constellation of beliefs, values, techniques, and so on shared by members of a given community” and which governs “not a subject matter but a group of practitioners.”

Peter Haas popularized the most widely quoted definition of the epistemic community in the international relations community in the early 1990s. Haas assembled ten representative essays on the influence of epistemic communities in a special issue of *International Organization* in 1992, and published the essays as an edited collection the
same year.\textsuperscript{22} His survey of epistemic communities has made Peter Haas’ definition the most referenced and most often quoted in the epistemic community literature. Haas wrote that:

An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area. Although an epistemic community may consist of professionals from a variety of disciplines and backgrounds, they have (1) a shared set of normative and principled beliefs, which provide a value-based rationale for the social action of community members; (2) shared causal beliefs, which are derived from their analysis of practices leading or contributing to a central set of problems in their domain and which then serve as the basis for elucidating the multiple linkages between possible policy actions and desired outcomes; (3) shared notions of validity---that is, intersubjective, internally defined criteria for weighing and validating knowledge in the domain of their expertise; and (4) a common policy enterprise---that is, a set of common practices associated with a set of problems to which their professional competence is directed, presumably out of the conviction that human welfare will be enhanced as a consequence.\textsuperscript{23}

Over the past two decades numerous scholars have suggested that epistemic communities have played a major role in both national and international decision-making and policy formulation in a wide range of disciplines including public administration,\textsuperscript{24} criminology,\textsuperscript{25} business,\textsuperscript{26} and banking.\textsuperscript{27} Scholars employ the term epistemic community in order to explain the formation and influence of knowledge communities that influence decision-making and policy in corporate,\textsuperscript{28} public,\textsuperscript{29} and government organizations.\textsuperscript{30} Within the discipline of international relations, studies describing the role and importance of epistemic communities have been conducted in such areas as nuclear arms control;\textsuperscript{31} international food aid;\textsuperscript{32} the creation of international economic regimes;\textsuperscript{33} and numerous facets of the environment, to include protection of stratospheric
As the world becomes more technical and complex, the problems and issues to be addressed by government have become equally complex and technical. The fact that policy makers at all levels have welcomed knowledge experts, or an epistemic community, to assist with the process of identifying problems, identifying possible solutions, and then selecting the best decision is well documented. In the growing complexity of national, regional, and international problems, one has to only remember H.L. Mencken’s aphorism that: “There is always a well-known solution to every human problem--neat, plausible, and wrong,” to appreciate government’s need for expert counsel when making complex decisions that affect humans, the environment, or the planet. Because government decision makers and bureaucrats are not generally technically sophisticated, and are rarely faced with decisions within their limited field of competence, their need for expert, technical, or professional advice on complex issues would seem to be the normal state of affairs. Thus, one concludes that decision-makers have always sought the advice and recommendations of subject-matter-experts in complex areas in which change was contemplated.

**The Nature of the Epistemic Community**

Once the historical existence and activities of epistemic communities have been identified under numerous appellations, one of the first things that a researcher of epistemic communities must do is to parse the concept so as to be capable of operationalizing and objectively applying the concepts to the identification of epistemic
communities within the privacy domain or issue-area. Peter Haas has provided us with several key characteristics of an epistemic community in his seminal essay. There are five characteristics that Peter Haas lists that would appear central to identifying and defining an epistemic community. Presumably, each of these plays an integral part in the creation of, activities of, and identification of an epistemic community. In order to fully understand and operationalize the concept of the epistemic community, I believe that each of the five defining characteristics must be thoroughly investigated. For analysis purposes, I renumber them as:

1. A **network of professionals** with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area;
2. A **shared set of normative and principled beliefs**, which provide a value-based rationale for the social action of community members;
3. **Shared causal beliefs**, which are derived from their analysis of practices leading or contributing to a central set of problems in their domain and which then serve as the basis for elucidating the multiple linkages between possible policy actions and desired outcomes;
4. **Shared notions of validity**—that is, intersubjective, internally defined criteria for weighing and validating knowledge in the domain of their expertise; and,
5. A **common policy enterprise**—that is, a set of common practices associated with a set of problems to which their professional competence is directed, presumably out of the conviction that human welfare will be enhanced as a consequence.39

Examining each of these five characteristics of an epistemic community in isolation, I should first note that many authors who have worked from Peter Haas’ epistemic community definition have focused primarily on the last four characteristics of an epistemic community, to the exclusion of the first.40 Perhaps this is because Hass
numbered the last four, where the first was the topic sentence of his definition. Second, I should note that a careful reading finds that several of the key concepts and phrases of the definition are difficult to operationalize in a research program, because they impute subjective criteria described in terms of normative and principled beliefs, causal beliefs, and notions of validity that do not lend themselves to objective characterization and observation by an external observer, and perhaps not even by the epistemic community actors themselves.

**Limitations of the Epistemic Community Approach**

Some scholars who have employed the epistemic community approach have observed that Haas’ criteria are overly specific, subjective, and “. . . actually identifying these communities can . . . be a very difficult process.” Numerous scholars have identified limitations or weaknesses in Haas’ epistemic community approach. These limits or weaknesses must be understood in order to bound the concept and operationalize those objective characteristics of the approach that are observable.

On the issue of objectively operationalizing a research program, Claire Dunlop says of Haas’ epistemic community framework that:

Wright correctly highlights the basic methodological complexity of operationalising such a micro-level approach . . . It seems likely that the practical obstacles entailed in the approach, such as identifying, locating and gaining access to those believed to be members of any epistemic community (this is before any attempt can be made to discern their importance), may have frustrated some scholars’ attempts to use and test the thesis effectively, if at all.
Additional examples abound in the literature. For example, even while employing Haas’ epistemic community construct in the analysis of European Union processes, “Verdun (The role of the Delors Committee in the creation of EMU: an epistemic community?) criticizes Haas’ definition for being too rigid ever to apply to any given community of experts, since his conditions are simply extremely difficult to meet.”\textsuperscript{43}

Because Haas’ lead essay, \textit{Introduction: epistemic communities and international policy coordination}, is just that---an introduction that lays the basis for understanding and evaluating the nine exemplar essays that follow it---Haas does not offer detailed evidence or empirical testing in his essay. Rather, Haas makes general assertions that in many policy areas epistemic communities have framed issues for debate, and thus influenced outcomes that were consistent with the community preferences.\textsuperscript{44}

The size of Haas’ “network of professionals” is undefined. No minimum or maximum size, number, or extent of the network is offered, nor does Haas define any formal criteria for the construction or organization of the network.\textsuperscript{45} Thus, one infers that the size, extent, or composition of the network is not important to the enterprise or undertakings of the community. The limiting criteria are all laid upon those members who make up the network . . . the experts, technicians, or professionals who share a number of subjective qualities and understandings. They must possess “recognized expertise and competence in a particular domain.” But nothing is said about who specifically evaluates the expertise and competence of the members of the community. One is left to conclude that it is the decision-makers who will rely upon their counsel who
must ultimately be the arbitrators of the *expertise and competence* that the members of the epistemic community possess.

When Haas invokes “a shared set of normative and principled beliefs, which provide a value-based rationale for the social action of community members” it implies a common culture, education, training, and experience across a community that Haas says “. . . need not be made up of natural scientists or of professionals applying the same methodology that natural scientists do.”46 This reflects the diversity of the scientific, government, and social world from which members of the epistemic community are drawn. While some core beliefs, for example, in the importance of individual privacy, may be found to be held nearly universally, others, such as the priority in which the many dimensions of privacy should be protected or how specific individual privacy rights can be guarded or guaranteed, may be in conflict.

Haas’ discussion of “shared causal beliefs, which are derived from their analysis of practices leading or contributing to a central set of problems in their domain and which then serve as the basis for elucidating the multiple linkages between possible policy actions and desired outcomes”47 suggests a commonality of belief of causality—as well as a static scientific and social view of the world—based upon an implied common culture, education, training, and experience. As with any group that is called together to address a new issue or new problem, there are initially many perspectives of both the problem and possible alternative solutions. Haas does not discuss the complex processes by which disparate views are debated and compromised within the epistemic community in order to produce the final short-list of possible policy actions and probable outcomes.
These are the decision-making processes within the community that ultimately produce the common policy behind which the epistemic community can unite and agree on shared beliefs, causal beliefs, and shared notions of validity. No evidence, documentation, or suggestion of the process by which shared beliefs, causal beliefs, and shared notions of validity are agreed upon by the members of the epistemic community is offered. The community is assumed to adhere to a common faith in the applicability of particular forms of truth and knowledge to the solution of specific issues or problems without the internal contest of ideas, concepts, and alternatives.\(^{48}\)

Similarly, Haas’ attribute of “shared notions of validity---that is, intersubjective, internally defined criteria for weighing and validating knowledge in the domain of their expertise” relies on imputed and empirically untestable qualities of the community. No documentation, evidence, or process is offered by Haas by which shared notions of validity within an epistemic community can be positively observed or ascertained.\(^{49}\) Although the process of validating truth and knowledge claims within the domain of expertise may be intersubjective and based on internally defined criteria, the outcomes may vary.

When engaged in “a common policy enterprise---that is, a set of common practices associated with a set of problems to which their professional competence is directed, presumably out of the conviction that human welfare will be enhanced as a consequence,” the implication is that all community members agree upon the set of problems and the possible solutions. As epistemic communities become institutionalized
through the Internet, the range of policy enterprises that they address increases significantly.

Are these the only criteria that one must entertain when one identifies or defines an epistemic community? Are these five characteristics of an epistemic community in themselves the only necessary, and simultaneously sufficient, attributes needed to bound the totality of epistemic communities? Haas himself notes that, “The term ‘epistemic communities’ has been used in a variety of ways, most frequently to refer to scientific communities.” He then goes on to qualify his definition saying that, “Our notion of ‘epistemic community’ somewhat resembles Fleck’s notion of a ‘thought collective’---a sociological group with a common style of thinking. It also somewhat resembles Kuhn’s broader sociological definition of a paradigm, which is ‘an entire constellation of beliefs, values, techniques, and so on shared by members of a given community’ and which governs ‘not a subject matter but a group of practitioners.’”

The Influence of the Epistemic Community

The narratives and discussions of epistemic communities by Peter Haas, et al., are descriptive of successful instances of epistemic communities influencing regime formation and/or legislation regarding issues/topics important to the international community. But how does the epistemic community influence exert influence on policy makers and ultimately, legislation? Adler succinctly summarizes the five mechanisms identified by Adler and Haas by which influence is exerted:

First, by policy innovation they frame the issue, i.e. decide the nature of the issue, the policy objectives, and at what level (in which forum) the issue should be solved. These initial choices set the stage for defining
national interests. Second, *policy diffusion*, which refers to the mechanism with which members of epistemic communities communicate using transnational links to make their views known. The acceptance of their ideas by others across the globe, in turn, can be used to put pressure on national governments. Third, *policy selection* can take place. In this case, decision-makers seek support from a *selected* epistemic community which they know will support their policies. This approach enables the decision-makers to legitimize their policy choices by referring to the community of experts who approve of their policy choices. Fourth, *policy persistence*, the continuation of consensus of ideas, beliefs and goals over time among the members of the epistemic community, contributes to their credibility, and hence their authority, and thus it also determines how long an epistemic community remains influential. Finally, by *policy evolution as learning*. Epistemic communities can contribute decisively to the process of learning, which is important as the final understanding of a policy issue determines the policy outcome. (Italics in original)\textsuperscript{52}

This raises the question: Are there any examples of unsuccessful epistemic communities? When following this line of inquiry, the first thing one must do is define what constitutes “successful” or “unsuccessful” in the activities of an epistemic community. One can posit several epistemic community scenarios that might lead to an “unsuccessful” conclusion, for example: 1) An epistemic community might exist, but take no action (or be ignored) in informing decision makers . . . thus no “success” or “failure” might be attributed to its “action” or “inaction;” 2) An epistemic community may counsel decision makers, and decision makers may implement the advice, but intervening variables may subsequently change the intended outcome; and, 3) Several epistemic communities may exist, each with a competing view or paradigm in a given policy area, with the result that a modified, compromised, or completely different outcome might result when policy makers ultimately make their decisions. In this third
instance, it is possible that no one epistemic community could claim complete “success” in promoting its course of action.

Instances of all three of these less-than-successful epistemic community outcomes can be found in the literature. For example, in his essay, *Epistemic Communities and the Diffusion of Ideas: Central Bank Reform in the United Kingdom*, Michael King notes that, “Good ideas or an academic consensus on a new paradigm, however, are not enough. The present study discusses circumstances where the ideas of an epistemic community were not adopted by politicians, and highlights that the electoral benefits of adopting the reform must exceed the electoral cost for ideas to survive the political process.” Thus King concluded that the policy maker’s perception of electoral or career self-interest was the deciding factor in whether or not the counsel of a broad epistemic community of economists and monetary experts would be acted upon.

In their essay, *The Interest-Based Explanation of International Environmental Policy*, Sprinz and Vahtoranta recognize the important role played by epistemic communities, but then qualify the influence of such communities by noting that intervening variables such as perceived political, domestic, or national interests may override or mitigate the advice of the expert community and cause decision makers to opt for an alternate or modified course of action. While not denying the importance of knowledge and the influence of the epistemic community, Sprinz and Vahtoranta argue that policy outcomes are often based most heavily on political cost-benefit considerations, and say that: “. . . epistemic communities in ecologically vulnerable countries will exert stronger effects on governmental elites to seek international
regulation as opposed to their impact in less ecologically vulnerable countries.” They believe that while the role of knowledge-based experts is important in shaping a country’s environmental policy, immediate national interest is a more important intervening variable than the knowledge and influence of the epistemic community in policy maker environmental decision-making. Thus, after counsel of the environmental epistemic community, the course of action chosen, and the ultimate outcome, would be evaluated as unsuccessful epistemic community influence.

In his essay entitled *Discourse, Ideas, and Epistemic Communities in European Security and Defense Policy*, Jolyon Howorth provides an example of an unsuccessful epistemic community as he recounts the story of the discursive search for a European Security and Defense Policy (ESDP) in the decade following the disintegration of the Soviet Union and the end of the Cold War. Howorth describes how British, French, and German leaders, diplomats, and bureaucrats came together to create an epistemic community and put forth new ideas regarding a common EU paradigm for security and defense via speeches, proclamations, and memos. The ESDP participants became “. . . part of a new international epistemic community that was to take up the new paradigm and refine it.” After a decade of consultation and negotiation, the work of the ESDP epistemic community was brought to ruin by the events subsequent to 11 September 2001, when the British, the French, and the German governments each refocused their individual defense policies based on the new terrorist threat. Each nation subsequently chose a different response to the American military invasion of Afghanistan, and later Iraq.
Several scholars have observed the development of competing, or counter, epistemic communities within the same policy area. In his essay *South Africa, AIDS, and the Development of a Counter-Epistemic Community*, Youde develops the idea that two or more legitimate epistemic communities may evolve simultaneously around a given policy issue, each possessing the requisite network of professionals, credentials, recognized expertise, competence, and an authoritative claim to policy-relevant knowledge within a particular domain—-but each possessing different world views and thus espousing dramatically different courses of action. Youde admits that eventually the influence of one of the epistemic communities can be expected to become dominant with policymakers, but this does not mean that the second (or counter) epistemic community will wither away and cease to exist as long as the policy issue remains active which initially gave rise to the creation of the epistemic community.

**The Life-Cycle Of Epistemic Communities**

Most epistemic community literature of the 20th century treats the formation and activities of the epistemic community as a relative snapshot in time, and the numerous examples cited by Peter Haas, are no exception. The community is formed in response to a specific issue or problem; it accomplishes a specific purpose, and it dissolves. That is, after its “success” of positively influencing treaties, agreements, or regimes, the individuals who comprised the “epistemic community” all returned to their respective vocations and the unique epistemic community that was so successful in influencing national and international events essentially ceased to exist. Although the members of the community were still active in their vocational specialty and available for
consultation, there appears to have been no continuity of the epistemic community through time, because once the treaty, agreement, or regime was concluded or created, the epistemic community melted away. Realizing that the role of the epistemic community is conditioned upon the perceived need on the part of its members to provide information, courses of action, and probable outcomes to decision makers operating under uncertainty and encountering complex problems surrounding seemingly time-critical policy issues, one can certainly see why this transience of the epistemic community would historically be the norm. Once the work of the epistemic community is completed with the resolution of the policy issue that gave it *raison d’être*, the epistemic community dissolved.

In the world of the twentieth century, the members of the epistemic community were often separated by distance and time from one another. When major international or domestic policy issues arose, members of the community were sometimes alerted by the news media, but more often communicated and coalesced using the technology of the time: post mail, telephone, facsimile, and physical transport by automobile, train, ship, or airplane. Professional conferences have always been an excellent venue for meeting, learning, and sharing of information and ideas, but they also require considerable time and resources to attend. Thus the convocation of epistemic community members took considerable time and effort to execute. The effort and resources required to maintain contact almost ensured that minor policy issues would rarely evoke the coalescence of the epistemic community and a coordinated community response. In this first decade of the
21st century, however, many of these constraints to the continuous networking of the epistemic community have been overcome.

**Institutionalizing the Epistemic Community**

The advent of the Internet has produced a global infrastructure that facilitates the permanency and continuity of epistemic communities. In many ways, the Internet has institutionalized many epistemic communities by allowing for continuity in epistemic community communication, activities, and relationships that extend beyond the issue or problem that gave rise to the epistemic community in the first place. Internet presence is essentially global, and 24 hours a day/7 days a week. The ability to permanently upload or “post” digital data and information, including e-mail, digital books, issue studies, opinion pieces, photos, graphics, digital video and electronic mailing lists gives the epistemic community a permanent near-real-time global network---as well as a venue for informing, educating, and proselytizing not only members, but also the global public and decision-makers. As will be seen for the privacy epistemic community, a computer search for any privacy issue will elicit dozens of permanent websites that support and link members and topics across the privacy epistemic community.

A constellation of privacy organizations now forms the global privacy epistemic community. Each organization offers a variety of information, education, and guidance regarding issues of privacy. Each organization has a specialty or primary focus within the broad field of privacy, but many have overlapping secondary or peripheral privacy areas of interest. Although in most cases the alignment of these privacy organizations on major privacy policy issues is similar, the number and breadth of privacy issues
represented occasionally presents the opportunity for competing views on privacy policy issues. When such competing views, advice, or courses of action are offered to decision makers by the privacy epistemic community, it requires: 1) competition of ideas within the privacy epistemic community to agree on a common position or course of action, or 2) the decision maker(s) to choose (and follow) what they feel to be their best counsel.

Within just the past decade the Internet has created an omnipresent global network around which an epistemic community can grow and evolve as a permanent presence. Thus, the privacy epistemic community has become a permanent fixture through their Internet web sites, allowing privacy epistemic community members to meet asynchronously around the clock and contribute to a constant dialogue in response to issues and problems of even marginal saliency. They are capable of expressing well-researched positions on even minor privacy issues, influencing all privacy legislation, and are often important voices in advising decision makers and legislators on a multitude of privacy issues over time.

Self-Aware Epistemic Community?

Is an epistemic community an epistemic community if the members of the informal epistemic community network do not know, or understand, the concept of an epistemic community? As demonstrated by the nine essays in the Peter Haas’ collection, and the dozens of essays that have subsequently used the phrase “epistemic community” in the last decade of the twentieth century to characterize a knowledge group meeting the criteria established by Haas, most members had probably not intuitively self-identified as being an epistemic community. But as the phrase and the concept of an epistemic
community have become more well known in the past decade, it is probable that members more readily identify themselves as being part of an epistemic community.

With the permanence of epistemic communities that has been created by the advent of the Internet, it is likely that many members of epistemic communities have become more self-aware today. Sociologist Howard Becker posited that for one to distinguish any specific group from the others, one must attempt to understand how the members of the group look at themselves, as well as how those on the outside see members of the group. Becker would thus suggest that to truly be an epistemic community, the epistemic community must be recognized by both the “ins” and the “outs” of the community. Ultimately a group is recognized as a unique and separate entity because both the members of the group (the epistemic community “ins”) and those outside the group (the “outs”) recognize the distinct and unique nature of the group. This is not to say that the members of the epistemic community define themselves and their belief paradigm in terms of the five characteristics delineated by Haas. No more than the Anglo-American economists and policy specialists described by G. John Ikenberry in Haas’ collection of epistemic community essays as creating the post-World War II Bretton Woods agreement would have described themselves as constituting an epistemic community, or thought in terms of the five community characteristics described by Haas.

The Global Privacy Epistemic Community

Based upon Internet presence, studies, white papers, and public announcements of support for privacy issues and legislation it appears that there has been a well-developed
global privacy epistemic community represented by a large number of privacy organizations for several decades. Evidence of the privacy epistemic community can be found in periodic comment, advocacy, and support by both individual privacy organizations as well as privacy issue-centered coalitions of organizations. As the immediate privacy issues change, from health privacy, to tracking Internet privacy, to digital surveillance in public areas for example, the composition of the active privacy epistemic community coalition changes accordingly. There are significant differences in the privacy concerns (and thus the composition and character of the epistemic communities formed) among the sub-areas within the privacy issue-area. That is, some organizations focus on individual privacy as a derived constitutional right, while other privacy organizations focus on discreet, and often very technical issues such as data privacy, surveillance/photography privacy, geo-location privacy, body DNA privacy, etc. That raises the natural question of whether these differences in privacy focus or emphasis by privacy organizations constitute a different epistemic community, or are these merely variations on a common theme of privacy? When major privacy issues arise that cut across many technical areas, such as government wire-tapping, the many privacy organizations come together to offer their expertise and technical knowledge to legislators and decision makers.

**Operationalizing the Identification of the Epistemic Community**

The discussion of limitations and weaknesses of the epistemic community approach discussed earlier in this chapter highlights the difficulty of applying subjective, soft, or “fuzzy” criteria based on *shared normative and principled beliefs, shared causal*
beliefs, or shared notions of validity. I will therefore meet these inherent limitations and weaknesses in the Haas epistemic community approach by identifying and employing the following empirical, readily observed, criteria by which the epistemic community can be characterized: 1) Recognized professional/technical expertise or “standing” in privacy issues; 2) Privacy publications; 3) National and international organizations with a privacy component; 4) Privacy websites on the internet; 5) Periodic privacy conferences; and, 6) Participation in government hearings, testimony, and other legislative meetings.

Each of these six criteria requires a more detailed discussion in order to operationalize the characteristic to the point of being able to identify the epistemic community. The first two criteria (1 and 2) are applicable to members of the epistemic community, the next three criteria (3, 4, and 5) are integral to the epistemic “network,” that facilitates the loose organization and continued interaction of the community which would promote Haas’ four implicit and inter-subjective characteristics of (1) shared normative and principled beliefs; (2) shared causal beliefs; (3) shared notions of validity; and (4) common policy enterprise. Finally, the sixth criterion identifies the ability of the epistemic community members to influence policy decision-making and legislation.

Identifying the Privacy Epistemic Community

In the following two chapters, I will apply the following six objective criteria in order to identify the existence of, the role of, and the activities of, the privacy epistemic community in influencing privacy legislation in the United States and the European Union case studies:
1) **Professional/technical expertise and competence in privacy issues** that are recognized by members of the privacy epistemic community and by those outside the community. The professional and technical expertise of members of the privacy epistemic community will be ascertained and recognized by other community members and those external to the community based on individual activities and/or membership in the following five areas. Most importantly, the professional and technical expertise of privacy epistemic community members must be recognized by policy decision-makers and legislators who will entertain their expert opinion and enact legislation.

2) **Privacy publications** by members of the privacy epistemic community that address, explicate, or amplify privacy concerns, issues, or problems for the epistemic community, legislators, and the public establish, maintain, extend the authors’ “expertise and competence” and “authoritative claim to policy-relevant knowledge within the domain or issue area.”66 Publications, which may include professional or technical authoritative “blogs” in today’s virtual world of the Internet, extend the bounds of knowledge and promote common beliefs and notions of validity.

Beginning in the late 1950s, individuals who became leaders of the epistemic community authored essays, articles, and books describing threats to privacy. These publications established the professional/technical expertise of the authors in the realm of privacy and educated other members of the privacy epistemic community in specific privacy issues, problems, and possible courses of action.

