An Examination of the Privacy Impact Assessment as a Vehicle for Privacy Policy Implementation in U.S. Federal Agencies

Susan M. Pandy

Dissertation submitted to the faculty of Virginia Polytechnic and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

In

Public Administration and Public Affairs

Anne Meredith Khademian, Chair
James F. Wolf
Karen M. Hult
Lawrence A. Ponemon

November 14, 2012
Alexandria, Virginia

Keywords:
E-Gov, Data Breach, FISMA, Implementation, Information Management, Privacy, Privacy Impact Assessment, Public Policy

An Examination of the Privacy Impact Assessment as a Vehicle for Privacy Policy Implementation in U.S. Federal Agencies

Susan M. Pandy

ABSTRACT

The Privacy Act of 1974 was designed to protect personal privacy captured in the records held by government agencies. However, the scope of privacy protection has expanded in light of advances in technology, heightened security, ubiquitous threats, and the value of information. This environment has raised the expectations for public sector management of sensitive personal information and enhanced privacy protections. While the expanse of privacy policy implementation is broad, this study focuses specifically on how agencies implement privacy impact assessments (PIAs) as required under Section 208 of the E-Government Act of 2002. An enhanced understanding of the PIA implementation process serves as a portal into the strategic considerations and management challenges associated with broader privacy policy implementation efforts.

A case study of how the U.S. Postal Service and the U.S. Department of Veterans Affairs have implemented PIAs provides rich insights into privacy policy implementation and outcomes. Elite interviews enriched by process data and document analysis show how each organization undertook different approaches to PIA implementation over time. This study introduces the sociology of law literature using Lauren Edelman's conceptual framework to understand how organizations respond to and interpret law from within the organization, or endogenously. Building upon Edelman's model, certain characteristics of the PIA implementation are analyzed to provide rich description of the factors that influence the implementation process and lead to different policy outcomes.

The findings reflect valuable insights into the privacy policy implementation process and introduce the sociology of law literature to the field of public administration. This literature furthers our understanding of how organizations enact policy over time, how the implementation process unfolds and is impacted by critical factors, and for identifying emergent patterns in organizations. This study furthers our understanding how privacy policy, in particular, is implemented over time by examining the administrative capacities and levels of professionalism that are utilized to accomplish this effort. This research comes at a critical time in the context of the emerging legal and political environment for privacy that is characterized by new expectations by the public and the expanding role of government to manage and protect sensitive information.

DEDICATION

This work is dedicated first to my parents, James John Pandy who passed away on December 21, 1993 and to Doris Brobst Pandy who resides in a nursing home in Ohio facing the challenges of Alzheimer's disease. Both of my parents raised me to believe I could do anything that I could put my mind to and I always thought that would be going to law school, so I'm sure my father is rolling over in his grave because finishing a doctorate was not among the many things that I set my sights on as a child. My parents cultivated a strong sense inquiry in me from a very young age; they exposed me to so many opportunities to feed my mind, to so many opportunities to grow and to seek knowledge.

I also dedicate this dissertation to the memories of both Dr. Larry Terry and Dr. Richard Worrall – two predominant influences in my doctoral journey. Dr. Terry ignited the passion in me for public administration and policy. He also talked me out of going to law school after completing my MPA at Cleveland State and sucker-punched me into pursuing a doctorate with the Center for Public Administration & Policy at Virginia Tech. Larry inspired me to start asking big questions early on in my MPA program and this often lead to long discussions and spirited debate over Hobbesian theory, studies in leadership, the leadership-management distinction, and reconciling bureaucracy with democracy. He introduced me to my first High Table event and I knew that CPAP was where I belonged.

On the other hand, Dr. Worrall took me to a new place in my quest for knowledge which resulted in us working together on digital divide issues in early 2000 when I moved to DC to work with him on electronic government implementation projects in collaboration with the National Academy for Public Administration & Policy. Dr. Worrall seeded this idea to develop this ambitious conference program that would address personal privacy in the digital age and it

would bring together well known and recognized privacy experts from all over the world. And we did just that, although Dick was not there to witness the fruits of our labor in May of 2002. Dr. Worrall planted this seed that ignited a passion for digital divide and privacy issues and how the rapid pace of technology change was going to seriously change the way we look at privacy and how we ultimately, govern information. Now after 10 years, privacy is getting the attention that it deserves will remain a very important policy issue well into the future.

The world of privacy is large and it is waiting for that group of scholars to embrace it and bring it to the level of attention that it needs in our public administration and policy programs.

ACKNOWLEDGMENTS

I would like to thank the members of my dissertation committee. As my chair, Anne Khademian was instrumental in "adopting" me from the series of pitfalls that I had in the early years of trying to find my direction and purpose in this study. Anne helped me to narrow the focus of my study and to anchor it in the literature of Lauren Edelman. She was very supportive throughout the process and endured the fits and starts of my writing and continued to help me structure my research. I genuinely appreciate the dedication and guidance that Anne has given to my research throughout this journey.

Karen Hult has been an inspiration since my first class with her in Blacksburg many years ago. I owe Karen for expanding my knowledge of the organizational theory literature and for helping me to develop as a writer and a scholar. Her insights into my research helped me to probe the political and environmental influences of my case studies. One can only hope to acquire the meticulous and thoughtful level of scholarship that Karen has achieved.

Jim Wolf has always been that friendly face throughout the entire process and encouraging me to finish. His comments helped me to probe the nature of policy implementation and to make distinctions between the process of policy implementation and the policy process, in general.

Finally, Larry Ponemon has been a mentor and friend to me from the very beginning of this journey when we met through my work at the National Academy of Public Administration. As a globally recognized privacy expert, Larry has influenced my research and professional work in the privacy field and data security. Larry was also instrumental in connecting me to the people interviewed in my case studies as well as many influential people in the privacy

profession. He has greatly shaped both my academic and professional work and has contributed to my undying passion for this topic.

I also owe my academic growth to many people in the CPAP community, especially the faculty that were influential while I was there: Gary Wamsley, Larkin Dudley, Joe Rees, Gerry Pops, John Dickey, Ray Pethtel, Susan Gooden, and Charles Goodsell. Charles Goodsell was a pivotal influence on me from the time I entered his Context in Public Administration class to being his teaching assistant in State Policy. Charles inspired me to be creative in my writing and to delve deep into the context of public administration and policy.

A very special thanks to the dedicated employees of the VA and the USPS that offered their time in the form of interviews, review, and feedback.

I want to thank many of my classmates Rick Morse, Matt Collins, Joe Mitchell, Bryce Hoflund, John Tennert, Melony Pride-Rhodes and Gail Ledford. Melanie and Gail have been rocks to me.

My best friend, Christine Salcedo, deserves special mention for never giving up on me. She's been my biggest cheerleader and supporter, not just through the dissertation, but from the time we met in first grade where we would spend recess doing our homework on the rock on the playground.

I also want to thank my colleagues in the payments industry who have also been supportive over the years. You know who you are and I thank you for always asking me about my progress and for the constant encouragement.

CPAP is a very special place and I will always consider my time in Blacksburg as some of the best times in my life. It was truly a "life of the mind" as Gary Wamsley often reminded us.

TABLE OF CONTENTS

ABSTRACT ii
DEDICATION iii
ACKNOWLEDGMENTS v
LIST OF TABLES AND FIGURES x
LIST OF ABBREVIATIONS xi
CHAPTER ONE - INTRODUCTION 1
Case Studies 8
Limitations of Research 15
CHAPTER TWO – THE PRIVACY IMPACT ASSESSMENT 18
Privacy and E-Government: The Emergence of the Privacy Impact Assessment 19
The Privacy Impact Assessment Legal Mandate 21
The Mechanics of a Privacy Impact Assessment 23
Factors that Influence the PIA: Training, Professional Expertise, & Organizational Structure 24
Training 25
Professional Expertise 27
Organizational Structure 28
Summary 34
CHAPTER THREE – METHODOLOGY 36
Research Design 38
Case Study Selection Process 41
Data Collection Procedures and Process 43
Factors that Influence the PIA Process: Training, Professional Expertise, & Organizational Structure 55
Training 55
Professional Expertise 57
Organizational Structure 60
Validity and Reliability and the Role of the Researcher 63
Limitations of Study 63
CHAPTER FOUR – INTRODUCTION TO THE CASE STUDIES OF THE DEPARTMENT OF VETERANS AFFAIRS AND THE U.S. POSTAL SERVICE 65
United States Department of Veterans Affairs 66
U.S. Department of Veterans Affairs – Emergence of the Privacy Impact Assessment 67

Participants in the PIA 71
Training for the PIA 74
Professional Expertise and the PIA 75
Organizational Structure and the PIA 77
Summary 82
United States Postal Service – Emergence of the Privacy Impact Assessment 84
Underpinnings of the BIA: Leadership, Policy, and Structure 85
Participants to the BIA 88
Training for the BIA 89
Professional Expertise and the BIA 91
Organizational Structure and the BIA 93
Summary 95
CHAPTER FIVE – CASE STUDY ANALYSIS 96
USPS and the VA – Context for Analysis 99
The VA and the Evolution of the Privacy Impact Assessment 101
PIA in the Post-Data Breach Years: 2007-2010 106
Procedural, Technical and Design Changes to the Privacy Impact Assessment 108
Policy and Management Changes that Influenced Structural Changes 110
The PIA and Professional Expertise 115
The PIA and Training 117
Patterns and Change in the Policy Implementation Process 118
Lessons Learned 120
Conclusions 121
United States Postal Service (USPS) and the Evolution of the BIA 122
Organizational Structure and the BIA 125
Professional Expertise and the BIA 132
Training and the BIA 135
Summary 138
Conclusions: Disparate Approaches to Policy Implementation 139
CHAPTER SIX – ADVANCING IMPLEMENTATION 143
Edelman's Model 144
Privacy Impact Assessment in the Literature 151
Privacy in the Public Administration Literature 153
CHAPTER SEVEN - CONCLUSIONS 159

Real-World Mapping and Privacy By Design 173
Future Research – In Other Areas 175
Recalibrating Policy Management for Achieving Success 178
BIBLIOGRAPHY 180
APPENDICES 195
APPENDIX A: Agency Interview Recruitment Emails 196
APPENDIX A: Agency Interview Recruitment Emails 197
APPENDIX B: List of Interviewees 198

LIST OF TABLES AND FIGURES

Page

Table 1: Privacy Act of 1974 Protections (Fair Information Practices) 18

Table 2: Essential Elements of the PIA required by the Office of Management and Budget 20

Table 3: Sample PIA Training Workshop Agenda 26

Table 4: Roles and Responsibilities to Support PIA 33

Table 5: Document Analysis 45

Table 6: Books Reviewed in this Study 47

Table 7: Interview Questionnaire / Guide 50

Table 8: VA Privacy Policy Directives between 2003 and 2010 69

Table 9: VA PIA Position Responsibilities per VA Directive 6508 (2008) 72

Table 10: 2004 Metrics Reported by Agency VA CIO 104

Table 11: Research Conclusions and Takeaways 159

Figures

Figure 1: Mechanics of the PIA Process 23

Figure 2: Research Design to Support Case Study 40

Figure 3: Stages of the Privacy Impact Assessment Process 54

Figure 4: Interplay among Influential Factors on the PIA Process 77

Figure 5: VA Triumvirate 78

Figure 6: Organizational Chart for the Office of Information Technology 79

Figure 7: Three Stages of PIA Process Analyzed in this Study 102

Figure 8: Timeline of Privacy Policy Implementation for the VA 107

Figure 9: Timeline of Privacy Policy Implementation for the USPS 137

LIST OF ABBREVIATIONS

ARMA	American Records Management Association
AA	Affirmative Action
CIPL	Center for Information Policy Leadership
CRM	Certified Records Manager
CEO	Chief Executive Officer
CIO	Chief Information Officer
CIPP	Certified Information Protection Professional
CISO	Chief Information Security Officer
CISSP	Certified Information Security Systems Professional
CPO	Chief Privacy Officer
CTO	Chief Technology Officer
DHS IRC	Department of Homeland Security Incident Response Center
EEO	Equal Employment Opportunity
EIA	Environmental Impact Assessment
EIS	Environmental Impact Statements
FIP	Fair Information Practices
FISMA	Federal Information Management Security Act
FTC	Federal Trade Commission
GARP	Generally Accepted Recordkeeping Principles
GAO	Government Accountability Office
IAIA	International Association for Impact Assessment

IG	Inspector General
IPRM	Information Protection and Risk Management
ISO	Information Security Officer
ITOC	Information Technology Oversight and Compliance
NARA	National Archives and Records Administration
NCA	National Cemetery Administration
NIST	National Institute for Standards and Technology
OI & T	Office of Information and Technology
OMB	Office of Management and Budget
OPRM	Office of Privacy and Records Management
OECD	The Organization for Economic Cooperation and Development
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RMA	Records Management Association
RIM	Responsible Information Management Council
SSN	Social Security Number
UIP	Unique Identification Program
USPS	United States Postal Service
VA	United States Veterans Administration
VHA	Veterans Health Administration
VBA	Veterans Benefits Administration

CHAPTER ONE - INTRODUCTION

> The appropriate balancing of the increasing need for information in guiding our economy to ever higher standards of living, and the essential need of protection of individual privacy in such an environment, will confront public policy with one of its most sensitive tradeoffs in the years immediately ahead. Alan Greenspan (1998 letter to Congressman Edward J. Markey)

Alan Greenspan could not have made a more accurate prediction of the state of affairs resulting from the expansion of the information economy in the 21st century. Information is the driving force of this new economy.[1] New technologies and the Internet have advanced our ability to access and use information in ways that were once unimaginable. The result has been one that places unique challenges on policymakers, particularly for driving broad privacy policy implementation efforts in organizations. In a sense, privacy policy is a new frontier for public management in that it manifests policy demands that require unique tools and methods for effective outcomes. These demands translate into sound practices of information governance to combat the risk of data compromise in an information-rich, yet vulnerable environment.

The presence of this vulnerable environment has created a modern-day dilemma for government in both governing and managing information. Recent years have witnessed an unprecedented number of government and private sector data breaches involving sensitive personal information, coupled with identity theft[2] and terrorist activities. Accordingly, data breach and identity theft represent the greatest facets of privacy policy concerns and require organizations to be even more vigilant in their information protection practices, less they bear the consequences of lost customers, damaged reputations and considerable monetary damages.

---

[1] A 1983 cover article in *Time magazine*, "The New Economy", described the transition from heavy industry to a new technology based economy, retrieved on September 10, 2012 from http://www.time.com/time/magazine/article/0,9171,926013-1,00.html.

[2] Although identity theft is defined in many different ways it is defined as "fundamentally, the misuse of another individual's personal information to commit fraud," by the President's Identity Theft Task Force in *Combating Identity Theft: A Strategic Plan*, April 23, 2007, retrieved from http://www.idtheft.gov/reports/StrategicPlan.pdf.

The establishment of new technology systems that allow for the easy access and transference of personally identifiable information (PII) between parties raises the need for additional safeguards in securing these systems. However, this security must be balanced with the need for privacy protections. Existing public opinion on privacy already reflects a broad desire for more accountability and security in the protection of sensitive personal information.[3]

It follows that the state of information privacy policy[4] in a democratic government has considerable implications for the field of public administration and policy and research should focus on the actual process of privacy policy implementation.[5] Lauren Edelman's work in the sociology of law literature provides a useful lens for studying this process by understanding the dynamics of how personnel and structural changes can impact the implementation process over time. Edelman (1992) assumes that organizations respond uniquely to ambiguity in the law and applies this assumption to the case of equal employment opportunity and affirmative action (EEO/AA). The E-Government Act of 2002 (the "E-Gov Act)[6] presents a similar opportunity for studying how federal agencies should give meaning to the ambiguity in privacy policy by

[3] Best, Krueger and Ladewig (2006) present longitudinal data on public opinion about privacy from 1990 through 2006 and conclude that three major developments have resulted in the shifting of public opinion about privacy: (1) the emergence of the Internet as a new communication technology; (2) the war on terrorism; and (3) the development of a wide array of new surveillance technologies. Together these events have spawned considerable polling on opinion toward different forms of surveillance and their threat to civil liberties (Huddy, Khatib, and Capelos, 2002). The research by Best et al. evaluates public support for the concept of privacy both generally and narrowly and gauges whether the public feels their privacy has been threatened or invaded and also considers perceived threats to personal privacy from government.

[4] Privacy policy involves setting security levels for different types of information. But it also includes deciding what information to collect in the first place, under what circumstances the agency might share it, and how to notify customers that the data is being collected.

[5] Clune describes implementation as an "interactive process" and defines implementation as "the design of government policy, the choice and administration of policy instruments for social purposes, and the management of government policy in a complex and politicized environment" (1983, p. 49).

[6] The E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803), is a United States statute enacted on December 17, 2002, with an effective date for most provisions of April 17, 2003. Its stated purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.

analyzing the process of PIA implementation within organizations. Edelman's model (2002, 1992) is transferable to the case of privacy policy because these policies have translated to a broad discretion and uncertainty surrounding appropriate roles, responsibilities, and organizational structures[7] necessary for fulfilling policy enactment requirements.

An empirical study of the variation between two very large federal agencies' approach to implementing privacy policy in the context of the PIA process will contribute to our field's knowledge of *how* organizations construct and develop their respective understandings of the law. The case studies show how statutes are brought to life in the implementation process and that this process matters in terms of what policy outcomes emerge. The approach to implementation that is undertaken by an organization can vary and some approaches lead to learning while others do not. These approaches are also influenced by the external environment. This is not to say that one organization implements privacy policy better than the other; that is not the intent of this study. Nor is this study intended to provide generalizations about the policy process or implementation in general. Accordingly, this dissertation will address the following overarching research question:

> *How have PIAs been implemented within the USPS and the VA and how has implementation changed over time?*

The goals of this study are simply to understand what is often considered an ambiguous process within federal agencies based on empirical evidence gathered from qualitative interviews with senior agency officials and extensive document analysis. My approach builds on the work of Lauren Edelman (2003, 2002, 1999, 1997, 1992, and 1990) and begins with outlining the stages of organizational response to law, or in this case, the stages of the PIA implementation

[7] The term organizational structure is used in this study as defined by Edelman as "new offices, positions, rules, and procedures" (1992, p. 1542). The use of "structures" by Hult and Wolcott (1990) is also useful in the context of this study in defining structures as "recurring patterns of relations within or between organizations and organizational units."

process which provide a useful method for exploring changes in policy implementation over time. Like Edelman (1992), this study assumes that the laws that drive various policy implementations are often grey and lead to different interpretations within organizations. However, the approach that an organization takes to translating law through the implementation process varies and some organizations may take a compliance-focused approach, some may start off strong with high intensity and sweeping changes and then diminish in their momentum, or some may have a strong start where policies and procedures become the status quo or *modus operandi*, while others may need more time to get started or to get off the ground that can lead to a continuous improvement or learning approach. Certain dimensions of the policy implementation process can help us to understand the context for different agency approaches and how different characteristics of the process can lead to different policy outcomes.