3) **National and international organizations** with a privacy component provide a network framework for members of the privacy epistemic community to network,
exchange knowledge, study issues and options in their professional/technical area of expertise, and educate (some might say proselytize) new members to the epistemic community.

The two primary organizations that have facilitated networking across the privacy epistemic community were the Council of Europe and the Organization for Economic Cooperation and Development (OECD).

4) Privacy websites on the Internet provide an ever-present virtual domain for members of the privacy epistemic community to network, exchange knowledge and opinions, educate new members of the epistemic community, and coordinate their “common policy enterprise . . . (that) set of common practices associated with a set of problems to which their professional competence is directed . . . .”

5) Periodic privacy conferences and convocations provide important opportunities to physically network and maintain epistemic community contact, knowledge, and coordination as described in paragraphs three and four immediately above. The importance of conferences is emphasized by Cogburn, who notes that conferences serve different roles, and some international conferences are more important than others, saying of conferences that:

Their influence on the epistemic community and components of an emergent regime varies significantly. Some international conferences plan an extremely important role in debating and articulating the principles, values, and norms of a particular regime, but may not have any rule-making, decision-making, or enforcement capabilities. Other conferences may be more influential in decision-making and enforcement, while having less influence on the generation of new principles, values and norms for the issue area. High-level conferences, at which formal conference ‘agreements’ containing
principles and values for the particular issue area are tabled, debated and adopted, are certainly more important in regime formation than others. These conference agreements often serve as reference point for policy-makers and other stakeholders who use these documents to rally support for strategic plans and resource allocation in pursuit of the conference objectives as codified in agreements.68

6) Participation in government hearings, testimony, and other legislative meetings is necessary for the members of the epistemic community to share their epistemic community knowledge with decision-makers and policy-makers, influence state interests and thus influence decisions and national/international legislation.69

Most of the privacy epistemic community members identified as representatives have authored privacy publications have been participants in government hearings, testimony, and congressional legislative studies and have directly or indirectly played active roles in influencing decision-makers and privacy legislation.

Following the two case studies recounting the role of the privacy epistemic community in influencing privacy legislation in the United States (Chapter Four) and the European Union (Chapter Five), the impact, effectiveness, and limitations of the privacy epistemic community will be analyzed in Chapter Six.

Chapter Summary

While the concept of the epistemic community is really only about four decades old, the characteristics of the epistemic community can be recognized in networks of “professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area”70 from much earlier periods in history. Over the past two decades, the epistemic community
scholarship of Peter Haas has dominated the literature and has become the benchmark for its study. However, some scholars have identified limitations or weaknesses in Haas’ constructivist description of beliefs, values, validity, and “intersubjective, internally defined criteria” on the part of epistemic community members who have made it nearly impossible to operationalize Haas’ epistemic community definitions and create a viable research program. I agree with those scholars who suggest that there is no reliable method of measuring or gauging the beliefs, values, validity, or intersubjective, internally defined criteria of members of an epistemic community and have therefore identified what I consider to be six objective criteria for identifying the privacy epistemic community.

In Chapter Four, I present the United States Case Study in which I trace the activities of a nascent privacy epistemic community of computer scientists, academics, lawyers, and legislators from the late 1950s to the creation an informal privacy network that wielded influence through publications, conferences, classes, studies, reports, and testimony at congressional committee hearings, that led finally to the passage of the Privacy Act of 1974.
Chapter Three Notes

1 See Margaret Mead quotations at: http://www.bookbrowse.com/quotes/detail/index.cfm?quote_number=88

2 Foucault, The Order of Things: An Archaeology of the Human Sciences, See Chapter 10, the Human Sciences, 344-387.

3 See: http://www-history.mcs.st-and.ac.uk/Societies/RS.html regarding the use of the phrase invisible college in London circa 1645.


6 Ernst B. Haas, When Knowledge is Power: Three Models of Change in International Organizations (Berkeley, CA: University of California Press, 1990), 42. Haas identifies the invisible college as a form of epistemic community and references the work of Diana Crane on the Invisible College for additional epistemic community examples.

7 Most of the invisible college literature of the past several decades focuses on the synergistic development of scientific research, technology, and innovation and the desire of the invisible college members to influence decision-makers or policy makers to provide more money for basic science and research and development.


12 Ibid., 72.
13 Ibid.

14 Ibid.

15 Foucault, The Order of Things: An Archaeology of the Human Sciences, 387.

16 Haas, When Knowledge is Power: Three Models of Change in International Organizations, 221, ff 21.


18 Ibid.

19 Haas, When Knowledge is Power: Three Models of Change in International Organizations, 41.


communities to explain international regulatory communities, suggesting that epistemic communities need not be based in “science,” and can be adversarial in reaching the common viewpoint described by Haas as being one of their hallmarks. Braithwaite then goes on to describe the historical origin of business epistemic communities in the guilds and professions of the Middle Ages.


28 For discussion of the epistemic community approach in the corporate context, see: Lars Hakanson, "Epistemic Communities and Cluster Dynamics: On the Role of Knowledge in Industrial Districts," Industry & Innovation 12, no. 4 (December, 2005), 433; Kasper Edwards, "Epistemic Communities, Situated Learning and Open Source Software Development" (Trodheim, Denmark, Epistemic Cultures and Interdisciplinary Practice Workshop, June 11-12, 2001, 2003); Patrick Cohendet, Frederic Creplet, and Olivier Dupouët, "Communities of Practice and Epistemic Communities: A Renewed Approach of Organisational Learning within the Firm" Workshop on Economics and Heterogeneous Interacting Agents, 2001); F. Creplet et al., "Consultants and Experts in Management Consulting Firms," Research Policy 30, no. 9 (2001), 1517; and Braithwaite and Drahos, Global Business Regulation, 704.


30 Discussion of the epistemic community approach in the government can be found in: Patrik Marier, "Empowering Epistemic Communities: Specialised Politicians, Policy Experts and Policy Reform," West European Politics 31, no. 3 (May, 2008), 513; Silke


37 Brooks, *Scientific Concepts and Cultural Change*, 66-83. As early as 1965, Brooks could identify the increasing complexity of government decision making, and the
growing trend toward dependence upon experts to inform policy makers on options, choices, and consequences.


42 Claire Dunlop, "Epistemic Communities: A Reply to Toke," *Politics* 20, no. 3 (2000), 141.


44 Ibid.

45 Peter M. Haas, ed. *Knowledge, Power, and International Policy Coordination*, ed. Peter M. Haas (Columbia, South Carolina: University of South Carolina Press, 1992), 390. Neither Peter Haas, nor the authors of the accompanying eight empirical exemplar essays wrote of the size, extent, or composition necessary for a successful epistemic community.

46 Ibid.

47 Ibid.

48 Ibid.
49 Ibid.


51 Ibid.


56 Ibid.


58 Ibid., 4.

59 Haas, Knowledge, Power, and International Policy Coordination, 390.

60 Ronald J. Deibert, "International Plug'n Play? Citizen Activism, the Internet, and Global Public Policy," International Studies Perspectives 1, no. 3 (2000), 261-67. Diebert analyzes the role of the Internet in the context of coordinated global “community” action and concludes that the World-Wide Web provides a global presence and international
reach that no previous communications technology possessed. Thus, the Internet supports global education, communications, and cooperation on a level never before seen.

61 Ibid.


64 Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy (Chapel Hill, NC: University of North Carolina Press, 1995), 310. Although Regan does not employ the phrase epistemic community she devotes 21 pages (191-211) to describing the evolution of the privacy policy community from the late 1960s to the early 1990s, focusing on key individuals and organizations that emerged to champion the issues of privacy.

65 Haas, Introduction: Epistemic Communities and International Policy Coordination, 3.

66 Ibid.

67 Ibid.


69 See Privacy Online: OECD Guidance on Policy and Practice, 4-5, at: http://titania.sourceoecd.org/v1=528517/cl=44/nw=1/rpsv/cw/vhosts/oecdthemes/99980134/v2003n13/contp1-1.htm (Last accessed 07 September 2010).

70 Ibid., 3.

71 Ibid.
See Dave Toke, "Epistemic Communities and Environmental Groups," *Politics* 19, no. 2 (1999), 97; Dunlop, *Epistemic Communities: A Reply to Toke*, 137-144; and Wright, *Knowledge and Expertise in European Conventional Arms Control Negotiations: An Epistemic Community?*, 1-16.
Chapter Four

The Privacy Epistemic Community and the United States Privacy Act of 1974: A Case Study

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and "bugging" run rampant, without effective judicial or legislative control.¹

Justice William O. Douglas,
Osborn v. United States (1966)

Introduction

As recounted in Chapter Two, by the mid-1960s the advances in automated data processing technology had made several communities aware of the threats posed by computers to the privacy of individuals. Although privacy as a conceptual “right” had been introduced in 1890 by Brandeis and Warren, it had most frequently been invoked in the following half century in rather isolated cases addressing specific issues which incrementally expanded the purview of the Fourth Amendment such as Weeks v. United States,² regarding illegally seized evidence, and Olmstead v. United States,³ addressing wiretapping. In Griswold v. Connecticut (1965),⁴ the Court first identified individual privacy a constitutional right that extended to the right of married couples to use birth control. The general right of individual privacy regarding information collected, processed, and stored by the government had not been addressed, because the nascent threat of government computer databanks had not been openly discussed and the public had not become conscious of the issue.
Those on the forefront of awareness regarding the threats that advancing technology posed to the privacy of individuals were the early data processing engineers and operators who set up and operated the large mainframe computers. Engineers and operators were often scientists and mathematicians who designed and installed the hardware, uploaded unique software they wrote—and then maintained hardware, firmware, and software, and operated processing capability for government agencies or large industry. In the 1960s there were no computer degrees that trained one to build, operate, and maintain a computer. The early, highly skilled cadre of data processing specialists usually held advanced degrees in mathematics, engineering, or the physical sciences—it was only later that they could rightly claim the moniker of data-processing scientist and subsequently, computer scientist.  

**Genesis of the Privacy Epistemic Community**

**The Path From Security to Privacy**

It was only as an after-thought to the operation of the data processing “computer” for classified government projects and business-sensitive industrial projects that many of these early computer scientists became aware of problems of security—and eventually privacy—in the context of computer operations. Thus it was that the first discussions regarding the social and legal dimensions of computer data processing revolved around issues of physical security, access, and control of the computer, its input, and its output. This would appear to be natural because the relatively small number of mainframe computers of post-World War II were employed by the federal government, the department of defense, and defense-related industry. Early security-focused technical
papers generally explored means and methods of securing and safeguarding critical data from intrusion and theft. The primary concern was theft of military, government, and industrial secrets. Only in the late 1950s and early 1960s did the issue of privacy begin to appear in the literature of computer journals, conferences, and symposia.⁶

**Technical Conferences and the Nascent Privacy Epistemic Community**

Computer professional organizations became a primary catalyst in the formation of the early privacy epistemic community in the United States. Beginning with the formation of the first computing society, the Association for Computing Machinery (ACM) in 1947, numerous associate and spin-off computer-centric societies were established over the next two decades to network, explore, and institutionalize the new technical computer field. Special Interest Groups, or SIGs, were established within the ACM to focus on specific specialties and interests within the computer field. Two of these SIGs appear to have been particularly important in generating security and privacy-related discussion and papers in the frequent conferences hosted by the ACM. The ACM Special Interest Group on Computers and Society (SIGCAS), and the ACM Special Interest Group on Security, Audit, and Control (SIGSAC) both acted as fertile ground for the gestation of computer security, and later, computer privacy concepts and discussions, and the formation of the privacy epistemic community.⁷

Other technology-focused organizations such as the Institute of Radio Engineers (IRE) and the American Institute of Electrical Engineers (AIEE) existed side-by-side with the ACM and participated collectively in annual regional and seasonal joint conferences. The ACM, IRE, and AIEE jointly sponsored technical conferences such as
the Eastern Joint Computer Conference (EJCC), Western Joint Computer Conference (WJCC), the Spring Joint Computer Conference (SJCC), and the Fall Joint Computer Conference (FJCC). The proceedings of these conferences indicate that the early years were dominated by highly technical computer sessions, however in the mid-1960s the issues of information security and privacy in computing databases began to emerge. These frequent conferences created a natural environment for like-minded computer professionals to gather in special interest groups, exchange information and ideas, and identify problems or issues to be resolved. The SIGCAS and the SIGSAC became special interest groups that promoted the growing issues of security and privacy in their conference sessions.

In 1961, the ACM-IRE-AIEE triumvirate merged their organizations with eight others to form the American Federation of Information Processing Societies (AFIPS). The AFIPS was the single umbrella organization that represented the entire U.S. computer field, “... and computer field was the right phrase for the time, because it had not yet broadened to the information-oriented one that we know today.” The AFIPS continued to sponsor the same several annual computer conferences from 1961 through 1984, when AFIPS and its component organizations IRE and AIEE coalesced to become the Institute of Electrical and Electronic Engineers (IEEE). Under the IEEE the annual conferences continued, and again featured sessions and special interest groups (SIGs) that focused on security and privacy issues, continuing the growth, networking, and reinforcement of the privacy epistemic community.
Dr. Willis H. Ware and the Rand Corporation

A central figure in the early privacy epistemic community was Dr. Willis H. Ware, who joined the RAND Corporation in 1952 after working with John von Neuman developing early vacuum tube computer prototypes at the Princeton Institute for Advanced Studies from 1946-1951. In the following decades Willis Ware became a subject-matter-expert in the computer security and privacy epistemic community. The RAND Corporation was founded in 1946 to support the United States Army Air Corps and became an independent, nonprofit organization, in 1948 with the mission: “To further and promote scientific, educational, and charitable purposes, all for the public welfare and security of the United States of America.” Because the RAND Corporation originated within the military, was chartered as a nonprofit, and focused on scientific pursuits for public welfare, it became an early nexus for computing excellence within the defense department, the federal government, and within the defense-related industries. Many computer scientists, including Willis Ware, worked to develop improved automated data processing capabilities for the Department of Defense and the Federal Government, where the largest concentration of, and users of, computers in the 1950s and 1960s were found. These technical computer pioneers were the first to confront the issue of security of data and information—and the derived issue of privacy—in regard to computer databanks. Ware became the chair of the RAND Corporation’s computer Science Department and in 1967 led a Defense Science Board task force that investigated computer security for the first time. Ware’s involvement in the security-privacy epistemic community can be measured by the fact that of the 77 studies and reports listed
by the RAND Corporation as being authored by Willis Ware between 1953 and 2008, 33 contain the words security or privacy in their title, and most address both security and privacy.\textsuperscript{16}

Ware was active in the promotion, development, and networking of computer professionals as well as non-computer scientists who had interests in security or privacy. He frequently took visible leadership roles in the regional joint conferences conducted by the Association for Computing Machinery, the Institute of Radio Engineers, and the American Institute of Electrical Engineers. In 1958, Ware was the Conference Chairman for the Western Joint Computer Conference (WJCC).\textsuperscript{17} Subsequently, he was a founder member, and first president, of the American Federation of Information Processing Societies (AFIPS) in 1961.\textsuperscript{18} In 1961 he was also the Conference Chairman of the Eastern Joint Computer Conference.\textsuperscript{19} The visibility and reputation that Ware achieved in the late 1960s and early 1970s, both as an active leader in computer professional organizations and as the security and privacy subject-matter-expert at the RAND Corporation, made him a natural choice to chair the Secretary’s Advisory Committee on Automated Personal Data Systems in the Department of Health, Education, and Welfare (HEW) in January 1973.\textsuperscript{20}

**Privacy Awareness in the United States**

**The National Data Bank and Congressional Privacy Hearings**

In the mid 1960s, at the same time that Willis Ware was authoring several of his first papers on computer security and privacy at the RAND Corporation,\textsuperscript{21} other members of the nascent privacy epistemic community were responding to the Social Science
Research Council’s proposed creation of a National Data Center. The National Data Center proposal “advocated a centralization of federal statistical programs based on new computer techniques of data storage and retrieval.” The intent of the proposal was to create a centralized national database that would facilitate social and economic statistical research and lead to better understanding of national issues. Ultimately this statistical research capability would lead to greater knowledge and understanding, and thus better decisions by leaders and lawmakers. Studies were conducted for the Bureau of the Budget to evaluate and define the proposal. The Social Science Research Council Committee on the Preservation and Use of Economic Data began research in 1959 and delivered its report to the bureau of the Budget in 1965. The “Ruggles Report” strongly recommended the creation of the National Data Center and described the many benefits that would accrue to government departments and agencies as a result of such a central government databank. The Ruggles Report and its recommendations were subsequently evaluated, critiqued, and refined in several additional studies and for a time a National Data Center appeared to be on the path to realization.

In the late 1960s and early 1970s, when it was proposed that a National Data Center would collect all government data for the use of statisticians and social researchers, the American public still had a rather ambivalent relationship with the threat of computers and their personal privacy. In 1971, the AFIPS and Time Magazine conducted a national survey inquiring about public attitudes toward computers. Nearly 40% of the respondents felt that the computer posed a real threat to privacy. Yet at the same time 85% of the respondents felt that their lives had been made better by inventions
and technology in the previous 25 years.\textsuperscript{25} Thus, it was not the public that motivated action in response to the issue of a National Data Center, but congressmen, academics, and lawyers who recognized the emerging issues and were willing to take action.

Elevation of the proposal for a National Data Center for evaluation and analysis at the department and agency level triggered intense interest in privacy issues by Congress. That interest led to extended hearings and debate by numerous congressional committees and subcommittees over the following several years.\textsuperscript{26} These congressional hearings on computer, databanks, and privacy issues tapped the expertise of many individuals who subsequently became identified as core members of the privacy epistemic community. From 1965 when computer, databank, and privacy hearings began until 1974, when the Privacy Act was passed into law, the many hearings, panels and reports generated provided opportunity for the development of a well-informed and well-networked privacy epistemic community.

\textbf{Congressional Hearings and the Privacy Epistemic Community}

The Senate Subcommittee on Administrative Practice and Procedure, chaired by Senator Edward Long of Missouri, conducted hearings on \textit{Invasions of Privacy} from 1965-1966.\textsuperscript{27} Arthur R. Miller, a lawyer and professor at the University of Michigan Law School, was asked to testify at the \textit{Invasions of Privacy} hearings about the effects computers may have on individual privacy. In the preface to his very influential 1971 book \textit{The Assault on Privacy: Computer, Data Banks and Dossiers}, Miller later wrote: “Since that first appearance before a congressional subcommittee I have slowly been devoured by the issue (of privacy), although I must confess that because of the inherent
fascination of problems of interrelating law and technology I have done little to avoid this detour from my more traditional research activities.”

Miller went on to become a key member of the privacy epistemic community, authoring one of the most often cited and influential books on privacy, testifying numerous times at congressional hearings, and serving on the Secretary’s Advisory Committee on Automated Personal Data Systems which authored the report that most privacy scholars credit with having the most influence in the creation of the U.S. Privacy Act of 1974.

Once congressional interest in privacy-related issues was piqued, the number of hearings seemed to explode, with more than 30 privacy-related congressional hearings between 1967 and 1974. For example, a Senate Subcommittee on Constitutional rights held hearings on Psychological Tests and Constitutional Rights in the summer of 1965, while a House Subcommittee chaired by Representative Cornelius Gallagher, began hearings under the title of Special Inquiry on Invasion of Privacy that ran from the summer of 1965 through the spring of 1966. A Senate Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, conducted hearings in the spring of 1971 on the subject of Federal Data Banks, Computers, and the Bill of Rights.

When describing the many individuals who were drawn to the privacy epistemic community by the many hearings, studies, and meetings of the late 1960s and early 1970s, Priscilla Regan notes that:

Within the privacy community, personal relationships are critical; the policy network is cemented by interpersonal relationships rather than by institutional links. Congressional hearings, OTA studies, executive agency committees, and privately funded workshops and conferences provide important opportunities of the
privacy community to meet, discuss ideas and policy proposals, and attract new members.31

Each of these hearings involved congressional legislators, congressional staff, academic researchers, interest group members, journalists, and the public to delving into the complex morass of technological, constitutional, and legal issues that surrounds the evolving right of privacy in the United States. As a result of many months of meetings involving privacy witnesses and privacy research over the almost nine years of hearings by various committees from 1965 to 1974, a large number of hearing participants were educated, motivated, and sensitized to the issues surrounding the interplay of computer technology, databanks, and privacy. Many of these hearing participants went on to become active members in the privacy epistemic community and have continued their active association with evolving privacy-related issues. Examples of this include privacy epistemic notables such as Alan Westin, a lawyer and Professor of Law at Columbia University, who participated in privacy hearings while completing his book *Privacy and Freedom*,32 as well as Arthur Miller, mentioned earlier, who participated in privacy hearings and went on to author the book *The Assault on Privacy*. Hope Eastman, acting director of the American Civil Liberties Union (ACLU) office in Washington D.C.; John Shattuck, who had litigated in areas of privacy, government secrecy, and political surveillance in 1971-1976 and was legislative director for the ACLU from 1980-1984; Lewis Branscomb, IBM vice-
president, author, and technologist; and Willis Ware, RAND Corporation Chief Computer Scientist, chair of the HEW Secretary’s Advisory Committee on Automated Data Systems, participated in privacy hearings and went on to become active privacy advocates and long-time privacy epistemic members. Robert Gellman was an attorney-advisor on the House Information, Justice, Transportation, and Agricultural Subcommittee of the Committee on Government Operations in the 1970s and participated in numerous congressional hearings during which he became an information privacy expert and advocate. He has become one of the most prolific authors of the privacy epistemic community and has become a privacy and information policy consultant.\textsuperscript{33}

Numerous academics participated in the privacy hearings of the 1960s and 1970s and became key leaders in the privacy epistemic community. “A number of academics who wrote about privacy in the 1960s were instrumental in getting privacy and technology issues on the public agenda and then in testifying and crafting policy alternatives (became) privacy experts.”\textsuperscript{34} While Westin and Miller were two of the earliest, and perhaps best known, academic participants in congressional privacy hearings, committees, and studies who went on in the following decades to advocate for privacy issues and legislation as part of the privacy epistemic community, there have been many other notable privacy advocates. James Rule, a sociologist specializing in privacy, authored numerous books on privacy issues, including \textit{Private Lives & Public Surveillance: Social}
Contract in the Computer Age, \textsuperscript{35} The Politics of Privacy, \textsuperscript{36} and Privacy in Peril: How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience, \textsuperscript{37} and has been active as a distinguished Affiliated Scholar at the Center for the Study of Law and Society, UC Berkley. \textsuperscript{38} Marc Rotenberg, who was an intern with the Privacy and Technology Project at the ACLU under Alan Westin, later went on to lead the Computer Professionals for Social Responsibility (CPSR), now specializes in Information Privacy Law as a law professor at Georgetown University Law Center, serves as director of the Electronic Privacy Information Center (EPIC), has authored and coauthored numerous books on privacy, and has served on many national and international panels and committees. \textsuperscript{39} David Flaherty, who studied under Alan Westin and was a professor at the University of Western Ontario, has written several books on privacy including Protecting Privacy in Surveillance Societies. \textsuperscript{40} “Flaherty became an active member of the privacy (epistemic) community in this country (US) as well as internationally and serves as the information and privacy commissioner in the province of British Columbia, Canada.” \textsuperscript{41} George Trubow, who represented the American Bar Association (ABA) at many hearings and meetings, became the General Counsel to the Committee on the Right to Privacy, Executive Office of the President, went on to become the Director of the Center for Information Technology and Privacy Law at John Marshall Law School and has authored numerous books and journal articles on issues of privacy,
information security and government privacy policy.\textsuperscript{42} That these many privacy epistemic community members were important in influencing the eventual passage of privacy legislation is without doubt. Priscilla Regan notes that:

In the case of information privacy, especially government collection and use of personal information, privacy advocates were the core of the advocacy coalition, working almost alone for passage of legislation and monitoring implementation legislation. No other group or interest aligned itself directly with the information privacy community.\textsuperscript{43}

Congressional privacy hearings generated considerable media interest, and resulted in an ongoing interest in the privacy issues that continues to the present. For example, after following privacy hearings, \textit{New York Times} reporter David Burnham became part of the privacy epistemic community by following privacy issues and events as his journalistic specialty and authoring \textit{The Rise of the Computer State}.\textsuperscript{44} Motivated by the important issues revealed in the privacy hearings, Robert Ellis Smith founded \textit{Privacy Journal} in 1974 as both an educational and networking medium for the privacy epistemic community and also as an educational tool for academics, lawyers, and the general public who wanted to know more about the issues surrounding privacy.\textsuperscript{45} In 1981 Evan Hendricks began publishing \textit{Privacy Times},\textsuperscript{46} which “provided sustained coverage of privacy issues and facilitated the maintenance and growth of the privacy community.”\textsuperscript{47}
Databanks in a Free Society Project

In 1968, the Russell Sage Foundation, a New York based social science research organization, funded the Project on Computer Databanks for the National Academy of Sciences Computer Science and Engineering Board. Dr. Alan Westin, who had participated in congressional hearings and had just published his book Freedom and Privacy, directed the study which was designed to examine the end-to-end government and private use of computers for collecting, processing, and using information about individuals to make decisions regarding the rights, benefits and opportunities of individuals, and how computerized records might influence privacy and due process. Michael Baker, Kenneth Laudon, and Robert Belair worked with Westin on the study and subsequently became active in the privacy epistemic community as lawyers and authors. The final report, Databanks in a Free Society, was published in 1972 and concluded that the use of computers had not yet produced the exceptional data collection and surveillance capabilities that many people concerned with privacy had suggested, but that policies for computer use had not evolved along with the proliferation of computers. The report recommended that compulsory data collection be limited and that a new set of “fair information practices” be established to guide in the collection, processing, and use of data on individuals.49

HEW Secretary’s Advisory Committee on Automated Personal Data Systems

Following the plethora of congressional hearings on technology, computers, databanks, privacy, and civil rights in the late 1960s and early 1970s, the Secretary of Health, Education and Welfare, Elliot L Richardson, established the Secretary’s Advisory
Committee on Automated Personal Data Systems in May 1972. The Committee, chaired by Willis Ware of the RAND Corporation, included a second member of the privacy epistemic community, Arthur Miller, who had previously testified at congressional hearings on privacy and had authored one of the classic books on privacy, *The Assault on Privacy*. The Committee was asked to analyze and make recommendations about four areas of interest:

- Harmful consequences that may result from using automated personal data systems;
- Safeguards that might protect against potentially harmful consequences;
- Measures that might afford redress for any harmful consequences;
- Policy and practice relating to the issuance and use of social Security numbers.