Edelman brings the public administration field one step closer to a deeper understanding and analysis of the process of policy implementation and what this means for public management. The importance of distinguishing implementation efforts as substantive versus symbolic can drive future research into how organizations seek legitimization through the process of policy implementation. For example, in her research, Edelman characterizes implementation as being either "symbolic" or "commitment-oriented" (1992) or what I described in my conclusions in Chapter 7 as an implementation process that takes a "check-box" or "baked-in" approach. A check-box approach may indicate one that is more expedient for the organization and largely focused on achieving compliance as a means to an end. A "baked-in" approach is one where the implementation process has become part of the overall organizational culture and social norms of the organization. By analyzing the impact of a certain factors that influence the PIA process, assumptions can be made about whether or not the organization has

taken a symbolic or commitment-oriented approach to policy implementation. Edelman (1992) points to changes in structure, such as the creation of new offices, which create the perception of action and attention to policy implementation, however, these changes may only be symbolic and done to advance the perception that the agency is responding to legal mandates and in effect, the new office or structure holds no authority within the organizational hierarchy. The mere creation of new structures to support policy implementation does not necessarily mean that agencies are actually committed to the process, but may only be "window-dressing."

In terms of the PIA itself, this process may often merely be a symbolic approach to implementation in that the process is not fully integrated into an organization, that is lacks executive-level buy-in, and may result in assessments that are meaningless or receive poor grades which can be reflected in reporting requirements under the Federal Information Management Security Act (FISMA) under the E-Gov Act of 2002.

Because the *process* of policy implementation is one that is scarcely studied in the public administration and policy literature, this study focuses on the PIA implementation as a process that evolves over time and is influenced by factors such as training, professional expertise, and organizational structure. The impact of external environmental factors is also considered to provide more context for the agencies being studied.

Analysis of the dynamics of the PIA process will show how privacy policy is operationalized within the U.S. Postal Service (USPS) and the U.S. Department of Veterans Affairs (VA). My findings show how two organizations take very different approaches to policy implementation and that broader privacy policy can be better understood by analyzing these approaches and the contextual factors that may shape these approaches. For instance, some organizations may develop a centralized approach to policy while others may have a fragmented

or decentralized approach and each leads to different outcomes. Therefore, understanding the process of PIA implementation using Edelman's argument (1992) supports the empirical focus of this study and is further informed by process data and the literature on implementation. This leads to a rich description of an important policy implementation process, the internal and external factors that impact it, and subsequent policy outcomes. My study enriches our ability to understand mandates in the context of implementation with a primary focus on privacy policy.

This study also shows that leadership is a critical component to any policy implementation approach and the process that unfolds. While leadership was not part of the original research design, the findings showed the importance that it plays in shaping the PIA implementation process or challenges faced in its absence, particularly in relationship to other factors such as training, professional expertise, and organizational structure. Therefore, the use of leadership in this study is based on previous literature from Larry Terry (1995), Price (1962), Doig and Hargrove (1987), and Selznick (1968). Terry's (1995) work is particularly useful for framing the exercise of bureaucratic leadership drawing upon legal, managerial, and sociological research. Terry's (1995) definition of bureaucratic leadership based on managerial tradition requires careful attention to the conventional instruments of managerial control such as executive recruitment, training, constituency support and cultivation, organizational design and policy development and implementation. The role of leadership in the policy implementation process also raises historical questions about the expanse of broad discretionary power into administrative agencies (Lowi, 1979 and Schoenbrod, 1993, as cited in Terry, 1995, p. x).

The requirement to implement PIAs under the E-Gov Act was challenged from the beginning by a lack of leadership to guide agencies in their policy design that was recognized by the Government Accountability Office (GAO) in its request for better oversight and guidance by

the White House and the Office of Management and Budget (OMB).[8] In 2005, the GAO recommended leadership in the privacy management structure of agencies through the designation of a Senior Agency Official for Privacy (SAOP). In the absence of strong leadership, individual agencies were left to fend for themselves in bringing their information practices in line with both the Privacy Act and the E-Gov Act.

This lack of leadership and guidance only widens the existing gap between the growth of new technologies that collect personal data and the laws designed to protect that data, resulting in policy vacuums. A 2009 Report issued by the Information Security and Privacy Advisory Board[9] explains that policy vacuums result from the inability of agency policy and procedure to adapt to technological change and legal requirements. However, this study shows that organizations can adapt to the presence of policy vacuums by taking a learning approach in response to ambiguous legal mandates by creating implementation processes that are adaptive and flexible in response to a continuously changing policy environment.

The next section provides a brief introduction to the case studies and to the organizational environments for which they are embedded to provide context for later analysis.

[8] U.S. Government Accountability Office (2003). *Privacy Act: OMB leadership need to improve agency compliance.* Washington D.C.: Government Printing Office.

[9] The Information Security and Privacy Advisory Board (ISPAB) is a group that advises the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Commerce Department. ISPAB was created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board and amended by the E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) (P.O. 107-347). One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative and physical safeguard issues relative to information security and privacy.

Case Studies

The Department of Veterans Affairs (VA) and the Postal Service (USPS) were selected as case studies in this research because they each represent forty percent (40%) of the federal government with the USPS as the third largest employer in the U.S. and the VA, the second largest employer with 263,350 employees and a projected Veteran population of 22.2 million.[10] Each agency is responsible for the management of an extraordinary amount of sensitive citizen information, both physically and electronically; therefore, privacy risk and the potential for information compromise is very high and makes these agencies worthy of investigation in the context of how they have implemented the PIA as a facet of broader privacy policy implementation over time.

The longevity and reputation of these agencies is largely dependent on their ability to protect sensitive citizen information, something that each agency has historically done well, with the exception of two breaches at the VA in May 2006 and January 2007. The USPS serves as a minor case study, particularly given the challenges of gathering interview data. However, rich process data helps to understand the PIA as a tool for privacy policy implementation particularly since the USPS began conducting PIAs long before they were mandated rendering the agency as a pioneer on the privacy protection front.

Understanding the unfolding process of PIA implementation in both of these agencies lends itself to a deeper knowledge of how policy is enacted internally. Edelman's (1992) model helps to identify the various stages of the implementation process and strengthens this study's focus on the *process* of policy implementation helping to identify inconsistencies and internal dynamics.

[10] Retrieved on September 21, 2012 from http://www.va.gov/vetdata/docs/Quickfacts/Stats_at_a_glance_FINAL.pdf and VA Strategic Plan http://www.va.gov/VA_2011-2015_Strategic_Plan_Refresh_wv.pdf.

Factors that are likely to influence the process begin with a condition of ambiguity in the legal mandate for which the organization must construct a response. The way that organizations interpret this ambiguity can vary and can be understood by looking at different characteristics of the implementation process such as training, professional expertise, and organizational structure. For Edelman, structural changes in the organization provide a highly visible response to ambiguity and weaknesses in legal mandates (1992). In this study, structural changes are particularly useful for assessing how the policy implementation process changes over time. Professional expertise and training are integral to these structural changes and also shape the process. Edelman's (1992) model also shows how professionals are pivotal to helping organizations interpret the law and enact policy.

An analysis of the role of professional expertise in the process of policy implementation also helps to understand administrative processes as well as changes in rules and procedures (i.e. policy). Professionals and experts help the participants assign meaning to policies and to the implementation process in order to make sense out of it. Elite interviews with staff at both agencies delve deeper into how professional expertise shapes the PIA process and privacy policy across the organization.

Expertise is a particularly influential factor to the policy implementation process and that can be influenced by the type of expertise that is present in an organization, which can be understood by looking at the role of career civil servants versus political appointees and their respective impacts on policy and agency performance (Lewis, 2008). Lewis (2008) argues that appointees are more aligned with political preferences, whereas careerists tend to have more substantive expertise over a particular policy area that they manage. The majority of interviews in this study were representative of career civil servants and based on interview data, these

careerists reflected substantive expertise within their policy realms as will be discussed in further detail in the analysis in Chapter 5.

While this study was not designed to analyze the political environment of these organizations, the larger environments in which these agencies were embedded is worthy of attention to provide some context for the environmental influences on the PIA implementation process. Both agencies were impacted by a post-9/11 environment, growing budgetary pressures and fiscal constraints, congressional scrutiny, and an emergent e-government movement. The e-government movement is a key driver in the modernization of the federal IT environment in light of advanced technology such as the Internet and data security considerations driven by growing identity theft, data breach, and terrorism. This environment was also conditioned by a broader movement across government toward a standardized approach to technology and information management.

This emergent environment required agencies for the first time to submit reports on their IT systems in order to receive operational funding. The PIA requirement was directly tied to the ability to secure funding for IT projects. In the beginning this process was strongly weighted towards security, particularly in the aftermath of 9/11 but gradually tilted towards privacy. Both agencies were faced with varying pressures from Congress, inspectors general, fiscal pressures and mounting pressures to restructure.

Under Secretary Nicholson, the VA pursued its IT Realignment Plan which drove a huge shift from a decentralized to centralized IT infrastructure and management under a single Chief Information Officer (CIO). This effort responded to concerns about the age, efficiency and security of the whole VA IT system. The concern culminated in early 2005 with then-VA

Secretary R. James Nicholson authorizing a system-wide study to come up with options for what a restructured and modernized IT structure at the VA might look like.[11]

This Realignment was driven by continuous GAO scrutiny since the 1980s calling for reorganization of the VA, especially around IT. The VA faced many challenges in achieving its centralized vision as IT systems and services were completely decentralized. For instance, budget decisions completely decentralized and detached from any system-wide IT strategy. According to an Oct. 2005 memorandum from a former VA CIO, the CIO had direct control over only 3% of the department's IT budget and 6% of its IT personnel (Walters, 2009).

On numerous occasions, the GAO noted the criticality of the need for the VA's CIO to ensure well-established and integrated processes for leading, managing, and controlling investments and a transition to a decentralized management structure. A February 2005 contractor assessment of VA's IT organizational alignment also noted the lack of control around spending and found that project managers in the field had wide discretion to shift IT money to support varying projects, including those unrelated to IT. The assessment also found that department-level management was only focused on reporting expenditures to the OMB and Congress, rather than the management of expenditures within the department. The assessment resulted in a revolutionary and unprecedented plan for IT realignment that would centralize IT authority at the VA central office (Walters, 2009).

Internally, the VA was also challenged by high turnover and public scrutiny of its political appointees between 2003 and 2009. Bob McFarland was the CIO between 2003 and 2005 and resigned just as IT Transformation Governance Plan was being put in place.

[11] Walters, Jonathan. (2009). Transforming information technology at the Department of Veterans Affairs. *Governing Magazine.* Retrieved on October 28, 2012 from http://www.isaca.org/Knowledge-Center/cobit/Documents/WaltersVAReport-June09.pdf.

McFarland had previously been the vice president of government relations at Dell Computer and headed up business units.

Bob Howard inherited the IT Transformation Governance Plan in May of 2005 when he was appointed by President George W. Bush in 2006. Howard was a retired Major General from the U.S. Army in 1996. He had also served as the vice president and general manager of the analysis and learning technologies division at Cubic Corp. prior to the VA. Howard suffered from an IG investigation that implicated him in serious mishandling of VA funds, preferential treatment and an inappropriate relationship with a subordinate. The IG found that managers in the technology office were awarded $24 million in bonuses despite a large budgetary deficit and concluded in its report that managers "were not fiscally responsible in administering awards" and a senior manager was implicated (Dao, 2009). To exacerbate these conditions, Howard also took office as the VA experienced the largest data breach in American history in 2006, followed by another prominent breach in 2007.

Roger Baker became the CIO in 2009 under the Obama Administration. Baker was a long-time federal IT executive and had a lot of prior CIO experience, unlike some former VA CIOs. Baker had served as CIO at General Dynamics Information Technology and worked as the CIO of the Commerce Department under the Clinton Administration. Baker inherited a challenging IT environment at VA in light of high profile data breaches of 2006 and 2007. Baker grew to be a key participate in President Obama's key IT initiatives to develop a health network that would presumably reduce health care costs and medical errors. This initiative was prompted in response to the poor health care services that wounded soldiers returning from Iraq and Afghanistan received at Walter Reed which involved Baker in working on an electronic health records system with the Defense Department (Walters, 2009).

The PIA requirement under the E-Gov Act added to external and internal challenges of VA and added the burden of the number of systems that agencies have to report on – major and minor systems – the number of systems to report on presented a paramount task to the agency. The agency did not have a centralized approach to reporting on these systems – each VA hospital was an island unto itself, there was an enterprise infrastructure in place to implement or manage this extensive reporting. Often hospitals would buy their own servers and no one knew about it. Total systems to report on for all 25 agencies increased by nearly 20% between 2004 and 2005 (Walters, 2009).

The USPS, on the other hand, was also facing a large-scale transformation plan under Postmaster General John Potter as part of a larger effort to address its financial crisis and congressional scrutiny that had been building for throughout the 1990s. The Transformation Plan was developed in response to a request from Congress and the GAO that the USPS outline how it intends to function in the wake of changing markets, new technologies and a severe financial crisis.

The history leading up to the USPS's financial crisis was exacerbated by the 9/11 attacks and particularly the anthrax letter attacks that resulted in the deaths of several postal workers. The anthrax attacks changed the context of the working environment that the USPS operated in to a fear of being anthraxed or pipe-bombed versus being bitten by a dog. This largely resulted in considerable citizen safety concerns.

It should be noted that the operation of USPS and delivery of mail is critical to the economy; it is a linchpin to a $900 billion mailing industry that employs nearly 9 million

workers and is 8% of GDP. Its fiscal position brings decades long debates over whether USPS is a business or a service.[12]

Many of the USPS's challenges date back to 1990s and the rise of Internet technology and e-commerce. The Internet was noted as a key cause to the decreased volumes, revenues and growing deficits experienced by the USPS. The ability of the USPS to compete in the e-commerce environment raised questions about its ability to compete in the marketplace. A 1996 GAO report expressed concern with the inability of the USPS to structure, manage and categorize its ecommerce products and services and more specifically, its address correction services came into question under the Privacy Act. The GAO concluded that improved oversight was needed to protect privacy of address changes. The privacy of address changes was a pivotal issue because the USPS's address correction service was interpreted by some to violate privacy laws. However, the USPS defended this service as a "routine use" of data covered under the Privacy Act, which prohibits selling mailing lists without written consent. The USPS address correction service was deemed unclear in terms of whether or not it was a routine service permitted under the statute by the Clinton administration's chief counselor for privacy in the OMB from 1999 to 2001, Peter P. Swire (McElhatton, 2012).

In contrast to the VA, no presidential appointments or Senate confirmed appointees are designated to management levels at the USPS. The Postmaster General is appointed by the Board of Governors, and therefore, raises question of accountability to the American citizens.

---

[12] U.S. Senate Subcommittee before The International Security, Proliferation & Federal Services Subcommittee of the Committee on Government Affairs. (2002). *The Postal Service in the 21st century: the USPS Transformation Plan.* 107th Cong., 2nd Sess. Washington, D.C.: Government Printing Office. Retrieved on October 29, 2012 from http://www.gpo.gov/fdsys/pkg/chrg-107shrg80598/html/chrg-107shrg80598.htm.

Both agencies experienced similar political pressures and congressional scrutiny, fiscal constraints, and considerable management challenges to modernize their respective IT infrastructures. These external factors shaped different environmental contexts for each agency which led to distinctive approaches to policy implementation that can be better understood by focusing on a specific process throughout this implementation – the PIA and the various internal factors that shaped this process.

Limitations of Research

It is important to note that this research does not seek to define or analyze compliance as a component of the policy implementation process.[13] While a PIA is a component of compliance with privacy laws; compliance in this context has been rendered ambiguous because organizations are given wide latitude to construct their meaning of compliance with the established laws (i.e. the Privacy Act and the E-Gov Act) (Edelman, 1992). The laws are also ambiguous because they continue to evolve and Federal agencies have not been given clear guidance on what constitutes compliance with the requirements under the E-Gov Act for the completion of PIAs which has resulted in broad bureaucratic discretion for interpreting and applying the law (Bamberger and Mulligan, 2008). Edelman (1992) established ambiguity as a "condition of organizational mediation of law" noting that EEO/AA law was ambiguous with respect to the meaning of compliance, as construed by the courts, and because of weak enforcement mechanisms (p. 1536). Edelman (1999) also noted the problems associated with ambiguity in the law in her study of the implementation of the 1964 Civil Rights Act, an

[13] Much of Edelman's research is focused on compliance with ambiguous laws. For example, in Edelman's (1999) *The endogeneity of legal regulation: Grievance procedures as rational myth*, she argues that EEO grievance procedures have become a standard and rationalized form of compliance with EEO law. The Privacy Impact Assessment (PIA) in this study is analogous to this example; however, this study is less focused on compliance and more focused on the process of implementing the PIA and the factors that influence this process.

ambiguous legal mandate that made compliance difficult to define. She argued that "the more ambiguous and politically contested the law, the more open it is to social construction" (1999, p. 407).

It should also be noted that access to key staff in both organizations was limited. The USPS was the most challenging and only resulted in interviews with two individuals. Access in the USPS was limited to the privacy officer in consumer affairs who reported to the Chief Privacy Officer (CPO). Repeated attempts were made to interview the CPO, although these attempts were continually redirected to another staff member who could speak on her behalf. The Records Management Officer was also reluctant to be interviewed and questioned the value that she could provide to my research given her lack of involvement with the PIA process. However, the former and first CPO of the USPS made herself available to provide some historical context. The Chief Information Security Officer and other information security staff declined to be interviewed under the advisement of their legal department. In effect, the USPS was less willing to make itself available for this study, whereas the VA provided a greater degree of access. Despite this limited access, the interview data created a window to the way that both agencies interpret and understand the implementation of PIAs.