Many observers felt that the creation of the Committee on Automated Personal Data Systems was to serve as a palliative that would assuage the growing concern over privacy rather than to actually identify policy courses of action that might mitigate the problem. While “The committees’ membership encompassed a diverse range of expertise and viewpoints, and the early meeting were conflictual,” the “output of the committee was surprisingly coherent and influential.” The report essentially took the position of Westin and Miller that technology was the intrusive force that has created an erosion of personal privacy in society. This intrusive force of technology has created risk of abuse in all personal information systems and that possibility of abuse requires action to be taken to preclude injury of the individual. The report implies that the weaknesses of modern computerized personal data systems are inherent in their structure and that procedural corrections or controls must thus be implemented to protect society. Much
of the report, therefore, consists of recommendations of the committee based on a tacit acceptance that the personal-data systems are a *fait accompli*. Perhaps the most important part of the report consists of a code of five principles of “fair information practice” that “assure the individual a right to participate in a meaningful way in decisions about what goes in records about him and how that information shall be used.” These five principles are:

- There must be no personal-data record-keeping systems whose very 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 an individual to prevent information about him 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 reasonable precautions to prevent misuse of the data.

Some scholars note that these five “fair information practices” parallel the “fair information principles” of several other countries of about the same time-frame which suggests that there may have been communication of core privacy and data-privacy principles over time through a privacy epistemic community among British, German, Swedish, Council of Europe, Organization for Economic Cooperation and Development privacy commissions and experts. (See Appendix D for comparison of fair information practices/principles.) Colin Bennett devotes two chapters of his book *Regulating Privacy* to discussions of privacy-data protection “policy convergence,” and suggests that: “Tracking the genesis of ideas is an inherently difficult enterprise.” However, he says:
“Nevertheless, one line of development can certainly be traced to the debates in the United States in the late 1960s and early 1970s among the small number of data protection experts.” These “fair information practices” that Bennett suggests were generated as a result of the “debates . . . among the small number of data protection experts,” and were embodied in the HEW Records, Computers, and the Rights of Citizens report, are important because they became the core of the U.S. Privacy Act of 1974. “The Privacy Act of 1974 was written to apply the principles of the HEW report to the federal government’s use of personal data.”

The Privacy Act of 1974

The Privacy Act of 1974 was passed at a fortuitous time for the privacy epistemic community. Nine years of congressional privacy hearings, studies, and commission reports were punctuated by the Watergate Scandal, a Nixon administration scandal that stoked public concerns of surveillance, secrecy, and privacy. Surveillance became a front-page news issue, and no one wanted to appear to be condoning government surveillance of private persons. Distrust of the government for spying on private citizens was at an all time high. The resignation of President Nixon appeared to confirm all the charges of surveillance, spying, and breach of privacy by government in the eyes of American citizens. Thus, when privacy bills were introduced in Congress in the spring of 1974 they held center stage and garnered exceptional interest both within Congress and from the American public.
. . . hearings on a number of privacy bills were held in both the Senate and the House in 1974. In the Senate, the Committee on Government Operations, through its Ad Hoc subcommittee on Privacy and Information Systems, and the Judiciary Committee, through its Subcommittee on Constitutional Rights, held joint hearings on five privacy bills. The major bill on which debate focused was S. 3418 introduced by Senators Sam Ervin (D-N.C.), Charles Percy (R-Ill.), and Edward Muskie (D-Maine).59

Senate Bill S.3418 was comprehensive in that it covered all automated and manual information systems processing personal information in federal, state, and local government and also the private sector. It provided for a Federal Privacy Board with full regulatory authority . . . meaning the board had subpoena powers, the power to hold hearings, and the power to issue cease and desist orders. The bill established a code of “fair information practices,” modeled after the HEW committee recommendations, which gave individuals the ability to see and change their files and to be informed when information about them was disseminated.

Opposition to Privacy Legislation

Congressional hearings on the proposed bill focused on two contentious issues: 1) Applying the same privacy regulation to both public and private sectors; and 2) The establishment of a Federal Privacy Board. Both these issues were opposed by federal agencies and private-sector organizations, and in the end, the opposition was able to have both issues removed from the final legislation, significantly weakening the final protections afforded to personal data and information.
The major argument to having the proposed privacy legislation apply to the private sector was that there was little evidence to support the contention that there were abuses in private sector information practices. Congressional hearings and commissions had focused on government handling of personal data, not the private sector, so the burden of proof fell to those advocating private sector control to demonstrate abuses of personal data handling by the government. In the absence of conclusive proof, the opposition suggested that the private sector companies should adopt voluntary protections along the lines of codes of fair information practices. Such voluntary adoption of privacy protection procedures would reduce government regulations that would unnecessarily burden businesses. In the end, one of the key members of the privacy epistemic community, Dr. Alan Westin, agreed that it was unwise, at that time, to impose statutory privacy requirements on private organizations.\textsuperscript{60}

The second major issue of debate was whether a Federal Privacy Board should be established as part of the new privacy legislation. From the very first hearings, the idea of a privacy board or a privacy ombudsman had been strongly supported by the privacy epistemic community, but both the \textit{Databanks in a Free Society} report under the direction of Westin and Baker,\textsuperscript{61} and the HEW \textit{Records, Computers, and the Rights of Citizens} report created under the Chairmanship of Willis Ware, came out against regulation by an oversight board. The HEW Committee report stated:

\begin{quote}
We doubt that the need exists or that the necessary public support could be marshaled at the present time for an agency of the scale and pervasiveness required to regulate all personal data systems. Such regulation or licensing, moreover, would be extremely
\end{quote}
complicated, costly and might uselessly impede desirable applications of computers to record keeping.\textsuperscript{62}

In Senate hearings on S.3418, opposition to a privacy oversight board was again voiced by both federal agencies and private sector organizations alike. Government agencies argued against oversight claiming that it would be costly and that they could accomplish oversight within each agency. The Office of Management and Budget (OMB) and the Treasury Department both argued that an oversight agency was costly and unnecessary, because agencies were accountable for implementing privacy policies to both Congress and the public. From the private sector side, IBM argued against the creation of an oversight agency, claiming that fair information practices would protect an individual’s right of privacy.\textsuperscript{63} Additionally, President Gerald Ford expressed his personal belief that the creation of a privacy oversight agency was not needed, stating:

\begin{quote}
I do not favor establishing a separate Commission or Board bureaucracy empowered to define privacy in its own terms and to second-guess citizens and agencies. I vastly prefer an approach which makes Federal agencies fully and publicly accountable for legally mandated privacy protections and which gives the individual adequate legal remedies to enforce what he deems to be in his own best privacy interest.\textsuperscript{64}
\end{quote}

On November 21, 1974, the House and the Senate each adopted separate versions of the Privacy Act. The primary differences between the two versions were based on the Senate provision for the creation of a Privacy Protection Commission and greater restrictions on the use of information. With little time remaining in the legislative year, the Senate and House Committees opted to have the committee staffs work out a
compromise. The compromise bill leaned heavily toward the House version, which applied only to federal agencies and had no oversight agency. A code of fair information practices would apply to all federal agencies, which ensured that individuals would have access and knowledge of information in their personal files and the ability to correct their information. OMB was identified as the organization responsible for implementation and oversight of the act. A Privacy Protection Study Commission was directed to be established in order to investigate the need for additional legislation that applied to the private sector and the need for an oversight organization for federal agencies. Both the Senate and the House approved the compromise, and President Ford signed the Privacy Act of 1974 into law on January 1, 1975. The Privacy Act was to enter into force on September 27, 1975.

Privacy Act Expectations

As passed, the Privacy Act of 1974 represented a compromise between the privacy epistemic community and the opposition, the federal agencies and private sector organizations that feared the costs and intrusiveness of additional privacy regulation and oversight by the federal government. The Privacy Act reflected the minimum privacy protection that was advocated at the time of its passage. Within the federal government there was to be awareness and self-policing by agencies and oversight by OMB. But outside of government there was little regulation, and essential privacy guidance rested primarily on a code of fair information practice. In the end, even members of the privacy epistemic community such as Dr. Alan Westin had agreed that it was not the right time to
impose privacy regulation on private organizations. The argument that carried the day had been that of cost and burdens of increased regulation and oversight to both the government and to the private sector. While privacy had been shown to be important in congressional hearings and reports, it was balanced by the political need to limit the costs associated with implementing more stringent privacy protections for individuals.67

The privacy epistemic community was willing to “satisfice” for a first Privacy Act with limited impact because most believed that this was just the first step in achieving much broader privacy regulation in the future. Likewise, “Congressional advocates of stronger privacy legislation knew the barriers they confronted, especially opposition from President Ford. Privacy advocates spoke repeatedly of the Privacy Act as an “important first step.”68 The privacy epistemic community expected a continuation of high level of privacy interest that had been displayed over nearly a decade by Congress. The fact that the Privacy Act included a Privacy Protection Study Commission (PPSC) which was to investigate the need for a privacy regulatory oversight body and the need to extend the Privacy Act to cover all private sector organizations was seen as evidence that there would be a continuing interest and effort on the part of both the wider privacy epistemic community and Congress.

The privacy epistemic community was represented on the Privacy Protection Study Commission (PPSC) by two experienced members of the earlier HEW Records, Computers, and the Rights of Citizens report. Willis Ware of the RAND Corporation was the vice-chairman of the PPSC, while Carole Parsons, who had been the associate executive director of the HEW Committee, became the executive director of the PPSC.
In just over two years time the PPSC held 61 days of hearings, with over 300 private sector witnesses from the major business sectors, such as medical, banking, insurance, and credit testifying. Additionally, questionnaires regarding the handling of private sector information and the perceived costs and problems that firms would encounter in complying with proposed private sector privacy legislation were sent to 500 firms. Business and data processing firms were alerted to the importance of communicating their concerns to the PPSC by numerous articles that were authored in business journals and trade publications. The activities of the PPSC stimulated the privacy epistemic community and provided continued growth and development opportunities. Many privacy epistemic community members who had been associated with the earlier hearings and committees, which led to the Privacy Act, were attracted to, and participated in, the PPSC hearings.

The 654 page PPSC report, *Personal Privacy in an Information Society*, which was released in July of 1977, contains 162 recommendations and “… constitutes one of the most far-reaching inquiries into organizational uses of personal data ever assembled.” However, the considerable effort by the PPSC, its support staff, and witnesses in producing the report generated no new privacy legislation. Although the privacy epistemic community was energized by the two years of concerted interest in personal privacy, they proved unable to motivate additional action on privacy from Congress. In its report, the PPSC echoed the earlier HEW report and suggested that a voluntary approach would be the best near-term means of effecting private-sector privacy protection. They reasoned that: “… if individuals had the right to assert their interests,
organizations would find it more attractive to comply voluntarily.\textsuperscript{73} Members of the privacy epistemic community felt that the report placed too much emphasis on voluntary self-regulation by organizations and too much reliance on individual initiative in elevating privacy abuses.

The recommendations of the PPSC were forwarded to, and considered by, many congressional subcommittees. While some hearings were held on the recommendations of the PPSC, no action resulted. The “window of opportunity” for additional substantive privacy legislation had passed. Watergate and the surveillance excesses of the Nixon Administration had receded from the consciousness of the American public, and also from the immediate consciousness of congressmen.

Following passage of the Privacy Act and the recommendations of the Privacy Protection Study Commission, congressional interest in privacy was overshadowed by congressional and executive interest in the efficiency and effectiveness of programs. Consequently, the terms of debate shifted from an emphasis on individual rights to an emphasis on the detection of fraud, waste, and abuse.\textsuperscript{74}

Thus the privacy interests of the public and Congress evolved to the next issue, improving efficiency and effectiveness by eliminating fraud, waste and abuse using sophisticated computer matching programs to compare personal data. The privacy epistemic community turned its attention to the next threat to privacy, Project Match, which was to compare the computerized files of federal employees with the computerized files of those who were receiving benefits through programs such as Aid to Families with Dependent Children (AFDC). The privacy epistemic community moved on to confront this next challenge to individual privacy, a challenge that most thought was contrary to the recent Privacy Act of 1974, for which they had such high hopes.
Thus, the U.S. continued in its tradition of enacting narrow, sectoral, privacy laws that were directed to specific issues, problems, or sectors of society only after they were widely and clearly identified. This sectoral approach reacts to the threat or issue of the present instead of proactively responding to the larger threats that loom on the horizon; threats that can be seen by many technologists and privacy epistemic community members. The reasons for this narrow, sectoral, reactive approach to privacy protection will be addressed in the final chapter as part of the analysis of why, with a common privacy epistemic community working to protect the privacy of individuals, the United States and the European Union have arrived at such different privacy legislation.

**Chapter Summary**

This case study traces the influence of key members of the privacy data-protection epistemic community on the evolution of privacy policy and legislation in the United States from the late 1950s to the late 1970s. Scientific and technical members of the computer and database community working for government and industry, such as Willis Ware, were the first to recognize the threats posed to the privacy of the individual by these new technologies. Academic and technical papers authored for computer conferences were the first publications to alert the public to the new privacy problems. By the mid-1960s congress, lawyers, and academics were actively engaged in hearings, studies, and publications that sought to define, educate, and legislate bounds on computers, databases, and surveillance technologies. The privacy epistemic community grew with new members such as Alan Westin, Arthur Miller, Lewis Branscomb, Robert
Gellman, James Rule, Marc Rotenberg, David Flaherty, George Trubow, David Burnham, and Robert Ellis Smith began writing, testifying, and educating Congress and the public regarding the inherent dangers to privacy posed by the new technologies. Through the late 1960s and early 1970s numerous congressional hearings and studies were conducted on privacy issues in which members of the privacy epistemic community actively participated. However, it was not until 1974, following the Watergate scandal and the resignation of President Richard Nixon, that Congress finally acted--in the short time of a few months--to pass the Privacy Act of 1974, the benchmark privacy legislation of the United States.

The next chapter, Chapter Five, will present the European case study describing the growth and influence of the privacy data protection epistemic community in Europe which resulted in the European Data Protection Directive 95/46/EC on the protection of personal data.
Chapter Four Notes


2 See *Weeks v. United States*, 232 U.S. 383 (1914) The United States Supreme Court held unanimously that the illegal seizure of items from a private residence constitutes a violation of the Fourth amendment and set forth the “exclusionary rule” that prohibits admission of illegally obtained evidence in federal courts.

3 See *Olmstead v. United States*, 277 U.S. 438 (1928) Justice Brandeis, in a dissenting opinion, attacked the proposition that expanding the Fourth Amendment to include protection of telephone conversations was inappropriate. *Olmstead* was reversed by *Katz v. United States*, 389 U.S. 347 (1967).

4 See *Griswold v. Connecticut*, 381 U.S. 479 (1965). The United States Supreme Court held that the constitution provides a right of marital privacy regarding the decision to use contraceptives, invalidated a Connecticut law prohibiting contraceptive use, and established a general expanded right of privacy.


6 Willis H. Ware, "Security and Privacy in Computer Systems." (Atlantic City, NJ, Association for Computing Machinery (ACM), April 18-20, 1967).

7 See the ACM Digital Library at:


10 See: [http://www.computerhistory.org/events/lectures/johnniac_09151998/ware_bio.shtml](http://www.computerhistory.org/events/lectures/johnniac_09151998/ware_bio.shtml) As of July 2009, Dr. Ware remains listed as a resident consultant with the RAND Corporation and can be contacted at 310-393-0411, Extension 6432, or at [Willis_Ware@rand.org](mailto:Willis_Ware@rand.org).
Dr. Ware occupied a central node in the privacy epistemic community based upon his leadership in security and privacy studies/publications as well as his participation in computer professional organizations such as ACM, AFIPS, and IEEE and his important role in several government privacy commissions and hearings.

http://www.rand.org/about/history/.

See the Project Air Force History in pdf book form found at: http://www.rand.org/about/history/.


See: http://www.cbi.umn.edu/ware for several archived histories of Willis H. Ware.

For a complete list of publications by Willis H. Ware, see the RAND site at: http://www.rand.org/pubs/authors/w/ware_willis_h.html.


30 Lexis-Nexis Congressional digital document site; search *Invasions of Privacy* for a complete list of privacy-related congressional hearings and reports. [http://0-web.lexisnexis.com.bianca.penlib.du.edu/congcomp/doclist?_m=f98c1c4111ffad0ecedc2e25c0024288&wchp=dGLbVzz-zSkSA&_md5=00a23dc27abb2e61ddc6176c57333d0f](http://0-web.lexisnexis.com.bianca.penlib.du.edu/congcomp/doclist?_m=f98c1c4111ffad0ecedc2e25c0024288&wchp=dGLbVzz-zSkSA&_md5=00a23dc27abb2e61ddc6176c57333d0f).


32 Alan F. Westin, *Privacy and Freedom* (New York, NY: Atheneum, 1967), 487. Westin’s book is without doubt the most often cited source-book on privacy. Being one of the first comprehensive books on privacy issues it has been a point of departure for most privacy books and journal articles since.


38 See [http://www.law.berkeley.edu/centers/csls/people/people-bio-jrule.html](http://www.law.berkeley.edu/centers/csls/people/people-bio-jrule.html).


43 Ibid., 198.


51 Ibid.


54 Ibid., 40-41.

55 Ibid.


57 Ibid., 96.


65 Ibid.


68 Ibid., 83.


71 Ibid.


74 Ibid., 86.
Chapter Five
The Privacy Epistemic Community
and the
Legislation of Data Protection in the European Union

A Case Study

Introduction

A factor of considerable influence was the development of data protection on the American scene. Almost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale. It should be remembered that the modern notion of privacy, around which the debate on computers and personal freedom was centered, is basically American in origin.

Frits Hondius, Emerging Data Protection in Europe

The privacy epistemic community played a critical role in the complex process by which the European Data Protection Directive 95/46/EC came into being. The following case study highlights the creation and role of the privacy epistemic community in influencing and defining the data protection and privacy guidelines, conventions, and legislation of non-governmental organizations (NGO), States, and the European Union. As in the United States, the privacy epistemic community in Europe consisted of individuals who had knowledge of computers and automatic data processing (ADP) technology, lawyers, academics, businesspersons and politicians who became aware of the threat to privacy that such technology posed, and then took an active role in the data protection debates. Unlike in the United States, where the period of time from
introduction of privacy legislation to enactment of the Privacy Act of 1974 could be counted in months, the gestation period for the European Union’s Data Directive can be counted in decades. From the creation of the first data protection law in Germany in 1970, it was twenty-five years to the enactment of European Data Protection Directive in 1995 (and another three years to full implementation in 1998).

This case study describes the process by which data protection awareness developed and grew in Europe and identifies the role that key members of the privacy epistemic community that influenced the significant national data-protection legislation that culminated in European Union Data Protection Directive in 1995.

While in the United States, the awareness of the threat of technology to individual privacy was first perceived by the technical computer personnel who created the computer programs and operated the automatic data processing machinery for government, in Europe the first sense of a privacy threat — or “data threat” as the Europeans characterized it---came primarily from the privacy epistemic community and the congressional hearings that took place in the United States in the mid-1960s. The early recipients of the incipient threat to individual privacy were the lawyers, academics, and bureaucrats, who were closest to the government data processing systems in the European nations.

By the end of the 1970s, the privacy epistemic community had expanded to include influential lawyers, academics, and elected government officials across Europe. Most of the privacy epistemic community members regularly met under the aegis of the
Council of Europe (C of E) Committee of Experts and the Organization for Economic Cooperation and Development (OECD) Committee of Experts. As this chapter will describe, the initial impetus for data protection evolved in a multi-step process from the epistemic community formed of C of E and OECD privacy experts, to the national data protection officials (who participated in national data protection debates, and thus grew to be part of the larger data protection epistemic community) -- and then to the enactment of the EU Data Protection Directive itself. Finally, the institutionalization of the privacy epistemic community networking and policy definition through literature, organizations, conferences, and Internet sites has served to extend the EU Data Protection Directive and its principles to non-EU governments around the world, and the institutionalization of the global privacy epistemic community is addressed in closing.

Response to the Privacy Threat

From the early 1950s, the perspective of Europeans regarding the threat of computers and databases to their personal privacy was somewhat less developed than in the United States. In the 1950s and 1960s, the great bulk of the data processing computer technology employed in Europe was of U.S. manufacture. The Europeans thus did not have the indigenous infrastructure of computer automation specialists found in the United States. Europeans found themselves as followers of the United States in not just the technology, but also in the problems, issues, and concerns surrounding security and privacy dimensions of the end-to-end automatic data processing system. While the actual privacy concerns in the European Union were much the same as those that produced
privacy activism in the United States, the Europeans had the advantage of learning from the experience of the nascent security-privacy epistemic community in the United States. In the early 1960s, European governments and businesses, with the intent of making their operations fast and efficient, began installing and employing the then state-of-the-art computer ADP technologies available. “Some governments envisaged the establishment of large integrated databases in order to obviate the proliferation of computers in separate public offices.”

Early plans to automate government lists, registers, and databases were often overly ambitious in their descriptions and raised concerns regarding the balance of power in democratic governments and the increasing power of administrative bureaucracies. In response to these perceived threats to individuals and society, concerned individuals emerged---joined with others, who like them, recognized the threat---and over time coalesced into the privacy epistemic community to address the threat.