Lastly, this study is limited by the sample size or from generalizations drawn based on only two organizations. Expanding the sample size across several agencies would produce results that are more conducive to broader generalizations and deeper analysis. A study that identified a typology of organizations relevant to the PIA and privacy policy would render more significant and reliable results that could be repeated and measured over time. I offer two suggestions for developing such a typology. The first approach would select a group of agencies based on an agency's historical perspective on privacy and how this historical perspective

applies to broader privacy policy implementation within the organization. Agencies could be analyzed not only by their historical predisposition to privacy issues but also by their sensitivity to privacy issues (e.g., high, medium, low or susceptibility to data breach). Second, a typology could be based on an agency's ability to integrate functions across the policy implementation process. Certain factors that influence the level of integration could include examining collaboration across departments, the creation of multidisciplinary teams, the role of technology in enhancing integration, or the role of leadership and expertise.

This study is organized as follows: Chapter Two presents a framework for understanding privacy from a historical and legal perspective and fully presents the background for the privacy impact assessment (PIA). Chapter Three discusses the research design and methodology used in this study, including how the research was conducted, how the data was collected, and how the data was analyzed. Chapter Four introduces a macro-analysis of the two case studies, the USPS and the VA. This chapter is more empirical than analytical and creates the foundation for understanding the evolution of privacy within each agency to support the case study analysis presented in Chapter Five. Chapter Six reviews the literature that supports this research, including a brief overview of some relevant privacy literature, scholars within the field of public administration that have examined privacy, the implementation literature, and the theoretical anchor to this research – Lauren Edelman and the sociology of law literature. Chapter Seven provides conclusions and broader findings from the research and presents recommendations and insights for future research in privacy policy and innovation in public management for the field of public administration.

CHAPTER TWO – THE PRIVACY IMPACT ASSESSMENT

The scope of privacy policy and law in the United States is broad and open to wide interpretation. In order to understand the complexity of the implementation of privacy policy, this study delves into a specific process for enacting privacy policy in organizations – the privacy impact assessment (PIA), mandated under Section 208 of the 2002 E-Government Act of 2002 (the "E-Gov Act").

The E-Gov Act marked the realization that the Privacy Act of 1974 (the "Privacy Act") was no longer adequate to protect privacy in a world characterized by advanced technology and increased electronification of data spawning an era referred to as "electronic government, or e-government." This era is largely a result of the rise of the Internet and the speed and frequency with which information is collected, stored, processed, and shared.

The Privacy Act remains the primary law regulating the federal government's use of personal information and regulates federal agencies' collection, maintenance, use and dissemination of personal information. Table 1 outlines the key protections afforded under the Privacy Act that provide a framework for fair information practices (FIP).

Table 1. Privacy Act of 1974 Protections (Fair Information Practices)
Prevention of secret systems of records.[14] Whenever an agency establishes or changes a system of records, it must publish in the Federal Register a notice known as a System of Records Notice (SORN). The notice must contain the name and location of the system, the categories of individuals on whom records are maintained in the system, the uses of the system, and other information.
Collection of only necessary information. Under the Privacy Act, agencies are permitted to maintain personal information about an individual only when it is relevant and necessary to accomplish a purpose the agency is authorized to perform by statute or executive order.
Ensuring data quality. Agencies are required to maintain all records used in making any determination about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. This provision is specifically meant to protect against erroneous decisions.
Information security. Agencies are required to establish appropriate administrative, technical,

[14] The term "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C.§552a(a).

and physical security protections to ensure the confidentiality of records and to protect against anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.
Access and correction. Individuals are entitled to obtain a copy of records about themselves and to request correction of any information that is not accurate, relevant, timely, or complete.
Accounting for disclosures. Agencies must keep an accounting of the date, nature, and purpose of each disclosure of personal information to other agencies.
Training employees. Agencies are required to provide training on the requirements of the Act to employees and contractors involved in the design, development, operation, or maintenance of any system of records.
Providing notice of exemptions. Agencies are permitted to exempt certain categories of records from some of the Act's provisions, but before an agency can do so, it must do so by means of a process in which it justifies the exemption.

Source: The Privacy Act of 1974, 5 U.S.C. §552a.

These principles are important to understand because of how they influence the process by which organizations design their unique approaches to the implementation of privacy policy, particularly the PIA process. Fair information practices become even more important in the analysis presented in Chapter 5 of this study because they have stood the test of time and application and remain at the core of basic privacy protection in organizations.

Privacy and E-Government: The Emergence of the Privacy Impact Assessment

The E-Gov Act was part of an initiative to expand e-government under the President's Management Agenda in 2001 and was aimed at ensuring the Federal government's annual investment in information technology significantly improved the government's ability to service citizens and to ensure systems are secure, delivered on time and on budget. Expanding e-government marked a noteworthy evolution in how the government looked at the use of technology to achieve the various purposes set forth by agency enabling statutes. The requirements to conduct risk assessments (i.e. PIAs) that would specifically identify and evaluate the potential threats to individual privacy and identify appropriate risk mitigation measures, marked an important step towards updating government privacy policy and focusing on measurable outcomes.

In particular, Section 208 of the E-Gov Act was designed to "ensure sufficient protections for the privacy of personal information" (PL 107-347, Section 208). To improve how government collects, manages and uses personal information about individuals, Section 208 required agencies to conduct PIAs. The Office of Management and Budget (OMB) was given authority for oversight and ensuring the implementation of PIAs across federal agencies as well as for providing guidance to agencies.

In 2003, the OMB issued a Memorandum to the heads of the executive departments and agencies. The Memorandum provided guidance to the agencies for implementing the provisions of the E-Gov Act and outlined the key elements that were required to be included in a PIA as outlined below.

Table 2: Essential Elements of the PIA required by the Office of Management and Budget

OMB Memo M-03-22 requires that PIAs have the following required minimal content:

1. What information is to be collected, (e.g., the nature and source);
2. Why the information is being collected (e.g., to determine eligibility);
3. The intended uses of the information (e.g., to verify existing data);
4. With whom the information will be shared (e.g., another agency);
5. What opportunities individuals have to decline to provide (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than the required or authorized uses), and how individuals can grant consent;
6. How the information will be secured (e.g., administrative and technological controls); and
7. Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

Source: U.S. Office of Management and Budget, Executive Office of the President (2003). *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002*, (M-03-22). Washington, D.C. Retrieved from http://www.whitehouse .gov/omb/memoranda_m03-22.

The primary intent of the PIA process is to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy *training*, gathering data from a project on privacy issues *(analysis)*, identifying and resolving the privacy risks *(review)*, and *approval*

by the designated senior agency official responsible for the privacy functions.[15] The actual preparation of the PIA document requires the system owner and developer to answer a broad range of privacy questions, including but not limited to the essential elements identified by the OMB as outlined in Table 2.

The Privacy Impact Assessment Legal Mandate

Section 208(b) of the E-Gov Act required agencies to perform a PIA before (i) developing or procuring new technology that collects, maintains, or disseminates personally identifiable information (PII), or (ii) initiating new collections of PII. These assessments are supposed to be public documents that contain a description of the project, a risk assessment, a discussion of potential threats to privacy and ways to mitigate those risks. In this way, PIAs are intended to ensure that privacy concerns are considered as part of the design of information systems and that the public has access to this element of the decision making process.

Over the last several years, PIAs have become an essential tool to help protect privacy. However, it is important to acknowledge the significance of the need for information security requirements to secure the information and systems that support federal agency operations and assets (i.e. an agency-wide information security program, evaluation and reporting requirements for federal agencies). The Federal Information Security Management Act of 2002 (FISMA) was created as a component of the E-Gov Act that responded to growing concerns about significant vulnerabilities in federal computer systems.

The FISMA (44 U.S.C. § 3541, *et seq.*) requires each agency to document and implement procedures for detecting, reporting and responding to security incidents. Agencies must also notify and consult with the federal information security incident center operated by the

[15] Federal Chief Information Officer's Council (2000). *Best practices: Privacy – Internal Revenue Service model information technology privacy impact assessment.* Washington, D.C. Retrieved from http://www.cio.gov.

Department of Homeland Security (DHS IRC). The FISMA also reports on the number of reported security incidents each year to the DHS IRC. The relevance of data breach on the PIA implementation process is discussed in the analysis of the VA in Chapter 5.

As FISMA has evolved over the years, so has the PIA, representing the increasing relationship between the two mandates with FISMA serving as a key benchmarking method for assessing agency enactment of privacy law. The FISMA has evolved by continuing to increase the reporting of key privacy measures and to provide more information to the public on agency privacy efforts.