When exploring the role of the privacy epistemic community that influenced data protection and privacy legislation in Europe that led to the ultimate creation of the EU Data Protection Directive of 1995, two international non-governmental organizations and three European nations stand out in the literature because of the unique circumstances surrounding their path to national privacy and data protection legislation. The early, and continuing, awareness that privacy was threatened by technology---and particularly information collection and data processing---made the Council of Europe, the Organization for Economic Cooperation and Development (OECD), Germany, Sweden,

Germany is the first of these three nations to respond to the technological threat to privacy. Germany created the first general data protection law in response to concerns about the social and individual implications of automated data processing by the state---even though this first data processing law was enacted by the Land, or state, of Hesse in 1970. Sweden, the second of the three, was the first nation to enact broad privacy and data protection legislation in 1973. Sweden’s approach to data protection has been unusual and therefore was instructive to other European nations. The third nation, the United Kingdom, took a long and arduous path in enacting a data protection law, and -- some suggest—was forced to act only when the economic disadvantage of not having a data protection law was fully recognized in the early 1980s.

When considering the data protection movement in Europe, Frits Hondius, an early member of the privacy epistemic community notes that: “A factor of considerable influence was the development of data protection on the American scene. Almost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale. It should be remembered that the modern notion of privacy, around which the debate on computers and personal freedom was centered, is basically American in origin.”

A number of events in the United States motivated the Europeans to become aware of their own need for data protection legislation. “The writings by American
authors about privacy and computers (e.g. Westin and Miller), the 1966 congressional hearings, and the examples set by federal and state legislation, such as the U.S. Fair Credit Reporting Act of 1970 and the U.S. Privacy Act of 1974, have made a deep impact on data protection legislation in Europe.6 Thus not only did privacy events and positive activities in the United States promote awareness of the nascent need for privacy protection of the individual in Europe, but publications by Alan Westin7 and Arthur Miller,8 two early members of the privacy epistemic community discussed in the previous chapter, were credited with early influence on the European privacy movement. This influence not only continued, but grew significantly as the Europeans evolved their concepts of privacy and data protection. As will be seen in the following pages, the influence of the privacy epistemic community in the United States informed and motivated the nascent privacy epistemic communities in Europe to seek a similar vision of the right to privacy---but ultimately led to a significantly different path to achieving that right of privacy.

**Germany**

German history created a paradox in German society regarding the issues of privacy and data protection. While “. . . order is characteristic of the German mentality, leading to a regimented society in which it is normally considered desirable for the state to manage without the direct participation of the citizens . . .”9 the experience of the repressive governments of the Nazis and the Communists over the previous several generations conditioned the German people to be wary of state surveillance and state
power. The use of data processing technology by the Nazis to identify and apprehend German citizens in the 1930s and 1940s was a reminder of the dark side of the power of data processing by the government. Thus, the trust in the state as a source of order has been tempered with strong skepticism on the part of the German people when it comes to data collection.

The German Land of Hesse is recognized as being the first government to enact a general data protection law in response to concerns regarding the impact of automated data processing by the government. This first Data Protection Act of the Land of Hesse was passed in 1970. Because in Germany most federal government administrative activities are decentralized and conducted at the Land level, it was natural that the individual Laender were aggressive in automating their administrative processes with computer automatic data processing technology. Several Laender created their first automated data processing facilities in the late 1960s and early 1970s, including Schleswig-Holstein, Bavaria, and Baden-Wuerttemberg, and in each case rules, regulations, and general protections for the rights of individuals were incorporated in guidance regarding the operations of the processing facilities. Hesse, however, was the first Land to create a separate data protection law that was not directly associated with the establishment of the data processing facility. The Data Protection Law of Hesse was not limited to just the data processing facility, but applied to all data collection and processing in the Land of Hesse. The Hessian Data Protection Law even established a Hessian Data Protection commissioner who was responsible for data protection
compliance oversight within the *Land*. Dr. Sprios Simitis, became the first Data Protection Commissioner (DPC) of the *Land* of Hesse in 1975. Simitis subsequently became an internationally recognized expert and advocate for privacy and data protection whose influence in the privacy epistemic community spread throughout Europe and to the United States. Although several additional *Laender* created data protection laws similar to Hesse, the German Federal Government was not moved to create a data protection law for several years. Only when proposals for computerization of population registers and creation of personal identification numbers for each individual in the country were advanced in 1973 was the need for a federal data protection law recognized in Germany.

The process of creating the federal data protection law was complicated and took almost four years. Flaherty notes that: “Popular debate in West Germany was low key in comparison to discussion of the U.S. Privacy Act in the circumstances surrounding Watergate.” There were no study commissions, no open hearings, and no public recommendations.

The German Federal Data Protection Act (BDSG) was enacted in January 1977 and Professor Hans Peter Bull was appointed as the first federal Data Protection Commissioner (DPC) in 1978. Spiros Simitis attributed the position of DPC established by the BDSG to the influence of German lawyers, “. . . whose National Conference of Lawyers (*Deutsche Jurisentag*) instituted a data protection commission in 1972 that set forth a series of principles for computer regulation.” Once established in law, however, the influence of the BDSG was to be found within Professor Bull who, by not being an
elected politician or a life-long civil servant, took an aggressive position in defining both the office and the duties of the federal DPC. Bull later observed that, “One of the main reasons for creating an independent external supervisory authority was that a special ombudsman would be necessary to whom people could address their complaints about inadequate processing, and this should be an trustworthy person (or commissioner) not too much involved in administration itself.” At the end of Bull’s five-year term as DPC the opposition Free Democratic Party (FDP) had come to power. The FDP “. . . wanted data protection to pose fewer hindrances to police and security work.” And thus Bull was not reappointed as DSPC. Bull returned to teaching and the law, but remained a strong privacy epistemic community voice for data protection in Germany as well as contributing to the data protection debates and negotiations over the five years (1990-1995) needed to draft and enact the EU Data Protection Directive. Flaherty suggests that the success of the German data protection system was attributable to the skills of Hans Peter Bull.18

Sweden

In 1973, Sweden became the first nation to pass national data protection legislation. Because it was first, Sweden did not have the advantage of insight, debate, and experience from other nations on the privacy-data protection issue. Sweden therefore became an early experiment or “test-bed” for privacy concepts and legislation which subsequently ” . . . had an enormous and direct influence on the development of data
protection in Western European countries, even though the exact details of the Swedish model have not been widely imitated.”

In addition to being the first nation to implement privacy legislation, two characteristics acted to propel the privacy-data protection debate to early resolution in Sweden. First, Sweden employed a policy problem-solving style that has been characterized as “prospective and preventive” rather than “retrospective and remedial.” In support of this proactive policy creation process, Swedish royal commissions have long been formal institutional mechanisms that act as policy analysis and evaluation fora, while the inclusive *remiss* procedure of including all affected groups and organizations early in the policy making process ensures that there is agreement and compliance with the final policy. Second, although having a relatively small population, Sweden employed computer data processing earlier, and in more applications, than other countries did. Jan Freese, who was Director General of the Swedish Data Inspection Board (DIB) from 1975-1986, estimated in the late 1970s that: “On the average, the name of every adult, unmarried and conscientious Swede appears in at least 100 personal files . . . With a population of roughly eight million, Sweden is one of the most computerized countries in the world.”

In addition to being a small, highly computerized society, Sweden has also had a unique history of openness that led naturally to recognition of the need for data protection. This history of openness, however, accentuated the tension between the principle of accessible and open information for both government and society, and the
perils of aggregated personal data in what was becoming an increasingly integrated, globalized world.

A key influence in the development of the Swedish data protection model, and one of the most influential members of not only the Swedish data protection epistemic community, but also the European, was Jan Freese.

Jan Freese, who was a senior staff member of the DIB from its inception and director general from 1977 to 1986, played a crucial role as a publicist and activist for data protection. He appeared regularly in the media to warn about the consequences of record linkages for increased surveillance in an automated society. Since high-quality, articulate, and activist leadership is essential to the success of data protection, Freese exemplifies one path to success.24

Flaherty suggests that the success of the Swedish data protection system was attributable to the skills of Jan Freese.25 Ultimately, however “Freese’s strong leadership also contributed to his departure from the DIB, when conflicts of ideology and practice with the elected government became counterproductive.”26 However, Freeses’s influence in the larger European data protection epistemic community continued after his departure from Sweden’s DIB in 1986 through his participation in the Council of Europe Committee of Experts, the OECD privacy-related working groups, and in debates and discussions leading to the European Data Protection Directive in the early 1990s.

Bennet also identifies Freese as the central actor in spreading the Swedish data protection model when he says that:
The 1973 Swedish Data Act had a more widespread impact because of the efforts of a single person, Jan Freese, the Chair of the DIB from 1974 until 1986, who ensured that the Swedish approach was widely known. Other countries were naturally eager to learn of the early Swedish experiences of implementation. The Swedish Data Act was translated into English, French, and German. Delegations of British, German, French, and other European officials visited Stockholm in the first years of the act’s existence. Even though its enactment came too late to influence the deliberations of the Younger and HEW committees, it aroused keen interest as the first national attempt to regulate data processing. The Swedish Data Act was regarded as far less relevant in the United States, however. For many experts its concentration on the technology rather than on the information as well as its comprehensive licensing approach to both the public and private sectors rendered the Swedish approach inapplicable to American conditions.27

United Kingdom

The United Kingdom (UK) had the longest time period between the first consideration of the privacy-data protection issues and actually passing national privacy and data protection legislation. In all probability, this was the result of several dimensions of the UK legal and social system: 1) the UK has no constitution or basic law that specifically guarantees a right of privacy; 2) privacy-related issues were commonly addressed under areas of common law such as the laws of confidence, trespass, or defamation, to which privacy is loosely related; 3) in the 1950s and 1960s privacy issues were focused on activities of the British press, which indulged in then rakish exposé journalism of film stars, celebrity personalities, and members of the Royal Family; and, 4) computers and databases were not immediately seen as problems in these early years of technological implementation.28
Several parliamentary member’s bills were introduced in the late 1960s that highlighted a growing interest in, and awareness of the concept of privacy, but none received recognition or substantial public debate until “Justice,” the British Section of the International Commission of Jurists, published Privacy and the Law in 1970. Nearly coincident with the “Justice” report, a “Right of Privacy” bill was introduced by Brian Walden in the House of Commons that had been authored by the Committee on Privacy of the Justice Society. As a result of this bill, the issue of personal privacy of citizens was debated in the House of Commons, and was thus opened to public discussion for the first time.

The broad scope of Walden’s bill and the possible implications of privacy legislation led to opposition on the part of some business organizations. The press, seeing possible limitations on their activities, raised freedom of speech issues and influenced the Labor Government to sideline the Walden Bill by creating a committee to study the privacy issue and the need for legislation. Thus, in May 1970, one month before the Labor Government fell in the general election, the Committee on Privacy was appointed under the chairmanship of Sir Kenneth Younger.

The terms of reference for the Committee on Privacy were in some ways rather general as the charter did not specifically identify computers, automatic data processing, or technology as areas upon which to focus. It merely called upon the committee:

“To consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusion into privacy by private persons and organizations, or by companies, and to make recommendations.”
Perhaps because of the broad, general nature of the study, the Report of the Committee on Privacy, presented to Parliament in July 1972, carried greater relevance and impact than it might otherwise have had. The Committee sought broad input from across British business and society, and fully one-third of the final report consists of appendices of contributions from subject-matter-experts in the areas of privacy, computer, and law. The Report made recommendations that addressed perceived privacy problems in business sectors such as the press, broadcasting, credit rating agencies, banks, employment, students and teachers, medicine, private detectives, as well as for areas of technology such as technical surveillance and computers. However, the Committee stopped short of calling for the creation of a general “right to privacy,” claiming that additional new laws were not needed, that such a right could compromise freedom of speech, and that it would be dangerous to enter into adjudication between the right to privacy and claims of “public interest.”

Regarding the threat of computers to privacy, the Younger Committee felt that the use of computers in the private sector was not at that time a threat to society, but it did recommend “... the immediate voluntary adoption by computer users of certain principles for handling personal information on computers.” Additionally, the Committee identified ten principles for handling personal information (See Appendix D). These ten principles for handling personal information were submitted to the Committee by the British Computer Society. Hondius suggests that: “The Report had a
great moral effect on computer users, particularly owing to the fact that computer practitioners were organized in an influential organization, the British Computer Society (BCS). Its members were bound by a Code of Conduct adopted in 1971 and to computer users it recommended for consideration a Code of Good Practice, published in 1972.”

In this case the BCS was part of a wider privacy-data protection epistemic community that influenced subsequent legislation, not only in the UK but well beyond, by contributing their expertise in the form of principles for handling personal information.

The ten principles for handling personal information enumerated in the Younger Report “was the first concise and comprehensive set of such principles to be published anywhere in the world” according to Paul Sieghart, a key privacy epistemic community figure in the promotion of data protection legislation in the 1970s and early 1980s. The Younger Principles comprise one of four fair information practice statements that were promulgated in the 1970s and early 1980s by the UK (1972), the United States (1973), the OECD (1980), and the Council of Europe (1981). (See Appendix D) Although the number of “fair practices” and the detail embedded in each varies greatly, the underlying similarity in basic privacy concepts suggests that common influences, or a common epistemic community, contributed to their collective creation.

It appears hard to overestimate the importance of the Younger Committee, for as Hondius commented:

Outside the United Kingdom, the Younger Report served as a basic document to many governmental and inter-governmental bodies dealing with data protection. Several proposals contained in the Report subsequently made their way into foreign legislation. Moreover, they
formed the basis for European common rules on the subject. The Resolutions which the Council of Europe adopted on data protection in 1973 (private sector) and in 1974 (public sector) received a great deal of inspiration from the Younger Report. The Chairman of the first Council of Europe committee of experts, which dealt with the matter in November 1971, Mr. Gerald Pratt, had been Secretary of the Younger committee. Since the Council of Europe’s Resolutions ((73)22 and (74)29) were also addressed to the United Kingdom, they did not fail to bring back as it were via Strasbourg, some of the viable ideas contained in the famous 10 points.40

However, while the Younger Report was well received and widely respected in government as a benchmark in the privacy-data protection debate, there was no immediately forthcoming privacy legislation proposed in Parliament. It was almost three years later, in December 1975, that the government issued two white papers that responded to the Younger Report recommendations on computers: the first entitled Computers and Privacy and the second Computers: Safeguards for Privacy. These reports “found no evidence of improper use of computers in the public sector,” but at the same time identified the need for regulation and identified five aspects of computer operations that could pose a threat to privacy.41

In July 1976, the Data Protection Committee (DPC) or Lindop Committee, was formed under the chairmanship of Sir Norman Lindop. In the course of its work, the DPC conducted several studies with the help of more than 300 organizations and individuals.42 The DPC studies were the first to look at all dimensions of public (government) and private (business and industry) use of personal data. In their report of July 1978, the DPC made distinctions between data protection and privacy rights and
suggested flexible legislation that would cover all forms of data collection and
manipulation (automated as well as manual). Warren and Dearnley suggest that an
important and lasting impact of the Lindop Committee was that, “Former members of the
DPC continued to lobby the government . . .”\textsuperscript{43} Two in particular, Paul Sieghart and
Charles Read, had a significant impact in keeping the pressure on for legislation.

Sieghart was a barrister, a human rights advocate and the primary author
of the Computers and Privacy White Paper. He was involved in
bringing together the members of the Committee other than the
chairman. Read, Director of the Inter-Bank Research Organization, was
described by Lindop as ‘an excellent Committee man.’ In the years
following the publication of the (Lindop) report, both lobbied the
government extensively.”\textsuperscript{44}

Once again, following the DPCs Lindop Report, there was no action for
legislation and a three-year period of “entropy” ensued in which no substantive action
was taken on privacy and data protection in Parliament. However, with the introduction
of the OECD Guidelines in 1980 and the Council of Europe Convention in 1981, pressure
was being applied to the UK to based on the fears “. . . that UK companies would be at a
disadvantage when competing in the international data processing market without
legislation.”\textsuperscript{45} Warren and Dearnley note that “. . . the role of dedicated former members
of the DPC was significant. In addition to Sieghart, Read, representing the banking
community, had been vigorous in campaigning for legislation in the wake of the Council
of Europe Convention.”\textsuperscript{46} As in the United States, the experience of serving on privacy
committees or commissions conditioned many members to continue to act as part of the
privacy epistemic community.
Finally, on December 22, 1982, the first Data Protection Bill was introduced in the House of Lords. Few were happy with the content of the bill. Newspaper accounts characterized the bill as being motivated by commerce and losing markets instead of defending individual privacy against computer intrusions. Although the bill was challenged by the Labour Party in standing Committee debates on many points, the overwhelming Conservative Party victory the previous year allowed the bill to be passed out of Committee. The Bill was reintroduced in the House of Lords in July 1983, and with minor modifications voted into law, receiving “Royal Assent on 12 July 1984.”

In the Data Protection Act of 1984, the UK opted for a minimalist privacy data protection solution that applied only to automatic data processing and created an isolated Registrar without an advisory committee to oversee the implementation of the law. There is good reason to agree with many observers who suggested that in spite of an inordinate number of well conceived and well documented privacy-data protection studies, reports, and white papers, the government had settled for a law privileging business, commerce, and industry over the privacy rights of the individual. Bennet confirms this view when he says:

“The Council of Europe Convention allows data protection authorities to refuse the transborder flow of data to countries that do not have adequate data protection legislation; it thus had a direct impact on those nations that legislated late. It was generally assumed in Britain that the final passage of the 1984 Data Protection Act took place for economic rather than libertarian reasons. Britain feared that personal data protection could be come a legal pretext for trade protectionism, and would lead to
the isolation of the country’s data processing industry as well as other service sectors of the economy that rely on unimpeded communications. The Conservative government admitted as much in its white paper of April 1982.”

**The Council of Europe**

The Council of Europe (CoE) was the first European institution to become interested in the privacy of individuals and data protection. Shortly after the founding of the CoE in 1949, the CoE adopted the first international legal instrument safeguarding human rights, a Convention for the Protection of Human Rights and Fundamental Freedoms. Thus, from its inception, the CoE has had a primary mission of protecting the freedoms and rights of its member populations. Since 1968 the CoE has involved itself with wide-ranging activities regarding the use and influence of computers, with two primary objectives: 1) to encourage the use of computers and computer science to benefit the people of Europe, and 2) To assist member states in assessing the impact of computers on man, society, civil rights, and liberty in Europe. In 1971, a CoE Committee of Experts was established by the Council to focus on problems and issues of protecting privacy against the threat of electronic computer data banks. The Committee of Experts, all highly informed and knowledgeable on the issues of privacy and data protection in their respective countries, noted that the issue of protecting privacy from computer electronic data banks was already a subject of interest in several member-nation governments, and that the member states should work together on a common position in order to avoid divergent laws on electronic data processing and the protection of
The Committee of Experts therefore set about creating a set of principles that might be applied generally across member nations. Over the past four decades the Committee of Experts has become a locus of expertise regarding the many convoluted issues surrounding privacy and data protection. Bennett notes that: “The members of this committee (Committee of Experts) served a critical role in disseminating expertise and advice, as they were key actors in domestic data protection efforts at the time.”

Based on recommendations of the Committee of Experts, in 1973 and 1974 the Committee of Ministers adopted two resolutions on data protection. The first, Resolution (73) 22, established principles of data protection for the private sector and the second, Resolution (74) 29, established principles of data protection for the public sector. These two Resolutions led directly to the CoE Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Treaty 108), which was adopted by the Council of Europe in 1980, opened for ratification in January 1981, and entered into force on October 01, 1985. Bennett notes that:

The committee of Experts . . . served in the critical role of disseminator of fair information policy. Indeed, the members of this committee were both the core of the European policy community and the key actors in the domestic data protection efforts. Every subsequent national commission report, proposal, or bill has made reference to these two resolutions.

It must be noted that: “European Conventions and Agreements, however, are not statutory acts of the Organisation; they owe their legal existence simply to the expression of the will of those States that may become Parties thereto, as manifested inter alia by the signature and ratification of the treaty.” Thus the Convention served most European
nations primarily as a guide to action regarding privacy and data protection as well as a subsequent template for enactment of national data protection legislation. As was soon discovered, this led to a lack of uniformity of law as well as enforcement across those nations that responded to the Convention, and ultimately prompted data protection action by the European Union.

The CoE Committee of Experts on Data Protection (CJ-PD), later renamed the Project Group on Data Protection, has continued to have an important investigative, reporting, and educating role over the past two decades in the extended CoE data protection community. Not only have the studies and reports of the group been important in defining and clarifying major European privacy and data issues from use of data by the police sectors, transfer of personal data to third party nations, to biometrics, smart cards, and smart passports, but many of the CJ-PD members are long time privacy and data protection subject-matter experts within their home nations. Many members hold, or have held, key positions within CoE member-state privacy organizations and thus truly qualify as experts in both technical knowledge and privacy-data protection experience. For example, of special interest regarding the influence of this epistemic community of data protection experts is the participation of Dr. Spiros Simitis. Dr. Simitis has had a long history of being an influential member of the Council of Europe Committee of Experts on privacy and data protection issues as well as a participant in a broader epistemic community of privacy and data protection experts in the international legal community. In 1999, Dr. Spiros Simitis, a Professor at Johann Wolfgang Goethe
University of Frankfurt am Main and Director of the Research Centre for Data Protection (Germany), authored a CoE report entitled “Revisiting Sensitive Data,” which reviewed and analyzed responses to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) held in Strasbourg from 24-26 November 1999.\textsuperscript{61}

**The Organization for Economic Cooperation and Development**

Composed of 20 countries when the Organization for Economic Cooperation and Development (OECD) was founded in 1960, the OECD consists of 30 member-nations in 2009.\textsuperscript{62} The OECD brings together the governments of countries committed to democracy and the market economy from around the world to support sustainable economic growth, boost employment, raise living standards, maintain financial stability, assist other countries' economic development, and contribute to growth in world trade.\textsuperscript{63}

The OECD played a leading role from the late 1960s in influencing a broad array of computer policies, and by extension, privacy and data protection policies. In the context of this broad mission, the emerging problems of data security, privacy, and data protection became important issues for member-states. Initially, the broader issues surrounding the employment of computers in business and international trade dominated the OECD agendas---privacy was not the central issue. Only after Council of Europe efforts had clarified the issues surrounding privacy and data protection in the international context did the OECD become proactive and make privacy a principal effort.\textsuperscript{64}
Based on the hypothesis that post-industrial society would depend upon information as a production factor, the OECD created a Computer Utilization Group in 1969 that, working in concert with the Information Policy Group and the Committee for Science Policy, studied a wide variety of computer-related issues, including: “electronic data banks, interaction of computers and telecommunications, computer manpower education, computer utilization surveys, efficiency audits for computer systems, and potential of information technology in urban and regional planning.” The OECD focused specifically upon the problems associated with privacy and data protection by creating a Data Bank Panel that conducted seminars on issues such as trans-border data flows, personal identifiers, and data protection guidelines. By 1975, the several OECD computer and privacy-data protection groups had documented their reports and recommendations by publishing more than ten volumes of the *OECD Informatics Studies*. This early work was subsequently incorporated into the current OECD guidance on privacy policy and practice for OECD members.

The influence of the OECD in framing privacy and data protection issues, sponsoring conferences, working groups and panels, and creating a set of guidelines available to members and non-members alike has had a significant impact on privacy legislation in Europe. Hondius suggest that there have been three reasons for the success of the OECD regarding computer-related problems:
First, the OECD is the only international organization which has tackled studies of informatics in their broadest sense, in conjunction with the study of policies for future society. Secondly, OECD is the only platform for regular exchange of information between countries in four continents having a similar political, economic, and social system. For example there is a close affinity between data protection problems and solutions in Europe and North America. Via OECD ideas have been exchanged between American and European Legislators. In the future the transfrontier data flow problems between the United States and Canada will be relevant case studies for similar transfrontier data flows in Europe. Eventually, a point may be reached where such problems will arise also between America and Europe. In the third place, the working methods of the OECD have been particularly conducive to fruitful results. Consequently, OECD documents are widely used also by other international organizations.  

The OECD responded to privacy-data protection threats posed by advances in computer-communications technology through Committees of Experts, studies, and conferences that address nascent privacy-data protection issues. The OECD thus served as a crossroads for the privacy-data protection epistemic community of its member-nations, expanding privacy-data protection related knowledge throughout its membership.