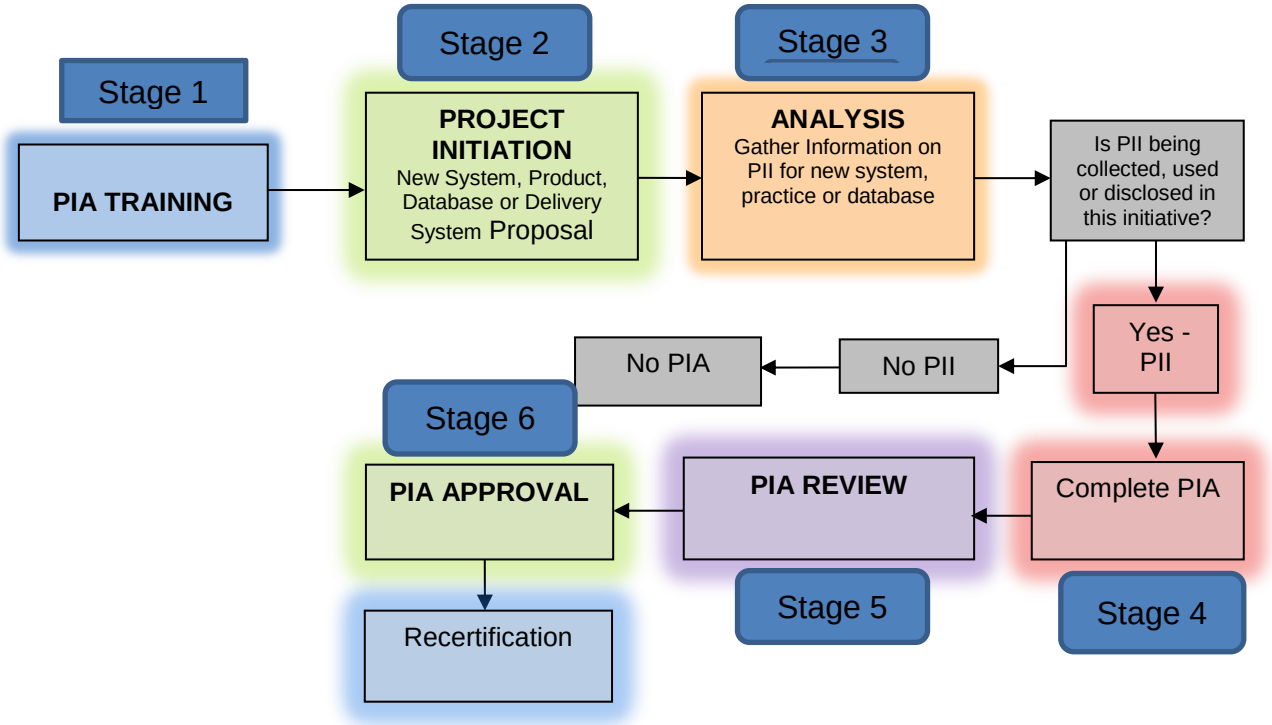
The FISMA reports submitted to Congress reflect reviews conducted by agency inspectors general and chief information security officers on their implementations of PIA requirements. The reports are worthy of mention because later analysis will show that while some agencies have set a high standard for the quality of their PIAs and have continued to improve them over time, other agencies have fallen short. Thus, these reports provide a method for evaluating whether or not an agency's PIA process is merely a "checkmark" to complete as part of a compliance process or whether it is more of an evolving process for agencies.

While FISMA requires PIA reporting from the agencies, the process itself still remains ambiguous and inconsistent across federal agencies. For instance, even those agencies that prepare in-depth PIAs are likely to complete them *after* a project has been developed and approved, whereas PIAs are supposed to inform the decision making process, not ratify it. The PIA should be prepared early in the system design process to identify privacy problems in advance of completing the system design. They cannot serve this crucial role if they are done after design is completed. A closer look at the mechanics of the PIA will illustrate the importance of conducting the process at the front-end of a project.

The Mechanics of a Privacy Impact Assessment

When a new system, product, practices, database or delivery system is proposed within an agency, it must justify itself within the agency budget, therefore, the procurement of any new information technology system or changes, requires a PIA. The system owner is responsible for gathering the relevant information to complete the PIA for the new system, practice, or database. The completed PIA is then reviewed by the designated agency team or official. The reviewing team or official may schedule a meeting upon reviewing the PIA to discuss any comments, questions or feedback. When the reviewing team or official is satisfied that the PIA is complete and accurate it is then approved and recorded in the appropriate database and then submitted to the OMB as the oversight body. Recertification launches the process all over again and is required when any technological changes are made to the system. Figure 1 illustrates the general mechanics of the PIA process.

Figure 1. Mechanics of the PIA



Note. Stage 1 begins with Training. Training describes the PIA process and provides detail about the privacy issues and questions to be answered to complete the PIA. The intended audience is the personnel responsible for writing the PIA document (e.g., system owner or developer). Stage 2 is the Project Initiation which takes place in the early stages of the development of a system and in some instances, preliminary new systems, systems under development, or systems undergoing major modifications are required to complete a PIA. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. Stage 3 is the Analysis that is based on previous privacy training. System owners or developers gather data from a project on privacy issues and identify and resolve the privacy risks. Together they must address what data will be collected, how and who will use the data, and whether the implementation presents any threats to privacy. Stage 4 is the Review of the completed PIA by a senior agency privacy official. The review is intended to identify privacy risks in the system. Stage 5 is the Approval of the PIA and is typically granted by a senior agency privacy official. Stage 6 is Recertification. The FISMA requires that systems be recertified every three (3) years.

Source: Federal Chief Information Officer's Council (2000). *Best practices: privacy*. Retrieved from http://www.cio.gov/documents/pia_for_it_irs_model.pdf.

In order for agency staff to properly complete a PIA, they must first be properly trained; therefore, the PIA process ultimately begins with training. Professional expertise is a factor that influences the process from beginning to end and is closely interrelated to both training and to the organizational structure that unfolds to support policy implementation. Each of these components is described in greater detail in the next section.

Factors that Influence the PIA: Training, Professional Expertise, & Organizational Structure

Several factors can influence the PIA process within any organization ranging from the organizational structure, culture,[16] leadership, budget/resources constraints, training, and education or level of expertise of the agency personnel (professionalism). This study's focus is limited to the influence of only three of these factors: training, professional expertise, and organizational structure. Each of these is given a cursory overview below and will be further detailed in Chapter 3 – Research Design and Chapter 5 – Case Study Analysis.

[16] Organizational culture has been conceptualized in numerous ways by neoinstitutional (DiMaggio & Powell, 1983; Meyer & Rowan, 1977; Scott & Meyer, 1983; and Scott, 1995) and organizational culture theorists (Martin, 1992; Pettigrew, 1979; and Smirchich, 1983). Mahler (1997) applies a common conceptual definition that "refers to the collectively held and symbolically represented ideas members of an organization have about the meaning of the organization and the work they do" (p. 526). Organizational culture used in this study is based on Edelman's (1997) use of the term based in the sociological and neoinstitutional traditions. Both focus on the creation of collective meaning structures through social processes.

Training

It is worthwhile to note that privacy training in federal agencies is not limited to only the PIA. However, this research is only concerned with training to support the PIA process because preparing a PIA document requires specialized training and represents the critical first step for completing a PIA. Therefore, PIA training is organized by agencies (usually the department or office with privacy policy authority) to describe the PIA process and provide detail about the privacy issues and privacy questions to be answered to complete a PIA. In this study, the VA has a Privacy Office that provides relevant training, while in the USPS this function is assigned to the Department of Consumer Affairs.

The typical audience for this training is the personnel that will be responsible for writing the PIA document generally, system owners and developers. The training provides the system owner or developer with the expertise and knowledge to determine the scope of the PIA based on the proposed project initiative. The training further provides staff with the appropriate knowledge related to how the agency has designed and structured itself around this process – the policies and procedures that have been established by the organization to support the process as well as the hierarchy of authority that governs the actual process itself. More importantly, staff must be trained to identify the necessary privacy risks involved with the project.

Staff is trained on how to provide a description and analysis of the business processes, architecture and detailed data flows contemplated for the proposal. This step helps to depict the personal information flows. The privacy analysis examines the data flows in the context of applicable privacy policies and legislation. Questionnaires are used as a checklist to facilitate the identification of major privacy risks or vulnerabilities associated with the proposal.

The actual report that is produced from the data analysis builds upon the outcomes from the previous steps and results in a document evaluation of the privacy risks and the associated implications of those risks along with a discussion of possible remedies or mitigation strategies. In this way, the PIA report can serve as an effective communications tool used by a variety of stakeholders both internal and external to the organization.

The report is granted final approval by the designated senior official for privacy within the agency and in some instances, by a team of senior officials to leverage a range of expertise.

Training is often also available outside of an agency through the federal government in the form of workshops and other means. For example, the DHS has regularly held workshops for operationalizing privacy. Table 3 illustrates a sample training workshop agenda and the key elements that need to be addressed as part of that training.

Table 3. Sample PIA Training Workshop Agenda

Session 1: Backgrounder on Privacy Impact Assessments
• History of the PIA • Reasons for conducting a PIA • PIA Goals • PIA Requirements • When to conduct a PIA • Staged nature of the PIA as it follows the system design lifecycle throughout conceptual design, detailed design and implementation • Global experience with PIAs • Identification of all major current methodologies in U.S./government and some comparisons
Session 2: Overview of Organization PIA Methodology
• Information gathering • Business process diagram • Data flow analysis • Privacy risk identification • Recommendations for risk mitigation
Session 3: PIA Exercise - Privacy Risk Identification
• Case study approach for identifying the major privacy risks associated with the implementation of a new information system (e.g., healthcare, personnel management, etc.). Participants learn how to develop and analyze business process diagrams and data flow analyses, critical tools for the successful completion of any PIA.
Session 4: How to Solve Common PIA Challenges

- Forming the right PIA team – recruitment and training
- Define the scope of the PIA and establish an effective project plan
- Learn how to conduct PIAs with minimal impact on the timelines of your system or program
- Securing stakeholder buy-in - how to gain senior management and stakeholder support by framing your recommendations in a report that will facilitate the development and implementation of your system or program

Source: Priva-C. Retrieved on January 11, 2012 from http://www.priva-c.com/corporate/training_pia.asp.

While the training component of the PIA process may seem fairly straightforward and rudimentary, in most cases, each agency develops a customized approach not only to conducting PIAs, but also to the training component.

The next section discusses the relevance of professional expertise to the PIA implementation process.

Professional Expertise

The completion of the PIA may need to draw upon a wide range of professional expertise or skill sets that can include: privacy and or legal expertise, operational and business design expertise, technology and systems expertise, and information and records management skills.

Privacy expertise is fundamental to provide advice and recommendations with respect to relevant program statutes, such as the Privacy Act and the Freedom of Information Act (FOIA). But privacy expertise expands to include well-developed knowledge of privacy issues, current privacy developments, as well as national and international privacy standards. Generally, privacy expertise is held by a privacy officer within an organization which often is structurally housed in an office designated for a chief privacy officer (CPO). The CPO position is given more attention in the next section because of the linkages between title and the creation of special offices to the organizational structure.

Legal expertise provides advice and recommendations with respect to privacy and program authorities, institutional oversight mechanisms and potential conflicts where multiple statutes or jurisdictions are involved.

Operational program and organizational design skills are important to examine proposals in terms of operational flow and context, stakeholder analysis, public/private partnerships, governance structures and feasibility in terms of mitigation strategies.

Technology and systems expertise is critical to provide technical and systems advice on mainframe and legacy systems, internet tools and system interfaces, information, security, technical architecture, and data flows. Together, operational, technical and systems expertise are characteristics that are related to the title and offices for a chief information officer (CIO) and /or chief information security officer (CISO). These positions are given more attention in the next section as they relate to the organizational structure.

Finally, information and records management skills are necessary to contribute expertise on how records are kept and the retention of information. Records management is also usually responsible for all information related to systems of records (SORNs) and closely related to FOIA.

Prominent credentialing and certification programs are also a critical factor in terms of expertise. The credentials for a Certified Information Protection Professional, or CIPP, the Certified Information Security Systems Professional, or CISSP, and Certified Records Manager, or CRM, are recognized as legitimate sources of training for privacy professionals and information security professionals, respectively.

The last factor to review is organizational structure.

Organizational Structure

The organizational structure that supports the PIA process is reflected by the various levels of expertise needed to effectively implement policy. However, any organizational structure should be supported by the necessary training programs. The underlying mission of the

agency influences the shape of the organizational structure that emerges to support policy implementation and the evolution of this structure over time. Critical and external events may also impact the organizational structure. The structure that takes shapes tends to vary by agency and can be driven by any number of factors from mission, or culture, to the level of resources available. Chapters 3 and 5 will further explore how these and other factors influence the organizational structure that unfolds to support the PIA implementation process.

The common organizational framework that supports a PIA includes a Chief Information Officer (CIO), a Privacy Director or Senior Privacy Official, and a Chief Information Security Office at the top of the hierarchy. The OMB actually requires that agencies designate a senior official for privacy. This designation can often reside with the CPO, but it is not uncommon for this designation to fall under the CIO. Historically, the trend has been toward the latter; however, recent years have seen an increasing trend in assigning this authority and accountability with the CPO.

The functions that each of these offices fulfill is broad and varied across federal agencies. These functions are generally organized to support oversight, management of the plan (or process), management of the resources, management of the information architecture, and to control and improve operations. Some offices or departments that may be created to support these functions include information protection and risk management; IT enterprise, strategy, policy, plans and programs; IT resource management; enterprise development; and enterprise operations and field development.

The managerial position of a CPO is designed to address growing concerns over information privacy abuse, potential lawsuits, and threats of increased privacy legislation. Therefore, the CPO helps the organization to address and cope with broad information privacy

implications within and across the organization. The breadth of accountability that can rest with a CPO is expansive and requires the assumption of multiple roles at the higher levels of the organization. These multiple roles and responsibilities can fall into four (4) main areas: information (monitor, disseminator, spokesperson), interpersonal (figurehead, liaison), conflict management (disturbance handler, negotiator, breach resolution), and strategic management (entrepreneur). This requires that a CPO possess strong organizational, communications, and technical skills (Kayworth, Brocator, & Whitten, 2005).

A long-running debate has existed about whether the role of the CPO belongs in legal, IT or in risk or compliance. Since information governance is about how we create information, how we keep it safe and secure and accessible during its lifecycle and how we thoughtfully dispose of it, the roles assigned to a CPO continue to expand. This expansion of responsibility can include document management and data lifecycle, data retention, e-discovery and a host of other disciplines, under the information governance umbrella.

The CPO ultimately helps to create a multidisciplinary approach to data governance – to both operationalize it and create a sustainable policy on the IT side of the organization. Ideally, a CPO should possess a vision of information as a legitimate asset of companies and be able to articulate that vision across departments.

In terms of the PIA, a CPO is responsible for the review of PIAs from beginning to end, for ensuring that PIAs get posted to the agency's website, to ensuring that disclosures regarding the types of PII used in the PIAs are adequate, and that descriptions of the agency's use of PII is also adequate. There is considerable support to hypothesize that the CPO has been a source of strength behind agency PIA procedures (Goodchild, 2008).

Ultimately, the CPO solidifies the privacy side of the organizational infrastructure. The security side of the infrastructure begins with the CISO. Naturally, strong cooperation and communication between these two structural components of an organization is critical to the PIA process and design. Ideally, the relationship should reflect a partnership. This relationship is closely tied to the office of information security and in some cases to the office of a chief technology officer.

The CISO governs the infrastructure for an agency's security controls. He is accountable for preventing critical events such as data breaches which can negatively affect the organization resulting in monetary damages, legal action, and reputational damage. Therefore, the CISO should have significant security experience since their main task is to develop, implement and monitor the information security program for the organization. To realize these responsibilities, the CISO requires a dedicated staff of security personnel to help execute the information security program (Raymond and LeClerc, 2006).

The CIO rounds out the organizational structure to support the PIA process. This title is commonly given to the most senior executive in an enterprise responsible for the IT and computer systems that support enterprise goals. The CIO also reports directly to the chief executive office (CEO) of an organization resulting in considerable authority and a close working relationship with the CEO at a very strategic level. In these case studies, the CEO is comparable to the Secretary of the VA and the Postmaster General of the USPS.

Historically, the CIO has been the highest ranking technology executive; however, recent years have witnessed the increased designation of a chief technology officer (CTO) to supersede the CIO or to work in conjunction with the office of the CIO. A notable example of this trend is

represented by President Obama's appointment of a CTO to the Executive Office of the White House.

Finally, records management expertise deserves special consideration as this role has acquired more authority and recognition in organizations and may often be housed under the authority of the CIO (e.g., Environmental Protection Agency) although records management can also fall within the purview of the CPO. These professionals are often participants in the American Records Management Association (ARMA), which recently promulgated generally accepted recordkeeping principles (GARP), thereby defining the discipline of records management and raising this function to a new level in organizations.

This area of the organization has grown in stature because a primary consideration for any organization that conducts a privacy audit or assessment is the organization's recordkeeping system; in particular; records professionals and their duties related to information used by the organization. The records analyst can and should be a key component to preserving privacy of all types of information in large organizations (Duff, Smieliauskas, & Yoos, 2001). Therefore, the records management function is increasingly critical to the organizational structure supporting the PIA process.

A relationship between records management and IT is important to collaborate on the impact of the evolution of new technology and applications on organizational recordkeeping. For example, the emergence of cloud computing is a ripe area for collaboration between IT and records management because the records management professionals need to understand how to manage records that are held in the cloud.[17] Another example would include the need for records management to understand how to leverage social media, such as Facebook, for critical functions such as correspondence for e-discovery (Hoke, 2011). It follows that the inclusion of

[17] Cloud computing is the delivery of computing and storage capacity as a service to a community of end-recipients.

information relevant to systems of record in the PIA requires knowledgeable records management personnel and the ability for IT staff to consult with this staff (Raths, 2010).

Roles and responsibilities in the PIA process may vary depending upon the organizational structure, size, and the PIA approach employed. Table 4 illustrates some of the common roles and responsibilities in supporting PIAs.

Table 4. Roles and Responsibilities to Support PIA

Role	Establish Organizational Imperative	Oversee PIA Process	Initiate PIA	Conduct PIA (collect data)	Compile Findings	Review Findings & Assess Risks	Define Design Requirements to Address Risks	Implement Remediation
Executive Sponsor	**X**	**X**						
Governance Committee		**X**						
System Owner / Developer			**X**	**X**	**X**			**X**
CIO			**X**				**X**	
CISO			**X**				**X**	
CPO						**X**	**X**	

Summary

The PIA has emerged as the primary symbol and most rational way for agencies to reflect privacy policy implementation as required under the E-Gov Act. However, each federal agency takes a unique approach to this implementation process. While the OMB has begun to take steps to address the inconsistent implementation of PIAs, its use as a tool for analysis and change should be a starting point for developing best practices for all federal agencies.