**The European Union Data Protection Directive of 1995**

Through the efforts of the data protection epistemic community previously described, by the late 1980s seven of the twelve nations of the European Community had created data protection legislation. However, even though there was a general consensus on the need for data protection among these nations, the actual data protection laws of the seven varied widely.

The Council of Europe Conventions and OECD Guidelines on data privacy had been only partially effective in motivating member states to create data protection laws.  

156
There was no uniformity across the seven states that had such laws--and no uniformity of enforcement. The five member nations that did not have data privacy laws showed no inclination to pass data protection laws anytime soon.

It was in this climate that the European Commission decided that there were critical economic issues at stake associated with the harmonization of data protection law among member nations that required the Commission to act. The creation of the Internal (Common) Market, which was scheduled to be instituted in 1992, would require the unimpeded flow of personal information throughout the EU. Obviously, the conflict in data protection laws would create a significant obstacle to the smooth and unobstructed flow of trade across the EU — a primary goal of the Internal Market movement.

There were three major “interests” that collided in 1990 to 1995 in the search for an EU-wide data protection standard in the face of impending completion of the common Internal Market: 1) interests in the EU common Internal Market that sought to achieve a common, level, unobstructed integration of all member-nation economies; 2) interests of a uniformly high standard of personal privacy-data protection across the EU; and, 3) business interests that feared obstacles to customer data processing and significant increases in costs as a result of data protection legislation. Each of these three interests attempted to advance their positions in the course of the five years of negotiation necessary to finally enact the EU Data Protection directive of 1995.70

Representatives of the seven countries that already had data protection laws in place, all of whom were members of the privacy epistemic community by virtue of their
close and continued association with their national and transnational data protection community, argued for community-wide data protection legislation in the late 1980s. They pointed out that citizens of those member-countries that already had data protection in place could find their privacy rights violated in nations that had little or no regulation.

Three data protection events occurred in late 1989 that clearly demonstrated the problems associated with transborder data flows in an environment of uneven (or no) data protection law. In July 1989 the French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés or CNIL) threatened to block data transfers of employees between Fiat’s corporate offices in France and in Italy. The CNIL argued that Italy’s data privacy rules were inadequate to protect the data, and therefore personal information about French citizens could not be transferred. Fiat Italy was forced to find a solution to the refusal of the CNIL to allow the transfer of data. Resolution of the impasse came when Fiat Italy signed a data protection contract in which it agreed to protect personal data coming from Fiat France in accordance with CNIL rules. This first episode clearly demonstrated how conflicting national data protection rules could perturb routine business activities between nations.71

A second data transfer event took place just two months later, in September 1989, when the CNIL blocked the plans of the Gustave Roussay Institute, a French cancer research center, to join the Belgian-based European Organization for Research and Treatment of Cancer (EROTC). The CNIL pointed out that Belgium did not have national data protection legislation in place, and therefore the Gustave Roussay Institute
could not send sensitive medical data to Belgium until such legislation was enacted by Belgium.\textsuperscript{72}

A third imbroglio took place over the Schengen Agreement for free movement of persons and labor among Germany, France, Belgium, Luxembourg, and the Netherlands. In order to secure the new external border encompassing these members to the agreement, a Schengen Information System (SIS) was proposed to network the existing border control and national customs databases so as to allow mutual policing of national borders. The Germans and French raised the issue that Belgium did not have a data protection law with the result that data protection experts from France, Germany, and Luxembourg objected to the violation of their national data privacy laws by sharing sensitive police information with Belgium. Only after Belgium bowed to pressure from the data protection community and pledged to expedite data protection legislation, were the data protection clauses and monitoring authority for the SIS developed.\textsuperscript{73}

With the increasing frequency of data protection issues arising within the community, the European Commission was forced to act. In 1990, with the impending creation of the EC Internal Market in 1992, the European Commission’s Internal Market Directorate drafted the first data protection directive. Over almost five years the data directive legislation was debated and modified in response to three powerful constituencies: 1) The EC Commission and Internal Market Directorate that sought a level and unobstructed internal common market and trade environment; 2) the privacy-data protection epistemic community that represented the goals of data protection
commissions of seven nations, the OECD, and the Council of Europe, and data protection human rights; and, 3) the European business and trade community, that wanted no increase in business regulation, trade restrictions, or costs related to privacy and data protection legislation.

Efforts by the data protection authorities to draft a common data protection position for the EC began at the Eleventh International Conference of Data Protection Officials held in Berlin in 1989. The strongest argument for a common EC data protection law was premised on the experience of Germany, which had already had several data processing companies relocate outside of Germany in order to avoid the strict German data protection laws. Obviously, businesses that depended on consumer data would relocate to data privacy havens where there were few or no restrictions on their collection and use of personal data. Data commissioners from the seven nations that had passed data protection laws pointed out that if the remaining five nations did not institute data protection laws by the time of the creation of the common Internal Market in 1992, that the five nations would have to be treated as if they were outside of the EC and the common market.

Recognizing that the Internal Market could never be achieved without uniform data protection law across all member nations, the Internal Market Directorate became the focal point for the creation of the first draft of EC data privacy legislation. Data protection commissioners took an active part in drafting and amending data protection legislation. After review, oversight, and amendment of proposals by data protection
commissioners---through three major revisions---accommodation among the parties was finally reached on the structure of data protection legislation.

After almost five years of long and difficult negotiations, Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council was passed on 24 October 1995. As a directive, 95/46/EC addresses only the member states, and is not legally binding on citizens. Each member state was required to transpose the directive into internal law by the end of 1998. All member states have enacted their own data protection legislation.

A significant feature of the European Data Protection directive has proven to be Article 29, which created a standing committee of national data protection experts consisting of one member from each EU member country, called the Article 29 Working Party. The effect of Article 29 has been to formally institutionalize the nucleus of a European privacy-data protection epistemic community. Article 30 identified the duties and tasks required of the Article 29 Working Party such as studying emerging data protection issues, advising the European Commission on data protection issues concerning the internal market, evaluating and making recommendations regarding the privacy protection in non-EU countries that desire to do business with citizens and businesses of the EU, and creating an annual public report “on protection of natural persons with regard to the processing of personal data in the Community and in third countries.”
The role of the Article 29 Working Party in evaluating and coordinating data protection throughout the EU, as well as beyond the borders of the EU, has greatly expanded in the past decade. Because the Working Party authors’ opinions, recommendations, and working documents are based on the expertise of data protection experts from each EU member nation, their influence has increased as organizations and nations external to the EU have realized that they could seek the guidance of the Working Party and preclude confrontation with the European Commission. The Article 29 Working Party thus represents a significant node of the privacy-data protection epistemic community in communicating, educating, and influencing privacy-data protection issues globally.

Two developments of the past several decades have influenced the growth and maintenance of the global privacy-data protection epistemic community. The first is the development and expansion of the Internet as a global communications tool, and the second has been the creation of periodic privacy and data-protection conferences held around the world. These two developments within the privacy-data protection epistemic community act as catalysts in informing, educating, and influencing privacy-data protection members from diverse academic, business, technical and social backgrounds regarding basic principles and rights regarding privacy and data protection. Appendices A and B identify some of the prominent privacy-data protection organizations that have a permanent Internet presence and authority in privacy-data protection issues. By having a permanent presence on the Internet, these organizations transcend the original life-cycle
limitations of the epistemic community as described by Haas, Adler, and others. The Internet provides a ubiquitous, physical presence and connectivity for the global privacy-data protection community in which they can participate in nascent and evolving issues on a daily, if not minute-to-minute basis. Thus, members of the privacy-data protection epistemic community are no longer limited to single-events, but continue developing their knowledge and expertise in the evolving privacy data protection issue-area by being constantly informed by other epistemic community members worldwide.

The second development that has influenced the growth and maintenance of the global privacy data protection epistemic community is the proliferation of the conference. The first annual International Data Protection Commissioners Conference was held in 1979. The 31st annual International Data Protection Commissioners Conference will be held in Madrid in November 2009. Over the past three decades these conferences have provided opportunities for networking, education, and debate on salient privacy-data protection issues. Newman says that trans-governmental cooperation in privacy-data protection intensified across the EC starting with the first annual International Data Protection Commissioners Conference and, “Over a ten-year period, the transgovernmental network of data protection agencies built up their credibility as data privacy experts and developed a coherent proposal for action at the EU level.”

Newman thus believes that the International Data Protection Commissioners Conferences played an important role in the development of the common proposal of the EU data privacy epistemic community of experts in the late 1980s and early 1990s. Continued
Chapter Summary

The privacy-data processing epistemic community in Europe evolved in response to the perceived need for national legislation to protect the privacy of the individual citizen from automated data processing (ADP) systems instituted by the government as a means of increasing efficiencies in state-run social programs.

Following the early creation of several national privacy-data protection laws, two non-governmental organizations (NGOs), the Council of Europe and the OECD, recognized the nascent problems both public and private ADP posed and created committees of experts, working groups, and conferences to study privacy-data processing problems and make recommendations. These committees, working groups, and conferences became networking opportunities for members of the privacy-data protection epistemic community, most of whom were already privacy-data protection subject-matter-experts in their respective European nations. The OECD adopted Privacy Guidelines in 1980, and the Council of Europe issued its data protection Convention in 1981. Both the OECD Guidelines and Council of Europe Convention allowed considerable variation in both the execution and the enforcement of data protection law—which resulted in great variation in privacy-data protection laws in the seven of twelve
member nations that legislated data protection laws. Five of the twelve EC nations chose not to create data protection law.

Following several data protection events in the late 1980s that demonstrated the problems associated with transborder data flows in an environment of uneven (or no) data protection law; the European Commission was forced to act. In 1990, with the impending creation of the EC Internal Market in 1992, the European Commission’s Internal Market Directorate drafted the first data protection directive. Over almost five years the data directive legislation was debated and modified in response to three powerful constituencies: 1) The EC Commission and Internal Market Directorate that sought a level and unobstructed internal common market and trade environment; 2) the privacy-data protection epistemic community that represented the goals of data protection commissions of seven nations, the OECD, and the Council of Europe, and data protection human rights; and, 3) the European business and trade community, that wanted no increase in business regulation, trade restrictions, or costs related to privacy and data protection legislation.

After almost five years of long and difficult negotiations, Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council was passed on 24 October 1995. As a directive, 95/46/EC addresses only the member states, and is not legally binding for citizens. Each member state was required to transpose the directive
into internal law by the end of 1998. All member states have enacted their own data protection legislation.

In the following Chapter Six, the privacy-data protection models of the United States and the European Union will be analyzed and compared. Though both the United States and the European Union share similar perceptions of the privacy-data protection problem, a similar privacy-data protection epistemic community of literature, subject-matter-experts, conferences, and internet Web sites, the privacy-data protection models or “regimes” of the two are very different. While the European Union chose a comprehensive or “omnibus” privacy-data protection approach, covering all aspects of the economic, political and social environments, the United States chose a limited or “sectoral” approach that addresses only specific issues and problems as they arose. Chapter Six will explore, among other issues, how and why the United States and the European Union chose such dramatically different responses to the common privacy-data protection problem.
Chapter Five Notes

1 Frits W. Hondius, Emerging Data Protection in Europe (Oxford, UK: North-Holland, 1975), 6. Dr. Frits W. Hondius was Head of Division II (Droit Public) for the Directorate of Legal Affairs in the Secretariat General of the Council of Europe. Dr. Hondius served as a representative of the Secretariat in the Committee of Experts on Data Protection that reviewed the Draft Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data promulgated by the Council of Europe. From Frits W. Hondius, "Data Law in Europe," Stanford Journal of International Law 16 (1980), 87.


3 Hondius, Emerging Data Protection in Europe, 5.


5 Hondius, Emerging Data Protection in Europe, 6.

6 Ibid., 6 Dr. Frits Hondius was an active member of the privacy epistemic community and contributed significantly to the data protection movement in Europe. He served as Secretary to the Council of Europe’s Committee of Experts on Data Protection.


10 Ibid., 24.


12 The German word *Land* identifies a component state in the Federal Republic of Germany, just as the American English word *state* identifies one of the 50 component states in the United States. *Laender* (the ae replaces the umlaut in modern German) is the plural of Land.

13 Data protection is a translation of the German word *Datenschutz*, meaning data protection. The term “data protection” is usually used in European law instead of the term “privacy,” which is preferred in the United States. As will be discussed in Chapter Six, this choice of terminology reflects a difference in perspective between the United States and the EU on the issue of privacy, as opposed to security—or protection—of an individual’s data or information. See Bennett (1992) for an in depth discussion of terminology.


21 Ibid., 61.

Quoted in Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, 264. Estimates a decade later were that personal information on each individual Swede was in between 50 and 300 databases. Sweden was also early to implement a national universal system of personal identification numbers that made it much easier to monitor citizens than in other European countries.


Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, 125. Bennett goes on to say: “With the exception of the United States, however, in each country there was an immediate awareness of overseas legislation and a keen desire to learn from the experience of others.” The data protection epistemic community of politicians, lawyers, and academics were keenly aware that they were all facing the same technologically induced data and information-based societal problems.

Ibid., 82 - 94.

Mark Littman and Peter Fredrick Carter-Ruck, Privacy and the Law: A Report by Justice (Justice Society, Committee on Privacy) (London, UK: Stevens, 1970), 1. This short tract by the Committee on Privacy of the Justice Society informed the debate on privacy and the perceived threats to privacy, thereby motivating action in Parliament that indirectly led to the appointment of the Younger Committee. According to Bennett, the Justice Society also drafted the Right To Privacy Bill that Brian Walden, MP, subsequently put forward. Bennett and Flaherty identify actions like these by members of the epistemic community of lawyers and legal organizations across Europe that educated and influenced legislators, businessmen, and citizens regarding privacy rights and threats to privacy.

Hondius, Emerging Data Protection in Europe, 49.


Ibid., 13-16.

Ibid., 16 Paragraph 54 also identifies an additional six recommendations for the monitoring and identification by government of computer problems that might arise in the future.

Ibid., 182-184.

Hondius, *Emerging Data Protection in Europe*, 51 Younger, *Report of the Committee on Privacy*, 331-335. Also see British Computer Society (BCS) archives at [http://www.bcs.org/](http://www.bcs.org/). The BCS has been a member of the security-privacy-data protection epistemic community and was one of the first organizations to create formal fair information practice principles, which were subsequently incorporated into the Younger Committee Report.


See Appendix D for enumeration of the fair information practices statements created as a result of commissions and studies by the UK (1972), the United States (1973), the OECD (1980), and the Council of Europe (1981).


Ibid., 245.

Ibid., 250.

Ibid., 245.

Ibid., 251.
Ibid., 251.

Ibid., 254.

Ibid., 255.


Ibid. Hondius describes in detail the four-year process (1968-1971) by which the Council investigated issues of human rights when confronted with “modern scientific and technological developments,” such as the electronic databases and the impact of the computer on individual privacy.

Ibid., 66.

Henry Farrell, "Negotiating Privacy Across Arenas: The EU-US" Safe Harbor" Discussions," *Common Goods: Reinventing European and International Governance* (2002), 84. The data protection epistemic community consisted of individuals who would have influential roles in privacy and data protection developments over the next two decades, such as Spiros Simitis of Germany; Jan Freese and Peter Seipel of Sweden; Paul Sieghart of the UK; and Louis Joinet and Jacques Fauvet of France.

For background on CoE investigative and reporting processes regarding privacy and data processing, see the ETS Explanatory Report at: [http://conventions.coe.int/treaty/en/Reports/Html/108.htm](http://conventions.coe.int/treaty/en/Reports/Html/108.htm). For a complete descriptive listing of the Recommendations et Resolutions of the CoE Committee of Ministers regarding privacy and data protection from 1981 to present (latest, 2002), see: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/12Recommendations%20and%20resolutions%20of%20the%20Committee%20of%20Ministers.asp#TopOfPage](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/12Recommendations%20and%20resolutions%20of%20the%20Committee%20of%20Ministers.asp#TopOfPage); For the text of Resolution 73/22 relating to the CoE principles of data protection for the private sector, see: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/1Resolution(73)22_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/1Resolution(73)22_EN.pdf); for Resolution 74/29, regarding principles of data protection for the public sector see: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/1Resolution(74)29_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal_instruments/1Resolution(74)29_EN.pdf).


As described in *About Conventions and Agreements in the Council of Europe Treaty Series (CETS)*, at: http://conventions.coe.int/general/v3IntroConvENG.asp. Last accessed 02 April 2009.


For reports and studies of the Council of Europe Committee of Experts on major privacy and data protection issues over the past decade see: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports%20and%20studies%20by%20Experts/.

See OECD membership and accession history at: http://www.oecd.org/document/58/0,3343,en_2649_201185_1889402_1_1_1_1,00.html.

OECD mission at: http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html.

Ibid., 137-40 Since the mid-1970s the OECD has been a prominent nexus of privacy and data protection panels, symposia, and convocations.

Ibid., 58.

See *Privacy Online: OECD Guidance on Policy and Practice*. 386, 2003 (Complete Edition: ISBN 9264101624) Electronic resource to subscribers found at: [http://0-puck.sourceoecd.org.bianca.penlib.du.edu/vl=4858425/cl=16/nw=1/rpsv/ij/oecdtthemes/9980096/v2003n20/s1/p1](http://0-puck.sourceoecd.org.bianca.penlib.du.edu/vl=4858425/cl=16/nw=1/rpsv/ij/oecdtthemes/9980096/v2003n20/s1/p1). Last Accessed 03 April 2009. The OECD guidance was created to respond to accelerated technological change and globalization, changes that create new challenges and opportunities for governments, businesses and the general public. The increasing use of online communication over public networks drew attention to privacy as a fundamental social value that concerns one and all. OECD countries recognized the need for comprehensive and consistent policies that build confidence in the online world and made it possible to develop its potential for economic and social well-being. This electronic volume draws together more than four decades of OECD work on measures for ensuring effective privacy protection on global networks while continuing to allow the trans-border flow of personal data. It argues for a blend of regulatory and self-regulatory approaches, including legal, technical and educational solutions, suited to the cultural and social context in which they operate. It draws attention to the need for the committed, complementary and co-operative involvement of all actors in society. The book contains specific policy and practical guidance to assist governments, businesses, and individuals in promoting privacy protection online at national and international levels. It proposes ways of adopting and posting privacy policies, mechanisms for enforcement and redress, and means of promoting education and user awareness.

Ibid., 59.


Abraham L. Newman, "Creating Privacy: The International Politics of Personal Information" (Doctor of Philosophy, University of California, Berkley, 2005), 106-117.

Ibid., 120.

Ibid., 120-121.

Ibid., 121-122.
74 Ibid., 122.


78 Ibid., 119.
Chapter Six

Analysis and Conclusion

At an early stage in the (privacy data-protection) debate, when the problems of computerization in government were first being recognized, the motivation to draw lessons from the early adopters (Sweden and the US) was strong, and thus the same transnational policy community emerged and coalesced. Conceptually, this process is little different from the “epistemic communities” identified in the international political economy literature (of Peter Haas).

By the mid-1970s, however, this policy community, working within the forums of the OECD and the Council of Europe also recognized the interdependence of global communications, the incipient problem of transborder flow and the consequent need to harmonize (privacy data protection legislation).\(^1\)

Colin J. Bennett, *Understanding Ripple Effects*

Introduction

This dissertation journey began with a discussion of the concept of privacy, describing how the concept of privacy had evolved and grown from antiquity to the post-Civil War era, when technological advances in newspapers, telegraph, telephone, and individual box cameras brought changes in the concept of privacy that resulted in Warren and Brandeis “inventing privacy law”\(^2\) through their essay *The Right to Privacy*.\(^3\) For more than a half-century the privacy concepts enunciated by Warren and Brandeis grew, expanded, and were tested in courts across the United States.

The U.S. Privacy Case Study found in Chapter Four describes the burst of technological innovation in computers, databases, and surveillance that followed the
Second World War and created a threat to individual privacy that galvanized privacy concerns across the nation and promoted the creation of the nascent privacy data-protection epistemic community. It is the existence, growth, and influence of that privacy data-protection epistemic community, first in the United States and then in the European Union, that has been the focus of this research. In the remainder of this chapter I will analyze evidence from the two case studies and the epistemic community literature and respond to the three research questions posed in Chapter One:

1) Does a (single) privacy epistemic community exist?

2) Did the privacy epistemic community influence privacy legislation in the United States and the European Union?

3) With the influence of a single privacy epistemic community, why was the resulting policy and legislation so dramatically different in the United States (Privacy Act of 1974) and the European Union (Directive 95/46/EC On the Protection of Personal Data)?

Evidence Addressing the First Research Question:
Does a single privacy epistemic community exist?

Employing the criteria identified in Chapter Three and evidence found in the Chapter Four and Chapter Five Privacy Case Studies regarding process, influence, and U.S.-EU policy-legislative outcomes we find both direct and indirect evidence of the existence of the privacy data-protection epistemic community.

Based on the six objective criteria identified in Chapter Three, a single privacy epistemic community has existed for at least four decades. Our six objective criteria were: 1) Recognized professional/technical expertise or “standing” in privacy issues; 2) Privacy publications; 3) National and international organizations with a privacy component; 4) Privacy websites on the Internet (after the Internet was established);
5) Periodic privacy conferences; and, 6) Participation in government hearings, testimony, and other legislative meetings.

The U.S. Privacy Case Study in Chapter Four and the EU Privacy Case Study in Chapter Five provide the following evidence regarding the six criteria by which I confirm the existence of the privacy data-protection epistemic community.

1) Recognized Professional/Technical Expertise or “Standing” in Privacy Issues

From the late 1950s, individuals can be identified who were recognized for their professional/technical expertise or “standing” in privacy issues, and who subsequently became active participants in the privacy data-protection epistemic community. Identified in the U.S. Privacy Case Study in Chapter Four were individuals such as Willis Ware of the RAND Corporation, who was one of the first to recognize and write about the threats of computers, databases, and surveillance to the citizen. Other privacy epistemic community members introduced in the two case studies who established their professional/technical credentials and played important roles in influencing privacy data-protection policy and legislation include Alan Westin, Arthur Miller, Lewis Branscomb, Robert Gellman, James Rule, Marc Rotenberg, David Flaherty, George Trubow, David Burnham, Robert Ellis Smith, Evan Hendricks, Spirios Simitis, Frits Hondius, Hans Peter Bull, Jan Freese, and Paul Sieghart.

2) Privacy Publications

Privacy publications have been authored by most privacy epistemic community members as a means of establishing their professional and technical expertise or “standing” on privacy issues within the community. For example, as noted in Chapter
Four, Willis Ware authored 77 studies and reports between 1953 and 2008, of which 33 contain the words security or privacy in the title, and most address both security and privacy.\(^4\) Alan Westin has been a prolific author of privacy literature and studies,\(^5\) to include classics in the privacy literature such as *Privacy and Freedom*,\(^6\) and *Databases in A Free Society*. Arthur Miller secured his privacy credentials with *The Assault on Privacy: Computers, Data Banks, and Dossiers*, in 1971.\(^7\) Robert Gellman has been a prolific author and commentator on privacy issues in journal articles, essays, and Congressional Legislative Reports.\(^8\) The sociologist James Rule has authored books on privacy such as *Private Lives and Public Surveillance: Social Control in the Computer Age*,\(^9\) *The Politics of Privacy*,\(^10\) *Privacy in Peril*,\(^11\) and *Global Privacy Protection: The First Generation*.\(^12\) Marc Rotenberg, a law professor at Georgetown Law School and Executive Director of the Electronic Privacy Information Center (EPIC), has co-authored and edited privacy books with other privacy epistemic community members such as Daniel Solove, Paul Schwartz, and Phillip Agre to include *Information Privacy Law*,\(^13\) *Privacy, Information, and Technology*,\(^14\) and *Technology and Privacy: The New Landscape*.\(^15\) David Flaherty authored two classics in the privacy literature, *Privacy in Colonial New England*,\(^16\) and *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*.\(^17\) Professor George Trubow was the director of the Center for Information Technology & Privacy Law and oversaw publication of the *Journal of Computer & Information Law* at The John Marshall Law School.\(^18\) David Burnham covered privacy issues as a journalist and became a privacy epistemic community member, authoring *The Rise of the Computer State*.\(^19\) Robert Ellis Smith, lawyer, expert witness on privacy, and publisher of *Privacy*
Journal has authored numerous journal articles and books, to include the privacy history:

*Ben Franklin’s Website: Privacy and Curiosity from Plymouth Rock to the Internet*. 20

Since 1981, Evan Hendricks has been the Editor/Publisher and founder of *Privacy Times*, a Washington, D. C.-based newsletter and has published nearly 3,000 pages covering a wide range of privacy and information law subjects. Spirios Simitis, German jurist, Data Protection Commissioner, and Chairman of the Council of Europe’s Experts Committee on data protection has authored numerous essays on privacy issues. 21 The life-long German privacy expert Frits Hondius authored the earliest survey of privacy in Europe, *Emerging Data Protection in Europe*, in 1975. 22 Jan Freese, Director General of the Swedish Data Inspection Board, authored *The Computerization of Society*, 23 describing the growing reliance on computers by all sectors of society. This overview of some of the key privacy epistemic community members supports the finding that publication of privacy books and essays has been an important means of establishing professional and technical expertise or “standing” on privacy issues within the community.

3) National And International Organizations With a Privacy Component

As noted in the case studies in Chapters Four and Five, the central organizations with a privacy component that facilitated networking for the privacy data-protection epistemic community were the Council of Europe and the Organization for Economic Cooperation and Development (OECD). The privacy components within these two organizations were the Committee of Experts on Data Protection 24 and the Working Party on Information Security and Privacy (under the auspices of the Committee for Information, Computer and Communications Policy 25) respectively. Additionally, dozens of organizations facilitate networking, communication, and education on privacy
issues, problems, policies, and legislation. See Appendix A for an overview of key organizations with a privacy component.

4) Privacy Websites on the Internet

Privacy websites on the Internet are an important tool for communication, education, and networking among members of the privacy epistemic community. The Internet has enabled a multitude of permanent privacy epistemic community fora to network, educate, and inform the global privacy epistemic community on a nearly infinite list of privacy-data protection topics, issues, and events. Through the Internet, the privacy epistemic community has become a truly permanent and ubiquitous presence at dozens of highly developed and active sites that focus on privacy-data protection issues. See Appendix B for privacy websites associated with dozens of privacy organizations.

5) Privacy Conferences

Privacy conferences are important networking opportunities for members of the privacy data-protection epistemic community. Members of the single trans-Atlantic privacy data-protection epistemic community regularly network at international conferences such as the Annual Conference of Data Protection Commissioners, initiated in 1979 and now in its 31st year, the British sponsored International Conference on Privacy Laws and Business, and the Computers, Freedom and Privacy Conferences held in the United States. Bennett notes that: “Scholars of international relations would conclude that a cross-national epistemic community had coalesced by the end of the 1980s.” Academic institutions of higher learning and law schools also frequently
sponsor conferences and symposia on privacy.\textsuperscript{32} See Appendix C for selected privacy data-protection conferences.

6) Participation in Government Hearings, Studies, Testimony, and Other Legislative Meetings

As noted in the case studies in Chapters Four and Five, members of the privacy epistemic community regularly participate in government hearings, studies, and legislative meetings, providing their expertise in privacy issues to decision makers and legislators. For example, Willis Ware chaired the Health, Education and Welfare (HEW) Secretary’s Advisory Committee on Personal Data Systems in 1972; Arthur Miller was a member of the same Secretary’s Advisor Committee, as well as a subject matter expert in many other privacy hearings; Alan Westin testified at numerous privacy hearings and chaired several privacy studies, to include Databanks in a Free Society, National Academy of Sciences Study on Computers, Record-Keeping and Privacy\textsuperscript{33}; and David Flaherty, likewise has testified at privacy hearings. Specific privacy epistemic community members’ participation in key privacy hearings and studies are discussed in more detail in the case studies found in Chapters Four and Five.

\textbf{Evidence Addressing the Second Research Question:}

\textit{Did the privacy epistemic community influence privacy policy and legislation in the United States and the European Union?}

As shown in the case studies in Chapter Four and Chapter Five, the influence of privacy data-protection epistemic community members was woven throughout the studies, hearings, reports, and discussions preceding the adoption of privacy legislation in
the United States and the European Union. Beyond the involvement in important privacy
hearings and critical privacy studies described in the two case studies, evidence of their
influence comes from statements attesting to their influence. For example, the influence
of the U.S privacy data-protection epistemic community in sensitizing Europeans to the
issues of privacy was professed by Frits Hondius, when he observed that:

A factor of considerable influence was the development of data
protection on the American scene. Almost every issue that arose
in Europe was also an issue in the United States, but at an earlier
time and on a more dramatic scale. It should be remembered that
the modern notion of privacy, around which the debate on
computers and personal freedom was centered, is basically
American in origin.34

Additional recognition for the influence of the privacy data-protection epistemic
community on the privacy policy and legislative process is found in the literature of
privacy data-protection epistemic community members such as Bennett, who states:

At an early stage in the (privacy data-protection) debate, when the
problems of computerization in government were first being
recognized, the motivation to draw lessons from the early adopters
(Sweden and the US) was strong, and thus the same transnational
policy community emerged and coalesced. Conceptually, this process
is little different from the “epistemic communities” identified in the
international political economy literature (of Peter Haas).

By the mid-1970s, however, this policy community, working within
the forums of the OECD and the Council of Europe also recognized
the interdependence of global communications, the incipient problem
of transborder flow, and the consequent need to harmonize (privacy
data protection legislation).35

While Bennett actually identifies the process by which privacy data-protection
experts coalesced into an epistemic community, other such as Burkert, describe rather
specifically how members of the privacy epistemic community acted to influence the
privacy data-protection policy and legislation. As this influence was described by Burkert:

Epistemic communities are—in the words of Braithwaite and Drahos—“loose collections of knowledge-based actors who share certain attitudes and values and substantive knowledge, as well as ways of thinking about how to use that knowledge.” It had been a relatively small group of such actors—their names are now inscribed in the hall of fame of data protection—who had helped to transform data protection from a scholarly concept into an operational regulatory concept. These persons appeared and re-appeared whenever a national government or international institutions were discussing data protection. In their testimonies they could mutually reinforce their arguments, refer to each other’s authority and succeeded in establishing an international state of the art for data protection regulation.  

**Fair Information Practices**

One of the indirect indicators of the influence of a privacy epistemic community on privacy policies can be found by examination of the similarities or common concepts found in declarations of “first principles” of individual privacy data-protection, often expressed as fair information practices (or principles) (FIP). Codes of fair information practice were advanced by U.S. and European privacy study groups and NGO expert committees as guides to the principles that underlie individual privacy in an age of advancing digital technology. Privacy scholars find a remarkable similarity and consistency in the ‘basic rules’ of privacy data-protection principles found in these FIP.
Table 6.1 Fair Information Practices/Principles (FIP) Sources

<table>
<thead>
<tr>
<th>Year</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1972</td>
<td>Report on the Younger Committee on Privacy (First FIP)</td>
</tr>
<tr>
<td>1973</td>
<td>Council of Europe Resolution (73) 22 On The Protection Of The Privacy Of Individuals Vis-À-vis Electronic Data Banks In The Private Sector, 26 September 1973.</td>
</tr>
<tr>
<td>1974</td>
<td>Privacy Act of 1974 (Incorporated FIP)</td>
</tr>
</tbody>
</table>

The United States and the EU have both subscribed to very similar FIP concepts of privacy safeguards and privacy outcomes that are needed to protect the privacy of their citizens. See Appendix D to compare FIP text from key privacy documents of the 1970s and 1980s and note the similarities. Many scholars observe that, although the language and the number of individual items in these fair information practice collections vary, the content of the fair information practice codes are all remarkably similar. This broad consistency in fair information practice may be attributed to the presence of the privacy epistemic community that informed and educated policymakers across the North Atlantic community.

Finally, although not specifically employing the phrase “privacy data-protection epistemic community,” the influence of epistemic community members has been identified by scholars though the process was described in other terms:
Evidence Addressing the Third Research Question:

Why did the influence of the privacy epistemic community result in dramatically different privacy legislation in the United States (Privacy Act of 1974) and the European Union (Directive 95/46/EC On the Protection of Personal Data)?

The U.S. Privacy Case Study in Chapter Four and the EU Privacy Case Study in Chapter Five focus on the influence of the privacy epistemic community in privacy policy and legislation. However, since the policy and legislative results were so different in the U.S. and the EU, it is necessary to determine what other intervening variables could be at work in influencing decision makers. The epistemic community literature suggests that there are three additional intervening variables that enter into policy and legislation decisions: 1) economic considerations; 2) socio-cultural considerations; and, 3) political considerations. I will review each of these intervening variables in turn.

A Framework for Analysis

As an aid in analyzing the economic, socio-cultural, and political factors that have been put forth in the literature attempting to explain why, given the common antecedents and understanding of the technological threat to privacy, that privacy legislation in the United States and the European Union have evolved so differently, I have adapted for my
discussion the graphic of a four-sided “diamond” similar to those often invoked in analysis of comparative politics. These four dimensions are best visualized in the four-sided graphic below, depicting the influence of the Privacy Data-Protection Epistemic Community, Economic, Social-Cultural, and Political considerations on the privacy data-protection policy and legislative process in the United States and the European Union.

**Figure 6.1: A Framework for Analysis**

Privacy Data-Protection Legislation Influences

Intervening Variables in the Public Policy Process

The importance of intervening variables has been recognized in comparative policy studies for more than four decades. Policy studies across the states of the United States as well as in cross-national studies, have suggested that: “policy differences . . . might be more strongly influenced by “environmental” variations (those outside the political system, such as economic conditions) than by various aspects of politics.” Prominent models of the policy process all include outside intervening variables in the form of “external conditions,” “Socioeconomic variables,” Environmental (inputs),
or “historic-geographic conditions” and “Socioeconomic Composition.” Blomquist notes that the models of the policy process “. . . are variants on systems theory: An external model influences a political system that produces policies that feed back into the environment.” Thus, the external influences, or intervening variables, become important determinants of policy outcomes in the public policy decision models.

Numerous comparative policy studies have shown that “. . . policymakers are constrained by a host of conditions over which they have limited control . . .” and that “. . . a valid account of the policy process will have to be more complex than might have otherwise been anticipated.” The complexity of the policy process recognizes the many “attributes of the community” involved in policy making, as well as the fact that many empirical studies show “. . . that culture and economic conditions affect the possibilities in and constraints upon policymaking.”

In spite of the significant role attributed to environmental intervening variables in the policy process, Blomquist observes that: “an empirical theory of the policy process that does not center upon human agency is unlikely to be able to explain much of what transpires.” In this study the “human agency” dynamic focuses on the privacy data-protection epistemic community, and the different policy outcomes achieved in the United States and the European Union when confronting different economic, socio-cultural, and political intervening variables.
Evidence of Economic Intervening Variables

Economic Impact of the U.S. Privacy Act of 1974

In the United States, concerns were voiced over the economic impact of privacy legislation on business and economic activity from the earliest consideration of privacy legislation by Congress. As described in Chapter Four, a strong U.S. business community voiced concern over the time and money resource costs of complying with restrictive privacy laws with government oversight. Such concerns helped to blunt the efforts of the privacy epistemic community to achieve a broader privacy protection law that they generally advocated. The U.S. enacted a narrow, “sectoral” law in the Privacy Act of 1974 that focused on government computer and database practices while trusting business and the private sector to self-regulate in accordance with fair information practices/principles. The effect of the Privacy Act of 1974 on business and the U.S. economy was therefore minimal because:

The North American response to private sector data protection issues has so far been to rely on an assumption that if consumers are concerned about personal privacy, their concerns will be reflected in complaints and a preference for businesses with more privacy-friendly practices. Voluntary codes of practice (based on the OECD Guidelines of 1981) have been the typical manifestation of the corporate response.60

Economic Aspects of EU Data Protection Directive

Arguments regarding economic motivations that may have influenced the European Union to adopt an omnibus data-protection law have been offered ever since the European Data Protection Directive was enacted. Most criticism is based on the perceived business advantages that would accrue to European firms in the computer-
based database market if the United States were shown to offer inadequate protection of personal data.61

For the past six decades the United States has been the dominant presence in the global computer services market, and “. . . information services and products are either the first or second largest sector of the U.S. economy, accounting for between ten and twelve percent of Gross Domestic Product.”62 The European nations have been at a disadvantage in both the technology of computers and the application of computer technology in database management in such business areas as banking, finance, and marketing. “The EU data protection Directive threatens U.S. leadership in the information economy and is heightening U.S. concern over protecting that so-called dominance. Some critics see the Directive as merely the newest in a series of European attacks on profitable U.S. information and programming industries.”63 Imposition of a restrictive privacy directive that privileged the EU nations at the expense of the United States would be a powerful equalizer in the international competition for computer and computer-related data business. At the very least, the EU Data Protection Directive would exclude the United States firms from the EU computer services market by virtue of the United Stateselecting to take a looser, sector-oriented response to data privacy that was not deemed “adequate” for protection of individual data by the EU.

Privacy scholars point to the economic factors that allegedly gave the British the impetus for enacting their Data protection Act of 1984. The British computer industry presented a compelling argument that in the absence of British data protection legislation computer hardware and software manufacturers and the computer-based service sector would be adversely affected. “Personal data protection could become a legal pretext for
trade protectionism, leading to the isolation of the British data processing industry and of other service sectors of the economy that rely on unimpeded communications." Bennett concludes that: “In the final analysis, the British Data Protection Act of 1984 was passed for economic rather than for civil libertarian reasons.”

Some scholars suggest that the EU has established a privacy data-protection law in 95/46/EC that effectively creates a de facto information and data-services “regime” that will “create extra benefits that can be divided amongst EU member states, and thus there is a strong economic incentive to become more effective in projecting EU preferences in international regimes.” The chief concern is that the EU Data Protection Directive becomes a vehicle for computer and data services trade protectionism that could restrict competition from the United States and other countries based on what the EU would claim to be inadequate privacy data-protection.

More that a decade after the 95/46/EC EU Data Protection Directive entered into force the economic impacts of the law are still the subject of discussion in academic literature, but there is no significant evidence that economic disruptions in the U.S. computer and data services industries have taken place. The Safe Harbor Agreements have become the procedural “fix” by which individual U.S. firms agree to abide by the privacy data-protection requirements of the European Union. Thus, it appears that economic influences, while a cause for concern, have not materialized as a significant motivation for the 95/46/EC European Data Protection Directive.

Evidence of Socio-Cultural Intervening Variables

Although there are many similarities between the social and legal systems of the United States and the European Union, and both the U.S. and the EU agreed on similar
fair information practices/principles and the same CoE convention and OECD guidelines, some privacy scholars suggest that different social and cultural traditions were the source of the conflict between privacy policies and legislation between the two.\(^71\) These social-cultural differences are cast in different terms based on the perspective of the authors, but generally they revolve around 1) privacy as an aspect of *dignity* versus privacy as an aspect of *liberty*;\(^72\) or 2) the *social protection* approach versus the *liberal philosophy* of privacy.\(^73\)

That the Europeans focus on *dignity*, while the American focus on *liberty*, is not unique to the rather recent discussion of privacy, but has been identified for more than a century as based on inherently different views of the world. Whitman suggests that these basic differences in social, political, and legal traditions condition citizens of the United States and citizens of the European nations to value much different dimensions of privacy. For example, Whitman says:

> Continental privacy protections are, at their core, a form of protection of a right to respect and personal dignity. The core continental privacy rights to one’s image, name and reputation, and what Germans call the right to informational self-determination---the right to control the sorts of information disclosed about oneself. These are closely linked forms of the same basic right: they are all rights to control your public image—rights to guarantee that people see you the way you want to be seen . . . . The prime enemy of our privacy, according to this continental conception, is the media, which always threatens to broadcast unsavory information about us in ways that endanger our public dignity . . . On the Continent, the protection of personal dignity has been a consuming concern for many generations.\(^74\)

The European focus on *dignity*, Whitman suggests, is significantly different than the American focus on *liberty*, and especially liberty against the state. This, he says,
accounts for the different policies and laws created in Europe after decades of agreement on the first principles of privacy. America, Whitman says:

... is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the eighteen century: It is the freedom from intrusions by the state, especially in one’s own home . . . . American anxieties thus focus comparatively little on the media. Instead they tend to be anxieties about maintaining a kind of private sovereignty within our own walls.\textsuperscript{75}

Reidenberg also argues that socio-cultural differences between the United States and the European nations account for differences in implementation of privacy policy and law. Both the United States and the European nations agreed to essentially the same “first principles” of privacy, or fair information practices. These fair information practices (or principles) were cooperatively drafted by privacy epistemic community members from the United States and the European nations in the Council of Europe Convention and the OECD Guidelines. Yet he too notes that the policies and laws that form the regulatory structure for privacy in the United States and the European Union focus on much different dimensions of individual privacy.

Like Whitman, Reidenberg identifies American law as based on a liberal 
philosophy, but characterizes the European philosophy as based on a social protection paradigm. The American liberal philosophy “emphasizes limits on government power and is characterized by its hostility toward regulation of private relations . . . . For privacy, the liberal approach prefers private rights and regards the state with suspicion.”\textsuperscript{76} Because the liberal philosophy focuses on the power and intrusion of the state, the power of the state is to be restricted as much as possible, and therefore the sectoral approach to
privacy law is naturally chosen. “Sectoral rather than omnibus laws minimize state intrusions on information processing. Sectoral laws . . . react to specific problems and provide only narrow state intervention to protect privacy. For information privacy, this also means that the public sector and police powers, rather than private conduct, are suspect.”77 This liberal American sentiment is echoed by Bennett, who asserts that the U.S. choice of a limited or sectoral response to the threat to privacy can be attributed to a long-standing culture based on distrust of government. “Fear of over powerful government is deeply ingrained in the American political experience. This fear is reflected in the fragmented and decentralized distribution of authority in American government, in the Madisonian tradition of checking the power of “faction,” and in the “Lockean liberal consensus.”78

The contrast to the American liberal philosophy, under the European social protection philosophy:

. . . public liberty derives from the community of individuals and law is the fundamental basis to pursue norms of social and citizen protection. This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop, and information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights.79

Thus, there are dramatic differences in the regulatory socio-cultures of the United States and Europe that are far broader than the different information cultures displayed in privacy data-protection policy and legislation conflict. The privacy-data-protection is just one of several areas in which the United States and Europe have a conflict of visions regarding the roles of the state and the private sector. Scholars in environmental, safety, and industrial regulatory disciplines echo observations regarding American and European
philosophical differences that have influenced the creation of dramatically different regulatory policies, practices, and laws. In their study, *Controlling Chemicals*, Brickman, Jasanoff, and Ilgen suggest that there has been a long history of policy-making, legislative process, and regulatory enforcement differences between Europe and the United States. Others, such as Lofstedt and Vogel, descriptively note the differences in consumer and environmental regulation between the United States and Europe in their analyses, but do not attribute those differences to socio-cultural factors.

Based on the observations of scholars from several disciplines in identifying different socio-cultural visions of the role of the state relative to the citizen in the United States and European nations, the role of the socio-cultural intervening variable in influencing privacy data-protection policy and legislation appears to have validity. In the words of Wright: “What we must acknowledge . . . is that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy.”

**Evidence of Political Intervening Variables**

In seeking evidence of a political intervening variable one must entertain the following two questions: 1) What political factors may have prompted the United States to enact the Privacy Act of 1974 at the time that it did? And, 2) What political factors may have prompted the European Union to enact the European Data Privacy Directive 95/46/EC at the time that it did?

**Evidence of Political Factors in the United States:**

As discussed in the Chapter Four case study, the political environment of the early 1970s conditioned politicians to see the need for immediate enactment of privacy
legislation. The Watergate scandal of the Nixon Administration, which began in June of 1972 and ended with the resignation of President Nixon in August, 1974, sensitized the nation to the issues of government surveillance, eavesdropping, and burglary and generated numerous bills in Congress to restrict wiretapping and surveillance. Congress and the public were shaken by the revelations of Executive Branch involvement in patently illegal activities and were concerned that the press was revealing only the “tip of the iceberg.” Hearings into privacy abuses of the Nixon Administration revealed a “trend toward privacy invasions” and the need to “reassert the right of the individual to be free of Government surveillance.” Thus, the investigations and hearings of the Watergate Scandal created a powerful political expedient to enact legislation to limit government ability to intrude into the privacy of individual citizens and opened a policy window for privacy legislation. After nine years of privacy hearings, studies, reports, and bills, public concern and a motivated Congress expedited privacy legislation. In just a few months in Fall 1974, the Privacy Act moved through Congress and was signed into law by President Gerald Ford on January 1, 1975. As the first, and broadest, of much subsequent privacy legislation passed over the subsequent decade, the Privacy Act of 1974 became an important benchmark in U.S. privacy legislation.

**Evidence of Political Factors in the European Union**

As described in the Chapter Five case study, the political environment of the early 1990s put political pressure on the European Community to harmonize data-protection by means of a uniform data-protection law. Three data-protection events occurred in late 1989 that clearly demonstrated the problems associated with transborder data flows in an environment of uneven (or no) data protection law that would preclude the planned
integration of European nations in the Internal Market. In July 1989, the French Data Protection Authority (Commission Nationale de l’Informatique et des Libertés or CNIL) threatened to block data transfers of employees between Fiat’s corporate offices in France and in Italy. The CNIL argued that Italy’s data privacy rules were inadequate to protect the data, and therefore personal information about French citizens could not be transferred. Fiat Italy was forced to find a solution to the refusal of the CNIL to allow the transfer of data. Resolution of the impasse came when Fiat Italy signed a data protection contract in which it agreed to protect personal data coming from Fiat France in accordance with CNIL rules. This first episode clearly demonstrated how conflicting national data protection rules could perturb routine business activities between nations.87

A second data transfer event took place just two months later, in September 1989, when the CNIL blocked the plans of the Gustave Roussay Institute, a French cancer research center, to join the Belgian-based European Organization for Research and Treatment of Cancer (EROTC). The CNIL pointed out that Belgium did not have national data protection legislation in place, and therefore the Gustave Roussay Institute could not send sensitive medical data to Belgium until such legislation was enacted by Belgium.88

A third imbroglio took place over the Schengen Agreement for free movement of persons and labor among Germany, France, Belgium, Luxembourg, and the Netherlands. In order to secure the new external border encompassing these members to the agreement, a Schengen Information System (SIS) was proposed to network the existing border control and national customs databases so as to allow mutual policing of national borders. The Germans and French raised the issue that Belgium did not have a data
protection law with the result that data protection experts from France, Germany, and Luxembourg objected to the violation of their national data privacy laws by sharing sensitive police information with Belgium. Only after Belgium bowed to pressure from the data protection community and pledged to expedite data protection legislation, were the data protection clauses and monitoring authority for the SIS developed.89

With the increasing frequency of data protection issues arising within the community, the European Commission was forced to act if the creation of the EC Internal Market was to be realized in 1992. Recognizing that the Internal Market could never be achieved without uniform data protection law across all member nations, the Internal Market Directorate became the focal point for the creation of the first draft of EC data privacy legislation. Data protection commissioners took an active part in drafting and amending data protection legislation. After review, oversight, and amendment of proposals by data protection commissioners---through three major revisions---accommodation among the parties was finally reached on the structure of data protection legislation. Thus, the timing of the integration of nations into the European Internal Market in 1992 put political pressure on the EC and individual nations to create a uniform data-protection law but has little effect on the content of the law.90

**Influence of the Three Intervening Variables**

While each of the three intervening variables, economic, socio-cultural, and political, obviously influenced the privacy data-protection legislation of the United States and the European Union, it appears that the socio-cultural variable offers the most powerful explanation of why the United States opted for a narrow sectoral approach to privacy regulation in the Privacy Act of 1974, while the European Union enacted broad
omnibus legislation in the 95/46/EC European Data Protection Directive. The liberal philosophy, privileging the individual and the market over the state, predisposed the United States to enact narrow legislation that primarily restricted the ability of the state to invade the privacy of the individual. In Europe, the socio-cultural focus on dignity and social protection inclined legislation that broadly protects the individual citizen’s image, name, and reputation.

As shown in the case studies, economic motives and influences in the United States were supported by the limited impact of the Privacy Act of 1974 in that the legislation did not impose significant new requirements or costs on business and industry. In Europe, business interests opposed broad data-protection legislation because of the obstacles to customer data processing and the significant increases in costs that data-protection would entail. However, the lessons of the several data-transfer problems among nations, and the pressure to create a uniform information environment prior to national integration into the Internal Market prompted their concerns to be subordinated to the common enterprise of market integration and unification. More than a decade after the 95/46/EC European Data Protection Directive went into force, it is probably safe to say that concerns that Europe was creating a “regime” based on restrictive data-protection law that would economically disadvantage U.S. international information services was ill-founded. Data-transfer under the Safe Harbor agreements has ameliorated most economic impacts to the U.S. computer and information service industries.

Evidence of political intervening variables shows that in the cases of both the United States and the European Union, political influences determined the “when” but not the “what.” In both cases political pressures and influences accelerated policy
decision processes that were already underway, but moving slowly. In the United States, the pressures of the Watergate Scandal and the revelations regarding government burglary, wiretapping, and surveillance prompted immediate legislation. In Europe, the need for common, harmonized, data-protection law prior to national integration into the Internal Market prompted action to enact the 95/46/EC European Data Protection Directive.

**Implications for Further Research**

This comparative analysis of the influence of the global privacy epistemic community on the privacy data-protection policy/legislative responses of the United States and the European Union leaves several important questions unanswered. The wide divide between the legislation enacted by the United States and the European Union suggests follow-on research regarding the constraints and benefits inherent in each of these two approaches to protecting the privacy data-protection of citizens.

Of interest would be the identification and analysis of the strengths and weaknesses of these two policy/legislative approaches to ensuring individual privacy. Can the limitations of privacy data-protection be shown to privilege or impair the information service industry of either the United States or the European Union? Are other nations choosing to emulate the policies and legislation of the United States or the European Union? Now that more than a decade has passed since the European Data Protection Directive entered into force (1998), are perceptible privacy data-protection alliances or allegiances identifiable that could be characterized as a privacy data-protection “regime?”
Conclusion

This, the first comparative study of the influence of the privacy data-protection epistemic community on privacy policy and legislation in the United States and the European Union, is important because it validates the epistemic community approach as an important method of analyzing policy processes and outcomes. As noted in Chapter One, the epistemic community approach is one of several policy approaches that offers strong explanatory power in policy and legislative realms requiring expert knowledge.

However, several problems in the application of Haas’ epistemic community approach require the researcher to rely on other attributes of epistemic community members in order to render them externally observable. Criticisms of the Haas definition of the epistemic community are correct when they identify the imputed attributes of “shared normative and principled beliefs,” “shared causal beliefs,” and “shared notions of validity” that are effectively impossible to operationalize in a research program. The lack of documentation, evidence, or the inability to ascertain these imputed “inter-subjective, internally defined criteria” and characteristics of epistemic community members, as well as the inability to gain insight into the networking activities of specific privacy data-protection epistemic community members all lead one to depend upon more objective characteristics that can be externally identified. In this study, these externally observable objective criteria are the six criteria identified in Chapter Three, that identify professional/technical expertise and competence, privacy organizations that promote the networking of the epistemic community, and opportunities to influence policy makers and legislation.
It is impossible to analyze and assess the role of the privacy data-protection epistemic community without taking into consideration the economic, socio-cultural, and political intervening variables in both the United States and the European Union. The limited success of the privacy data-protection epistemic community in achieving uniform privacy-data protection policy and legislation in both the United States and the European Union can be attributed to the economic, socio-cultural, and political intervening variables. Often characterized as environmental, external, or socio-economic by the classic comparative policy theorists, these intervening variables have been recognized as important determinants of policy and legislative outcomes in more than four decades of comparative policy studies.

The growth of the Internet over the past two decades has helped to institutionalize the privacy data-protection epistemic community by providing an ever-present global communications networking presence through which members can share, educate, and cooperate on all dimensions of privacy and data-protection. This institutionalization process promotes self-awareness among privacy epistemic community members that was not possible in the days before the Internet, and promises a stronger, more cohesive, and more dynamic privacy data-protection epistemic community in the future.
Chapter Six Notes


4 For a complete list of publications by Willis H. Ware, see the RAND site at: [http://www.rand.org/pubs/authors/w/ware_willis_h.html](http://www.rand.org/pubs/authors/w/ware_willis_h.html).


18 Professor George Trubow was director of the Center for Information Technology & Privacy Law at The John Marshall Law School. See: [http://www.jcil.org/journal/history/index.html](http://www.jcil.org/journal/history/index.html).


22 Frits W. Hondius, *Emerging Data Protection in Europe* (Oxford, UK: North-Holland, 1975), 282. Even in 1975, Hondius saw that nascent privacy issues in Europe had an American origin when he wrote: “A factor of considerable influence was the development of data protection on the American scene. Almost every issue that arose in Europe was also an issue in the United States, but at an earlier time and on a more dramatic scale. It should be remembered that the modern notion of privacy, around which the debate on computers and personal freedom was centered, is basically American in origin.”


25 See the Committee for Information, Computer and Communications Policy site at: [http://www.oecd.org/department/0,3355,en_2649_34223_1_1_1_1,00.html](http://www.oecd.org/department/0,3355,en_2649_34223_1_1_1_1,00.html).

26 See Appendix B for a listing of many of the more important privacy organizations on the Internet.
One of the best compilations of privacy-data protection online resources and URLs can be found at the Australian Office of the Data commissioner site: http://www.privacy.gov.au/links/index.html#12.


See: www.privacylaws.com/annualconference for the 2009 conference. Note the specialized sites and conference activities such as European Privacy Officer’s Network and International Privacy Officer’s Network.


Hondius, Emerging Data Protection in Europe, 6.

Bennett, Understanding Ripple Effects: The Cross-National Adoption of Policy Instruments for Bureaucratic Accountability, 227.


Ibid., 95.

Full text of Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector can be found at: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(73)22_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(73)22_EN.pdf).


For full text of OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980, see: [http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html).


50 I would like to thank Dr. Paul Viotti for the idea of this diamond design. Dr. Viotti employed a similar diamond schematic in his classes as a useful conceptual aid for evaluating the several interacting dimensions of a political regime.


57 Ibid., 220.

58 Ibid.

59 Ibid., 215.

60 Bennett and Grant, *Visions of Privacy: Policy Choices for the Digital Age*, 11.


Ibid., 440.


Ibid.


Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 1151-1221.


Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 1161.

Ibid., 1161-2.


Ibid., 1343.


Ibid. Brickman, Jasanoff, and Ilgen compare U.S., UK. French and German national regulatory processes and policies across the chemical spectrum from agriculture and food to heavy industry and toxic chemicals. They conclude that, “The task of balancing interests and striking compromises, classically a function of the legislature, is performed in Europe more often under the umbrella of the executive than in parliament. Because of this shift in function, the legislature enters the lawmaking process much later in Europe than in the United States.” (63).

Regulation, London School of Economics and Political Science, 2001), 22.; and Vogel, National Styles of Regulation: Environmental Policy in Great Britain and the United States, 325. Although Vogel describes the changes in U.S. and European risk regulatory practices, he offers no analysis of how socio-cultural factors might play into those changes. His descriptions do, however, validate differences in risk regulatory visions or paradigms held by the U.S. and Europe.

83 Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 1160.


85 Ibid.


87 Newman, Creating Privacy: The International Politics of Personal Information, 120.

88 Ibid., 120-121.

89 Ibid., 121-122.

Bibliography


211


Special Inquiry on Invasion of Privacy. 89th Cong., 1st Sess., 1965.


Culnan, Mary J. "How did they Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information use." *MIS Quarterly* 17, no. 3 (September, 1993): 341-363.


232


*Pavesich v. New England Life Insurance Co.* Edited by SE. Volume 50 Supreme Court of Georgia, 1905.


*Roberson v. Rochester Folding Box Co.* Edited by NE. Volume 64 NY Court of Appeals, 1902.


Soma, John T., Steven D. Rynerson, and Britney D. Beall-Eder. "An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The US/EU E-


Appendix A

Privacy Epistemic Organizations

The privacy epistemic community in the United States is made up of a diverse collection of organizations with members who profess to have an interest in, or focus on, one or more of the many ever-multiplying and evolving issues or topics associated with privacy. Individually, these organizations do not necessarily constitute an epistemic community---but as we explicated in Chapter Three---in the aggregate---and especially when acting in concert on a specific issue or problem area related to privacy---they come together to create a multi-faceted epistemic community of interest. Colin Bennett uses the generic phrase *privacy advocates* to characterize the multitude of individuals and organizations that can be found in a quick Google search for privacy advocates. In his global survey of privacy advocates, Bennett lists twenty-nine major privacy organizations that make their headquarters in the United States. (See Appendix B for a listing of these and other privacy organizations.) A quick perusal of just the organizational titles of these privacy advocacy organizations makes it obvious that, while some are very broad in their purview, others are extremely focused on one, or just a few, narrow privacy issues.

These privacy groups are an amorphous collection of academics, professionals, and laymen who generally have strong interest, knowledge, and expertise in one or more of the many privacy issue-areas. (See Table 2 below of a listing of the many issue-areas subsumed under the topic of *privacy.*) They come together when motivated by their common interest in influencing the landscape of legislation for a specific privacy issue-area or problem. For example, on Wednesday, 31 October 2007, NPR Marketplace
broadcast reported that nine privacy organizations were supporting do-not-track legislation to preclude commercial tracking of computer users online.\textsuperscript{1} Subsequent research showed that these nine organizations coalesced in advance of the Federal Trade Commission (FTC) Town Hall, “Ehavioral Advertising: Tracking, Targeting, and Technology,” held November 1-2, 2007 in Washington, D.C., and offered coordinated expert guidance supporting national computer “do-not-track” legislation for computer Internet users that would be similar to the national do-not-call legislation that has proven so successful in limiting telemarketer calls to individual’s homes.\textsuperscript{2} This type of concerted spontaneous organization from a diverse, distributed community of privacy advocates is at the heart of the privacy epistemic community concept. But how diverse and distributed is this community of privacy advocates? A survey of the recent history, missions or goals, and activities of the key privacy organizations identified by Bennett reveals significant differences in size, breadth, depth, and impact of these organizations, as well as differences in their individual abilities to participate as a member in a privacy epistemic community, seeking to influence privacy regulations or legislation.

**The American Civil Liberties Union (ACLU)**

The American Civil Liberties Union (ACLU) is the oldest of the privacy advocates identified by Bennett. Founded as a nonprofit, nonpartisan organization by several civil liberties activists in 1920 to focus on limiting the power of government and ensuring individual rights, privacy is today one of the four key freedoms that the ACLU seeks to protect and guarantee, along with First Amendment rights, the right to equal protection under the law, and the right to due process under the law.\textsuperscript{3} Today the ACLU
boasts of a physical presence in every state of the United States, one-half million members and supporters as well as involvement in over six thousand civil liberties-related court cases annually. While the ACLU website presents a wide collection of civil liberties issues in which the organization is involved, this study is specifically interested in privacy issues that the ACLU finds compelling. Under Privacy and Technology the ACLU website lists ten major privacy issue areas, to include: Anonymity on the Web; Biological Technologies; Consumer Privacy; Internet Free Speech; Internet Privacy; Medical Privacy; Scientific Freedom; Students (Privacy); Surveillance & Wiretapping; Workplace Privacy; and General (Privacy). In addition to privacy subject-matter areas, the ACLU provides privacy publications, fact sheets, legal documents, legislative documents, and other privacy-related resources as a means of educating and recruiting support for privacy issues. Clearly the size and diversity of the ACLU makes the organization a important participant in educating, supporting and influencing privacy issues and privacy legislation in the United States.

**Californians Against Telephone Solicitations (CATS)**

Californians Against Telephone Solicitations (CATS) represents itself to be a single-issue privacy organization that focuses on stopping telemarketers from invading the privacy of California state citizens by telephone calls and junk faxes. The web site provides contact information for the National Do Not Call Registry, copies of Federal Laws regulating telemarketers, selected court decisions having to do with violation of the Telephone Consumer Protection Act (TCPA), extracts of the TCPA as well as FCC regulations that augment and operationalize the TCPA, and personal blogs and
information provided by visitors to the CATS site regarding their success or failure in thwarting telemarketers.\textsuperscript{5} This particular privacy advocacy site focuses on how to defeat telemarketers and telephone solicitors and would presumably only join an epistemic community if its narrow field of interest.

**The CATO Institute (CATO)**

The CATO Institute (CATO) advertises “Individual Liberty, Free Markets, and Peace” as the focus of its organization.\textsuperscript{6} Founded in 1977 as a not-for-profit public policy research foundation, the CATO Institute lists five issue-areas under the heading of Telecom, Internet and Information Policy. These five issue-areas are Free Speech and Technology; Internet Governance and Regulation; Telecom Regulation; Intellectual Property; and Privacy Issues.\textsuperscript{7} Although privacy issues appear to be embedded in many of the studies, white papers, articles, and speeches found under the first four issue-areas, the Privacy Issues page presents a collection of book extracts, articles, studies and speeches on privacy issues dating as far back as 1995.\textsuperscript{8} While many of the studies and articles found under Privacy Issues are attributed directly to the CATO Institute and its Director, Jim Harper, many others indicate that they were written by the extended CATO staff for publication in popular print media. The diversity of privacy subjects and issues appears to indicate that the CATO Institute has a long-standing interest in, and commitment to, contributing to the dialogue and education of the broader privacy community as well as the general public’s desire to be informed on privacy issues. The speeches and congressional testimony files found under Privacy Issues show that the CATO Institute has played a role in educating and influencing both federal and state
congressional decision-makers regarding a wide variety of privacy issues from REAL ID to government data mining, genetic privacy, and the registered traveler program. The CATO Institute is thus positioned to be an important participant in several privacy epistemic community issue areas.

**Center for Digital Democracy (CDD)**

The Center for Digital Democracy (CDD) was founded in 2001 to ensure that the public, and public interest, were an integral part of the new evolving “digital landscape.” The founders migrated CDD from an organization they had founded ten years earlier called the Center for Media Education (CME), which focused on promoting public participation in nascent media and telecommunications issues. CME was a participant in the passage of the Children’s Online Privacy Protection Act. CDD has played a major role in influencing the Federal Trade Commission (FTC) to institute new policies governing online consumer privacy and more responsible online marketing practices. Since its founding CDD has specialized in monitoring and analyzing emerging media marketplace developments and alerting the public, policymakers, and the media to nascent issues and problems in the digital marketplace. Thus CDD has a history of educating and influencing policymakers and decision makers on privacy issues participating in an epistemic community of organizations influencing the FTC, the FCC, and Congress regarding legislation and regulations affecting privacy and the digital marketplace.
Center for Democracy and Technology (CDT)

The Center for Democracy and Technology (CDT), founded in December 1994, has a history of almost 14 years of promoting Internet openness and individual privacy. Originally founded as a spin-off of the Electronic Frontier Foundation, the CDT was created in response to the need to participate in a new type of advocacy role in protecting civil liberties while informing and influencing emerging legislation. The initial issue was the addition of privacy safeguards to the Communications Assistance for Law Enforcement Act (CALEA) that led to a rift over process and methods and the creation of CDT. CDT is one of the larger privacy advocacy organizations on the Internet as evidenced by both the breadth of privacy issues it represents and the number of professional or expert persons associated with the organization. The CDT declares its mission “to promote democratic values and constitutional liberties in the digital age” and brings together broad expertise in law, technology, and policy.

Attesting to the expertise and non-partisan advice (central to the epistemic community approach) was Senator Patrick Leahy’s (D-VT) statement that: “You can accept Jerry Berman’s advice and CDT’s as being more expert than partisan—very important, and too rare in this town.” CDT appears to be one of the best examples of an organization that was formed to provide expert advice to policymakers and decision makers on privacy issues and appears to come closest to being an epistemic community organization of any of the privacy advocate organizations reviewed in this study.
Coalition Against Unsolicited Commercial Email (CAUCE)

The Coalition Against Unsolicited Commercial Email (CAUCE) for North America (NA) was founded in March 2007 through merger of the earlier CAUCE US and CAUCE Canada organizations in order to better coordinate implementation of anti-spam and junk-FAX laws for all Internet users. The original CAUCE organizations were formed in 1997 and 1998 respectively as an anti-spam law group that desired to petition Congress for change of the Telephone Consumer Protection Act (TCPA) to include e-mail and junk-FAX. The CAUCE organization went global with the formation of CAUCE International, or iCAUCE, in 2002. A Google search on the term “CAUCE” shows that CAUCE now has a network of affiliate organizations around the world, including India (Asia-Pacific), several in Europe, South America, and Australia. In addition to its history of working with legislators to expand anti-spam and junk-FAX laws, CAUCE provides information and tools that help Internet users and consumers on the World Wide Web to identify and respond to spam and junk-FAX. CAUCE thus appears to serve not only the day-to-day mission of informing and assisting Internet users, but also the larger mission of influencing future Internet law by joining epistemic communities focused on enhancing the privacy of Internet consumers/users in the face of growing Web-based commercial mass marketing.

Computer Professionals for Social Responsibility (CPSR)

Computer Professionals for Social Responsibility (CPSR) describes itself on its website as:

“... a global organization promoting the responsible use of computer technology. Founded in 1981, CPSR educates policymakers and the public on a wide range of issues. CPSR has incubated numerous projects such as Privaterra, the
Public Sphere Project, EPIC (the Electronic Privacy Information Center), the 21st Century Project, the Civil Society Project, and the CFP (Computers, Freedom & Privacy) Conference. Originally founded by U.S. computer scientists, CPSR now has members in 26 countries on six continents.”

The CPSR shows a history of cooperation with other like-minded organizations in promoting a significant agenda of education, information, and influence to direct the future of information and communications technology and use around the world. Recognizing that in the present age digital communications and information technology is a global phenomena that connects all peoples via the Internet, the CPSR declares the following broad mission:

CPSR is a public-interest alliance of people concerned about the impact of information and communications technology on society. We work to influence decisions regarding the development and use of computers because those decisions have far-reaching consequences and reflect our basic values and priorities. As experts on ICT issues, CPSR members provide realistic assessments of the power, promise, and limitations of computer technology. As concerned citizens, we direct public attention to critical choices concerning the applications of computing and how those choices affect society.

By sponsoring international, national, and local projects, CPSR serves as a catalyst for in-depth discussion and effective action in key areas.

Every project we undertake is based on five principles:
We foster and support public discussion of, and public responsibility for decisions involving the use of technology in systems critical to society.
We work to dispel popular myths about the infallibility of technologies.
We challenge the assumption that technology alone can solve political and social problems.
We critically examine social and technical issues within the information technology profession, both nationally and internationally.
We encourage the use of information technology to improve quality of life.

An example of the CPSR operating within a privacy epistemic community to educate and influence was the following announcement found on the CPSR Homepage on 09 October 2008 that announced:
Clearly, the CPSR organization and membership appear to exhibit the characteristics of a privacy epistemic community member that one would expect to see regarding a collusion of activity on a common topic or issue of interest. The fourteen organizations that join with CPSR in the 11 October 2008 Freedom Not Fear Day appear to form a common privacy epistemic community of interest for these issues.
**Consumer Action (CA)**

Consumer Action (CA), founded in 1971, is a non-profit consumer education and advocacy organization that identifies privacy as one of its core areas of interest along with credit, banking, insurance and utilities. Of interest to this study are the CA activities in: 1) Advocacy and Media; and 2) Coalition Activism.

Under the heading of Advocacy and Media, CA describes its advocacy activities as: “. . . promoting pro-consumer policy, regulations and legislation and helping consumers be heard by those in power—is an important part of Consumer Action’s work. In 2004, the organization established an office in Washington, D.C., a strategic decision to create a constant presence in front of lawmakers and the national media. D.C. staff focus on credit card business practices, privacy rights, predatory lending, and telecommunications rights and access.”

Describing its broad network of community organizations and their coordinated efforts, CA says: “In an effort to mobilize widespread support for the passage of pro-consumer legislation, regulation and policy, Consumer Action is tapping its 9,000-member network of community-based organizations. Working as members of diverse coalitions, Consumer Action and participating groups amplify the voice of the consumer.”

Describing their activities in Coalition Activism, CA says: “As an active member of many formal and informal coalitions of like-minded organizations working to promote social change, Consumer Action works on a wide variety of issues including privacy, telecommunication rights, fraud prevention, fair access to financial services, pro-consumer changes to the credit card industry, anti-predatory lending, civil rights and the
needs of multicultural communities.” Their web links depict a long history of coalition building and common positions across a wide spectrum of consumer issues over previous years. Review of these coalition–building activities over the years demonstrates an epistemic community approach to educating and influencing the creation of legislation and regulations on diverse consumer issues including privacy.

**Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)**

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) is an organization that focuses on rather narrow consumer privacy interests within the much broader privacy arena. CASPIAN educates and advocates against loss of consumer and individual privacy based on market segmentation, identification, and tracking of consumer purchases over time. The use of “marketing” supermarket membership cards that establish an electronic link to individuals or families allows the collection of highly detailed purchasing, use, financial, and geographic data over time by not only the supermarket chains, but also any other organization given access to the collected data. Through the use of these supermarket cards, along with associated credit cards or bank checks, enables the collection of personal information detailing the choices, lifestyle, use patterns, financial means, and geographic locations of individuals and families. CASPIAN anticipates a growing problem with the widespread introduction and use of radio frequency identification (RFID) for all products in coming years. RFID will allow infinitely detailed automatic collection of data on individual consumer purchases, disposition, and geographic location within the next decade. The CASPIAN crusade against RFID chips is described on their recently launched Spychips site that alerts
consumers, lawmakers and companies on the inherent dangers to individual privacy posed by this new technology.23

While CASPIAN provides significant information and education for consumers, media, and lawmakers visiting their site, there is no indication of coordinated or concerted action with other privacy organizations that would constitute membership in a privacy epistemic community. There are no apparent links to other organizations or sites other than those created by CASPIAN such as the Spychips site.

**The Electronic Frontier Foundation (EFF)**

The Electronic Frontier Foundation (EFF) is a civil liberties organization founded in July of 1980 as a result of a specific intrusion on civil rights that presaged growing civil liberties problems in the evolving digital computer-based telecommunications world. Privacy is listed as one of the six major issue-areas upon which EFF focuses.24 Under the Privacy issue-area, EFF declares that:25

New technologies are radically advancing our freedoms, but they are also enabling unparalleled invasions of privacy. Your cell phone helps you keep in touch with friends and families, but it also makes it easier for the feds to track your location.

Your Web searches about sensitive medical information might seem secret, known only to you and search engines like Google. But by logging your online activities, these companies are creating a honeypot of personal information, potentially available to any party wielding a subpoena.

EFF fights in the courts and Congress to extend your privacy rights into the digital world, and supports the development of privacy-protecting technologies. Donate to EFF to help support our efforts.
And the next time you try to board a plane, watch out— you might be turned away after being mistakenly placed on a government watch list based on erroneous data.

Technology isn't the real problem, though; rather, the law has yet to catch up to our evolving expectations of and need for privacy. In fact, new government initiatives and laws have severely undermined our rights in recent years.

Privacy rights are enshrined in our Constitution for a reason — a thriving democracy requires respect for individuals' autonomy as well as anonymous speech and association. These rights must be balanced against legitimate concerns like law enforcement, but checks must be put in place to prevent abuse of government powers. The EFF description of their privacy educational and advocacy activities clearly emphasizes the role of law and congressional legislation in protecting the privacy rights of citizens in the face of growing technology that permits abridgement of privacy with ever-increasing ease. EFF is one of those fourteen organizations that came together to promote the 11 October 2008 Freedom not Fear campaign aimed at increasing awareness of the increasing surveillance of all aspects of life by both government and business. EFF appears to be a significant and active member of the privacy epistemic community in the United States.

**Electronic Privacy Information Center (EPIC)**

As indicated by its title, the Electronic Privacy Information Center (EPIC) is a public research center established in 1994 to promote public awareness of emerging civil liberties issues surrounding privacy in the digital-electronic future and other related civil liberties. The mission of EPIC includes policy research, public education, conferences,
litigation, publications, and advocacy. EPIC explicates or links to more than 130 unique privacy topics and issues under its umbrella of privacy.\textsuperscript{26}

EPIC lists eleven coalitions of which it is a member to include the Global Internet Liberty Campaign, In Defense of Freedom, Internet Free Expression Alliance, National Committee for Voting Integrity, On the Identity Trail, Privacy Coalition, Privacy International, The Privacy Site, The Public Voice, Security Framework Project, and Trans Atlantic Consumer Dialogue.\textsuperscript{27} Two of these that focus specifically on privacy issues have a considerable membership: Forty-two members in the Privacy Coalition,\textsuperscript{28} while Privacy International boasts more than a hundred privacy experts and Human Rights organizations from forty countries.\textsuperscript{29} The significant networks to which EPIC is linked imply an unusual interconnectedness that can only make the organization one of the more influential privacy organizations and an important member of privacy epistemic communities focused on specific privacy issues or topics.

**Privacy Rights Clearinghouse (PRC)**

Privacy Rights Clearinghouse (PRC) was established in 1992 with a mission of providing consumer privacy information and advocating for consumer privacy. PRC provides a variety of consumer services in educating consumers regarding the link between technology and personal privacy, assisting consumers in asserting their privacy rights, as well as assisting consumers in elevating their concerns to appropriate venues. For the purposes of this study, the most important activities in which PRC engages are to: “Advocate for consumers' privacy rights in local, state, and federal public policy proceedings, including legislative testimony, regulatory agency hearings, task forces, and
study commissions as well as conferences and workshops.”

PRC frequently joins with other privacy advocates to promote a common front in educating law-makers and advocating for important privacy issues of mutual interest. Because PRC grew out of a University of San Diego privacy project that was initially funded by the state of California, PRC has been most involved with California privacy issues and privacy legislation. However, PRC has occasionally joined with other privacy advocates to support changes to privacy legislation and regulation at the federal level. Further instances of PRC involvement with coalitions on significant privacy issues over the past decade, both within the state of California and the national level, will be provided by Beth Givens (Director) and Paul Stevens (Director of Policy and Advocacy).

Privacy Activism

Privacy Activism is a non-profit organization that seeks to educate and inform the public about the right of privacy and therefore create public demand for greater privacy safeguards in society. The Privacy Activism Front Page provides instances of Privacy Activism joining with other privacy organizations to influence regulators and legislators regarding privacy issues such as the Federal Trade Commission hearings on the “The Do Not Track List” that is intended to protect Internet users from having their online web activities tracked, stored, and used by marketers and advertising networks. No information on Privacy Activism activities has been posted to their web site since 31 October 2007 so there may be some question regarding the status of their organization.
The Privacy Journal

The Privacy Journal was founded in November 1974 in response to increasing public and privacy community interest in privacy as a result of the Federal Privacy Act and the Family Educational and Privacy Rights Act that were receiving much attention in Congress. The Privacy Journal subsequently began to publish privacy-related reference books in 1976 and began to sponsor privacy conferences to network and educate individuals and organizations interested in privacy issues. The Privacy Journal staff regularly communicates with many other privacy organizations regarding privacy issues, regulations and legislation including the Privacy Rights Clearinghouse, World Privacy Forum, ACLU, Center for Democracy and Technology (CDT), the CIPICC Ontario, Canadian privacy commissioners; the British Columbia Freedom of Information and Privacy Association, Privacy International, Dr. Alan Westin, University of British Columbia, University of Ottawa, Privacy Times, Robert Gellman, and individuals in 10 state capitals working for privacy reform. Privacy Journal has supported the Polygraph Protection Act, the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability and Accountability Act (HIPAA), state laws on protection of Social Security Numbers (SSNs), Caller ID privacy, and ID theft over the past decade; published two rankings of the states in privacy and sponsored a gathering in Providence of all privacy activists. Privacy Journal has published a variety of privacy-related reference books for the privacy movement, including a history of privacy, a directory of privacy professionals, a basic guide to privacy law, and a collection of state privacy laws.
Privacy Journal co-sponsors business-oriented privacy conferences and training sessions, have provided speakers on more than 500 occasions to trade associations and conferences, and has provided expert witnesses more than 25 privacy-related court cases. Additionally, Privacy Journal personnel routinely instruct university privacy courses in the Washington D.C. area, and brief an average of 10 news reporters a month on privacy issues. Finally, Privacy Journal participates in the Electronic Privacy Information Center (EPIC) hosted monthly privacy strategy conferences and information exchanges. These many networking and coalition-building privacy activities give the Privacy Journal entrance into several privacy epistemic communities.35

**Privacy Times**

Privacy Times, edited by Evan Hendricks since 1981, is a commercially published “Subscription-only newsletter covering privacy & Freedom of Information Law and policy. It is read largely by attorneys and professionals who must stay abreast of the legislation, litigation, and executive branch activities, as well as consumer news, technology trends and business developments. Since 1981, Privacy Times has provided its readers with accurate reporting, objective analysis and thoughtful insight into the events that shape the ongoing debate over privacy and Freedom of Information.”36 The Privacy Times web site provides links to Congressional testimony that was given by Evan Hendricks on eight occasions over the past five years but offers no indication that the Privacy Times, in the person of Evan Hendricks, enters into coalitions or epistemic communities to forward a common vision of privacy.37
Private Citizen, Inc.

Private Citizen, Inc. is a commercial membership service that promises to stop junk telemarketing telephone calls for a fee of twenty dollars and stop junk mail for a fee of ten dollars. Although there are links on the Private Citizen site to several privacy advocacy sites, there is no indication that Private citizen is actually an advocate of improved privacy or acts in concert with other organizations as an epistemic community.

Public Interest Computing Association (PICA)

The Public Interest Computing Association (PICA) could not be found as a stand-alone site through an Internet search. References to PICA, and PICA activities, dating to as early as 1987 were extant, but a web site home page was not found after several search attempts.

The Utilities Commission Action Network (UCAN)

The Utilities Commission Action Network (UCAN) is a utility “watchdog” organization located in San Diego, California whose goal is to educate, inform, and advocate for consumer rights. Although the “utilities” focus of UCAN has been on energy, gasoline, water, and telecommunications abuses, UCAN is the umbrella not-for-profit 501(C)(3) under which the Privacy Rights Clearinghouse (PRC) is hosted.

The World Privacy Forum (WPF)

The World Privacy Forum (WPF) “... is a nonprofit, non-partisan 501(C)(3) public interest research group. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of privacy. It is the only privacy-focused public interest research group conducting independent, longitudinal work. The
World Privacy Forum has had notable successes with its research, which has been groundbreaking and consistently ahead of trends. World Privacy Forum reports have documented important new areas, including medical identity theft. Areas of focus for the World Privacy Forum include health care, technology, and the financial sector. The Forum was founded in 2003 and works both nationally and internationally.\textsuperscript{40}

**Building the Epistemic Community**

This survey of key privacy organizations reveals the diversity of organizations—diversity in size, experience, size, goals and missions. Based on this diversity, one would expect that only a limited number of privacy organizations would find common interests and goals to surround any specific privacy issue, regulation, or legislation. Examples of coordinated privacy activity such as the 11 October 2008 International Action Day "Freedom not fear-Stop the surveillance mania!" and the 1-2 November 2007 Federal Trade Commission (FTC) Town Hall Meeting that focused on the privacy topic of “Ehavioral Advertising: Tracking, Targeting, and Technology,” each elicited participation by only 14 and 10 privacy organizations respectively. These 10-14 participating organizations are certainly sufficient to constitute an epistemic community for the purposes of a specific privacy issue or event. In fact, if only half that number came together to support the creation or modification of a privacy regulation or legislation it would suggest a solid case of privacy epistemic community formation.

Several characteristics related to the diversity of the privacy advocacy organizations surveyed argues for the absence of frequent formation of privacy epistemic communities to support specific privacy issues or problems. The several single-issue (or
limited-issue) privacy organizations—especially those that deal with rather concrete consumer marketing issues such as Private Citizen, Inc.—are not deeply concerned with the broader, more ethereal privacy issues that assume center-stage on the agendas of the larger privacy community members. Some privacy organizations, such as the Privacy Times, provide detailed privacy information to “attorneys and professionals who must stay abreast of the legislation, litigation, and executive branch activities, as well as consumer news, technology trends and business developments.” No mention is found at the Privacy Times website of advocacy or coalition-building for specific privacy issues, regulations or legislation—although the site does advertise Evan Hendricks as an individual expert witness in trials and before the U.S. Congress. At the same time, other privacy organizations, such as the Privacy Journal, are strong in information, education, networking, and join privacy coalitions that may occasionally be privacy epistemic communities, and advocate for improved privacy regulation or legislation. Robert Ellis Smith, publisher of the Privacy Journal, characterized the changing support within the privacy community for specific privacy issues as a case of “shifting coalitions” based on the multitude of privacy issues or concerns that have been created by new technology (and are still evolving), and the attempts by the changing coalitions to bound them by regulation or legislation.
1 See the National Public Radio (NPR) article “Do-not-track list proposed for Web” at http://marketplace.publicradio.org/display/web/2007/10/31/track_list/.


5 Ibid.

6 CATO Institute Homepage: http://www.cato.org

7 See CATO Institute, Telecom, Internet & Information Policy at: http://www.cato.org/researcharea.php?display=12


10 Center for Digital Democracy-history: http://www.democraticmedia.org/about/history

11 Ibid.


16 Chapters of CPSR are found outside the United States, including Canada, Spain, Peru, Africa, and Japan.


20 See Consumer Action (CA) at: http://www.consumer-action.org/about/articles/advocacy_media/ for a detailed discussion of CA activities and successes over the past three decades in influencing and promoting legislation and regulations benefiting consumers in the five key areas of interest to CA.

21 Ibid.

22 Consumer Action (CA) at: http://www.consumer-action.org/about/articles/advocacy_media/

23 See the RFID Nineteen Eighty-Four site created by CASPIAN at: http://spychips.com

24 Electronic Frontier Foundation at: http://www.eff.org presents a detailed discussion of the historical environment in which the EFF was founded as well as an overview of its present day activities.

25 EFF Privacy overview found at: http://eff.org/issues/privacy

26 At Electronic Privacy Information Center (EPIC): http://epic.org/privacy/default.html


28 Privacy Coalition membership at: http://privacycoalition.org/about.php


30 Privacy Rights Clearinghouse Mission & Goals at: http://www.privacyrights.org/about_us.htm

31 Telephone interview with Paul Stevens, PRC Director of Policy and Advocacy, 31/1145 Oct 08.

Privacy Activism Front Page at: http://www.privacyactivism.org/

Privacy Journal at: http://www.privacyjournal.net/

Robert Ellis Smith, Publisher of Privacy Journal, E-mail Response to Formatted Interview by George Richie on 20 October 2008.


UCAN at: http://www.ucan.org/

Telephone interview with Paul Stevens, PRC Director of Policy and Advocacy, 31/1145 Oct 08.


Privacy Times at: http://www.privacytimes.com/

Robert Ellis Smith, Publisher of Privacy Journal, Telephone Interview by George Richie on 14 October 2008.
Appendix B

Privacy Epistemic Community Organization
Internet Network Presence

The following organizations are illustrative of the global web that supports the networking of the privacy epistemic community. While some organizations have privacy issues as their primary mission, other organizations have a variety of missions, of which privacy may be only one. Privacy epistemic community members communicate, publish, research, and share information via these many organizations, promoting common privacy knowledge, beliefs, and policy enterprise. The Internet presence of privacy organizations also educates and influences the public, policy analysts, and decision-makers on privacy issues.

<table>
<thead>
<tr>
<th>Organization</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. American Civil Liberties Union (US)</td>
<td><a href="http://www.aclu.org">www.aclu.org</a></td>
</tr>
<tr>
<td>2. Amnesty International (International)</td>
<td><a href="http://www.amnesty.org">www.amnesty.org</a></td>
</tr>
<tr>
<td>3. Australian Privacy Foundation (Australia)</td>
<td><a href="http://www.privacy.org.au">www.privacy.org.au</a></td>
</tr>
<tr>
<td>4. BBBOnline, Inc. (US)</td>
<td><a href="http://www.bbbonline.org">www.bbbonline.org</a></td>
</tr>
<tr>
<td>5. Californians Against Telephone Solicitations (US)</td>
<td><a href="http://www.stopjunkcalls.com">www.stopjunkcalls.com</a></td>
</tr>
<tr>
<td>6. Canadian Civil Liberties Association (CAN)</td>
<td><a href="http://www.ccla.org">www.ccla.org</a></td>
</tr>
<tr>
<td>7. CATO Institute (US)</td>
<td><a href="http://www.cato.org">www.cato.org</a></td>
</tr>
<tr>
<td>8. Center for Digital Democracy (US)</td>
<td><a href="http://www.democraticmedia.org">www.democraticmedia.org</a></td>
</tr>
<tr>
<td>9. Center for Democracy and Technology (US)</td>
<td><a href="http://www.cdt.org">www.cdt.org</a></td>
</tr>
<tr>
<td>10. Coalition Against Unsolicited Commercial Email (US)</td>
<td><a href="http://www.cauce.org">www.cauce.org</a></td>
</tr>
<tr>
<td>Organization</td>
<td>URL</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>13. Consumers Against Supermarket Privacy Invasion and Numbering (US)</td>
<td><a href="http://www.nocards.org">www.nocards.org</a></td>
</tr>
<tr>
<td>14. Derechos Digitales (Chile)</td>
<td><a href="http://www.derechosdigitales.org">www.derechosdigitales.org</a></td>
</tr>
<tr>
<td>15. Electronic Frontier Foundation (US)</td>
<td><a href="http://www.eff.org">www.eff.org</a></td>
</tr>
<tr>
<td>16. Electronic Privacy Information Center (US)</td>
<td><a href="http://www.epic.org">www.epic.org</a></td>
</tr>
<tr>
<td>17. European Civil Liberties Network (Europe)</td>
<td><a href="http://www.ecln.org">www.ecln.org</a></td>
</tr>
<tr>
<td>20. Global Internet Liberty Campaign (International)</td>
<td><a href="http://www.gilc.org">www.gilc.org</a></td>
</tr>
<tr>
<td>21. Health Privacy (US)</td>
<td><a href="http://www.healthprivacy.org">www.healthprivacy.org</a></td>
</tr>
<tr>
<td>22. ID Theft Resource Center (US)</td>
<td><a href="http://www.IDTheftCenter.org">www.IDTheftCenter.org</a></td>
</tr>
<tr>
<td>24. Institute for the Study of Privacy Issues (CAN)</td>
<td><a href="http://www.privacynews.com">www.privacynews.com</a></td>
</tr>
<tr>
<td>25. Junkbusters (US)</td>
<td><a href="http://www.junkbusters.com">www.junkbusters.com</a></td>
</tr>
<tr>
<td>26. Liberty Coalition (US)</td>
<td><a href="http://www.tlcontheweb.com">www.tlcontheweb.com</a></td>
</tr>
<tr>
<td>27. Medical Privacy Coalition (US)</td>
<td><a href="http://www.libertycoalition.net">www.libertycoalition.net</a></td>
</tr>
<tr>
<td>29. National Consumer League (US)</td>
<td><a href="http://www.nclnet.org">www.nclnet.org</a></td>
</tr>
<tr>
<td>30. New York Surveillance Camera Players (US)</td>
<td><a href="http://www.notbored.org">www.notbored.org</a></td>
</tr>
<tr>
<td>31. Patient Privacy Rights Coalition (US)</td>
<td><a href="http://www.patientprivacyrights.org">www.patientprivacyrights.org</a></td>
</tr>
<tr>
<td>Organization</td>
<td>URL</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>32. Privacy Rights Clearinghouse (US)</td>
<td><a href="http://www.privacyrights.org">www.privacyrights.org</a></td>
</tr>
<tr>
<td>33. Privacy Activism (US)</td>
<td><a href="http://www.privacyactivism.org">www.privacyactivism.org</a></td>
</tr>
<tr>
<td>34. Privacy Exchange (US)</td>
<td><a href="http://www.privacyexchange.org">www.privacyexchange.org</a></td>
</tr>
<tr>
<td>35. Privacy International (UK)</td>
<td><a href="http://www.privacyinternational.org">www.privacyinternational.org</a></td>
</tr>
<tr>
<td>36. Privacy Journal (US)</td>
<td><a href="http://www.privacyjournal.net">www.privacyjournal.net</a></td>
</tr>
<tr>
<td>37. Privacy Laws and Business (UK)</td>
<td><a href="http://www.privacylaws.com">www.privacylaws.com</a></td>
</tr>
<tr>
<td>38. Privacy Mongolia (Mongolia)</td>
<td><a href="http://www.mongolia-property.com">www.mongolia-property.com</a></td>
</tr>
<tr>
<td>40. Privacy Times (US)</td>
<td><a href="http://www.privacytimes.com">www.privacytimes.com</a></td>
</tr>
<tr>
<td>41. Privacy Ukraine (Ukraine)</td>
<td><a href="http://www.privacyinternational.org">www.privacyinternational.org</a></td>
</tr>
<tr>
<td>42. Private Citizen, Inc. (US)</td>
<td><a href="http://www.private-citizen.com">www.private-citizen.com</a></td>
</tr>
<tr>
<td>43. Public Interest Computing Association (US)</td>
<td><a href="http://www.acm.org">www.acm.org</a></td>
</tr>
<tr>
<td>44. Seguridad en Democracia (Guatemala)</td>
<td><a href="http://www.seguridadcondemocracia.org">www.seguridadcondemocracia.org</a></td>
</tr>
<tr>
<td>45. TRUST.e (US)</td>
<td><a href="http://www.truste.com">www.truste.com</a></td>
</tr>
<tr>
<td>46. Utilities Commission Action Network (US)</td>
<td><a href="http://www.ucan.org">www.ucan.org</a></td>
</tr>
<tr>
<td>47. W3C World Wide Web Consortium (US)</td>
<td><a href="http://www.w3.org">www.w3.org</a></td>
</tr>
<tr>
<td>48. World Privacy Forum (US)</td>
<td><a href="http://www.worldprivacyforum.org">www.worldprivacyforum.org</a></td>
</tr>
</tbody>
</table>
Appendix C
Selected Privacy Conferences

The policy community associated with privacy attends, and has always attended, an enormous number of conferences, workshops, symposia, forums, and other events. These more traditional forms of networking have historically been the principal means by which privacy advocates have connected and shared information. There is no evidence that the scope and frequency of conferencing has decreased as online methods of networking have proliferated. Conferences may be organized by government agencies, by the private sector, by academic institutions, or by a combination. Privacy advocacy groups have played significant roles in all.¹

Colin J. Bennett, *The Privacy Advocates*

*The International Conference Of Data Protection And Privacy Commissioners* has been conducted annually since 1978 and brings together data protection and privacy commissioners, and the privacy epistemic community from around the globe.²

*The Computers Freedom & Privacy Conference* has been held annually since 1991 in the United States and Canada.³

*The Computers, Privacy, and Data Protection Conference* is an international privacy conference organized by European universities.⁴

*The International Association of Privacy Professionals* bills itself as the world's largest association of privacy professionals with more than 7,000 members in 52 countries. The IAPP conducts a conference in Washington D.C. each spring.

Law Schools and academic journals occasionally sponsor conferences or symposia that focus on privacy, and invite well-known privacy experts, faculty, and students to author
essays on privacy issues, and then publish journal editions devoted to privacy. The following are illustrative:


2 For information on the 2010 International Conference Of Data Protection And Privacy Commissioners see: http://www.privacyconference2010.org/ (Last accessed 07 September 2010).

3 See the *Computers Freedom & Privacy Conference* site at: http://www.cfp.org/ (Last accessed 07 September 2010).

4 See http://www.cpdpconferences.org/organisation.html (Last accessed 07 September 2010).
Appendix D

Fair Information Principles/Practices (FIP)

Similarities in the core fair information principles found in the United States, Europe, the Council of Europe, and the OECD suggest the influence of “debates in the United States in the late 1950s and early 1970s among the small number of data experts.”¹ Members of the nascent privacy epistemic community actively educated policy makers and new privacy epistemic community members in the Council of Europe and the OECD in the 1970s and 1980s.²

¹. Records, Computers, and the Rights of Citizens (1973)³
Subsequently Incorporated into the U.S. Privacy Act of 1974

1. **Openness** – Data policies should be open and clear and the entity or person controlling the data should be easily identifiable.

2. **Collection Limitation** - Collection of personal data should be limited and obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

3. **Purpose Specification** - The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation** - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified as described above, except with the consent of the data subject or by the authority of law.
5. **Data Quality** - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up-to-date.

6. **Individual Participation** - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request is denied and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

7. **Security Safeguards** - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

8. **Accountability** - A data controller should be accountable for complying with privacy measures.

Younger Committee Report, 1973 (UK)

1. Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes.

2. Access to information should be confined to those authorized to have it for the purposes for which it was supplied.

3. The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.
4. In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.

5. There should be arrangements whereby the subject could be told about the information held concerning him.

6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.

7. A monitoring system should be provided to facilitated the detection of any violation of the security system.

8. In the design of information systems, periods should be specified beyond which the information should not be retained.

9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

10. Care should be taken in coding value judgments.

---

**Council of Europe**  
**Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector**

1. The information stored should be accurate and should be kept up to date. In general, information relating to the intimate private life of persons or information that might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.
2. The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3. The information should not be obtained by fraudulent or unfair means.

4. Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5. Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7. Every care should be taken to correct inaccurate information and to erase, obsolete information or information obtained in an unlawful way.

8. Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirection of information, whether intentional or not.

9. Access to information stored should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10. Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.
Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector

1. As a general rule the public should be kept regularly informed about the establishment, operation and development of electronic data banks in the public sector.

2. The information should be: a) obtained by lawful and fair means; b) accurate and kept up-to-date; and c) appropriate and relevant to the purpose for which it has been stored. Every care should be taken to correct inaccurate information and to erase inappropriate, irrelevant or obsolete information.

3. Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination,
   a. Their existence must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state;
   b. Such law, regulation, statement or document must clearly state the purpose of storage and use of such information, as well as the conditions under which it may be communicated either within the public administration or to private persons or bodies;
   c. That data stored must be used for purposes other than those which have been defined unless exception is explicitly permitted by law, is granted by a competent authority or the rules for the use of the electronic data bank are amended.
4. Rules should be laid down to specify the time limits beyond which certain categories of information may not be kept or used. However, exceptions from this principle are acceptable if the use of the information for statistical, scientific or historical purposes requires its conservation for an indefinite duration. In that case, precautions should be taken to ensure that the privacy of the individuals concerned will not be prejudiced.

5. Every individual should have the right to know the information stored about him. Any exception to this principle or limitation to the exercise of this right should be strictly regulated.

6. Precautions should be taken against any abuse or misuse of information. For this reason:
   a. Everyone concerned with the operation of electronic data processing should be bound by rules of conduct aimed at preventing the misuse of data and in particular by a duty to observe secrecy;
   b. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information and which provide for the detection of misdirections of information, whether intentional or not.

7. Access to information that may not be freely communicated to the public should be confined to the persons whose functions entitle them to take cognizance of it in order to carry out their duties.

8. When information is used for statistical purposes it should be released only in such a way that it is impossible to link information to a particular person.
OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph (3) except: a) with the consent of the data subject; or b) by the authority of law.

5. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and
the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation Principle:** An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him:  i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **Accountability Principle:** A data controller should be accountable for complying with measures, which give effect to the principles stated above.

2 Ibid., 96-101; 248-250.


5 See Council of Europe Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector at: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(73)22_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(73)22_EN.pdf).

6 See Council of Europe Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector at: [http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(74)29_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international%20legal%20instruments/1Resolution(74)29_EN.pdf).