Therefore, this research begins with an empirical analysis of the PIA as a process within each agency, the factors that influence this process, and how the process changes over time. This study review trends in FISMA reporting between 2004 and 2010 to analyze shifts in the VA's approach to implementation. The USPS is exempt from this reporting requirement precluding the ability to make a similar analysis.

The results show that the PIA process can be evaluated as a tool for raising the level of attention to privacy within an organization, as an accountability mechanism, and as a means for bringing greater transparency to IT development and information management within organizations. Ultimately, the PIA is a risk assessment tool for decisionmakers that can address not only the legal, but also the moral and ethical issues of information protection.

The next chapter describes the research design used for this study.

CHAPTER THREE – RESEARCH DESIGN

This study was conducted to respond to the primary research question, "How have Privacy Impact Assessments (PIAs) been implemented within the USPS and the VA and how has this process changed over time?" Two case studies of each agency's approach to PIA implementation were analyzed using qualitative and process data collected through interviews with agency staff and further informed by extensive document analysis. The identification of stages in the PIA process and the use of two time periods provided an empirical framework for understanding the influence of both internal and external factors on the process over time (e.g., changes in the law, changes in values, and other critical events). Three key factors to the PIA process were also analyzed to understand their impact – training, professional expertise, and organizational structure. These factors are supported in the literature and based on preliminary analysis of the PIA process.

This research design is theoretically supported by Edelman's (1999, 1992) model which provides a framework for studying the *process* by which agencies implement ambiguous law and policy and adapt the law to fit their own interests. Edelman's sociology of law lens also helps to understand how implementation becomes understood within organizations because the factors that influence this process are internal to the organization. In the same fashion, this study examines the PIA process as a means of the legal construction of privacy policy and leverages Edelman's approach to studying the implementation of EEO/AA law in organizations.

While Edelman (1992) studies the impact of organizational *structures* on policy implementation, she concludes that structures (such as EEO/AA offices) do not represent the full extent of organization compliance activities. Other factors such as professional expertise and training influence the rate at which organizations create complex organizational structures

(Edelman, 1990, 1992). This conclusion supports the use of process analysis to understand the underlying social processes that transpire within the organization to effect policy implementation. Included in these social processes is the influence of professions, which Edelman (1999) contends are highly influential to the design and process of policy implementation.

Professional expertise is interrelated to changes in organizational structure and to the training necessary to support policy implementation. The variables for training and professional expertise represent the human dimension of the implementation process and findings show how this dimension meets the structural dimension. The findings also show how various professions develop, coalesce, and evolve over time to support the implementation process. Training also evolves as a critical element that underpins the entire implementation process. The influence of these variables reflects a recursive relationship and one that shapes organizational processes that have different characteristics making the findings descriptively theoretical.

Using this research approach and design, this study aims to inform the field of public administration and policy about the richness of the policy implementation process and to provide a model for future research into the public management challenges that are particularly germane to privacy policy and its enactment in organizations. For public administration scholars, understanding the underlying process of PIA implementation will provide valuable insight into understanding how privacy policy becomes manifest in organizations by specifically examining the administrative capacities[18] and professional perspectives that influence implementation process.

[18] Addison (2009) describes administrative capacity as a core concept in the public administration literature concerned with capacity building as a tool used for policy implementation.

The findings and conclusions show that the USPS and the VA take distinct approaches to implementation employing processes that have different characteristics; policy consistency is challenged by varied organizational capacities and perspectives. However, the conclusions also show that design is an important factor at the beginning of any policy implementation process that requires a strategic vision that takes into consideration the need for specialized and broad organizational training, professional expertise, and changes to organizational structure.

Each organization approaches the policy implementation process differently and the factors that influence this approach are expansive from agency culture, to internal processes, to availability of resources, and more. The characteristics of the implementation process can also help us to understand the subsequent policy outcomes by studying the internal nuances of organizations. An understanding of process of implementation lends itself to findings about how organizations learn in response to uncertainty in the policy and law environment.

Overall, this study's research design leads to better understanding of the qualities of the PIA implementation process as a vehicle for enacting privacy policy. The qualities of this process are malleable or can be established at the beginning of the process as goals. In a sense, the study of process is a study in strategy and of "strategy in the making" (Feldman & Orlikowski, Forthcoming). Feldman and Orlikowski describe "strategy in the making" as "a dynamic accomplishment rather than a static outcome."

The following section elaborates on the research design used in this study.

Research Design

This study initially set out to understand the origins and expanse of U.S. privacy policy and related laws in the U.S. and the challenges faced by government organizations that collect vast amounts of sensitive personal information. These privacy challenges have been exacerbated by rapid advances in technology, cybersecurity threats and incidents, and the need to protect

citizens' sensitive personal information. In order to narrow this research design, this study focused on the privacy requirements (i.e. PIAs) under the e-Gov Act. Case study methodology afforded a closer review of how this implementation process unfolded over time and led to the overarching research question, a critical first step in any research design: *How have Privacy Impact Assessments (PIAs) been implemented within the USPS and the VA and how has this process changed over time?*

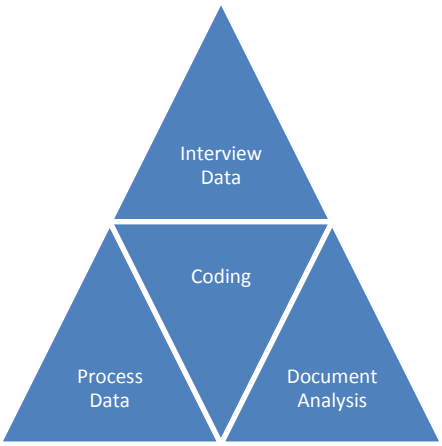
A case study design was also used because it is a useful method to build from Edelman's (1999, 1992) research and theory. In this study, the use of case study methods is applied to contemporary management situations to support a foundation for explaining the policy implementation process, its challenges, and dynamics. According to Yin (1994), case studies also help to answer research questions about the "how" or "why" of a particular issue and teach researchers about new management techniques, programs to solve chronic problems, or strategies to improve the quality of an agency. Hence, this empirical inquiry explores in depth the people, policies, structures, and other facets of policy implementation. This approach provides rich insights into individuals and their relationship to the organization, to their profession, and to the law that underpins broad policy efforts.

The case study was supported by rich process data and limited interview data as well as expansive document analysis. For this reason, the VA case study is the predominant focus of this study because it is supported by broader interview data. The USPS case study serves as a minor case study because of the limited interview data. However, the PIA process is studied in both organizations leveraging influential factors inspired by Edelman (1999, 1992) but also based on my own reflections from earlier analysis of the agencies. The data collected is

important to understanding the dimensions of these influential factors and how the processes within each organization have different characteristics that lead to different policy outcomes.

The research design is depicted in Figure 2 and each facet of the design is treated in further detail throughout this chapter beginning with an explanation of the case study methodology.

Figure 2. Research Design to Support Case Study



The steps taken in this research design are described below.

1. **Research question**: Identifying a research question to frame the study was the critical first step. Identifying the PIA as the focal process being traced and explained also led to the identification of influential factors that inform change over time.

2. **Select case studies**: Once the research question was identified, several federal agencies were considered based on size, expanse of data collection, and critical events.

3. **Design survey questionnaire/interview questionnaire**: The interview questionnaire was designed to gather detailed information about the PIA, the implementation process, and the influential factors on this process over time.

4. **Recruit interviewees and schedule interviews**: Interview candidates were identified based on their respective roles in the PIA process as well as their expertise.

5. **Data Collection:** The interview data was enhanced by the collection of process data, document analysis, and a literature review. The data was organized treating the PIA

as the focal process being traced and explained and training, professional expertise, and organizational structure were the treated as factors that influence this process.

6. **Data Coding**: Data was coded according to the focus process, or the PIA process, the factors that influence the process, and by the identification of critical events that influenced this range of factors such as changes in PIA implementation process over time (evolution), organizational patterns, external events such as data breach, changes in the legal mandate, changes in reporting requirements, and changes in leadership.

7. **Data Analysis**: The analysis was enriched with process data and the creation of a structure for analysis using stages and time periods for the PIA. The analysis was further informed by Edelman's research model.

8. **Findings and conclusions**: The findings and conclusions point to organizational dynamics that make any policy implementation effort distinctive, which also shapes various policy outcomes. The findings also have implications for future policy and research, particularly for public management considerations to support extensive privacy policy on a national level.

As noted above, once the research question was identified, several federal agencies were considered based on size, expanse of data collection, critical events, and the historical context of privacy in these organizations. The following section describes the case study selection process.

Case Study Selection Process

Defining the case studies is an important component of data gathering, together with creating the appropriate research questions, and identifying supporting data sources (Crabtree & Miller, 1992; Creswell, 2003; Kirk & Miller, 1986; O'Sullivan & Rassel, 1995; Yin, 1994). The examination of different sources of information from documents, interviews, and participant and direct observation is a demonstrated strength of case study research (Denzin & Lincoln, 2005). The identification of relevant data to be collected is important in defining the case that is explored and multi-source information strengthens the study.

The cases for this study were carefully selected based on their sheer size and relevant impact on privacy given the extent of personal and sensitive information that these organizations handle on a daily basis. These agencies also have a strong proximity to the public sphere and are

public-facing in that their practices for handling sensitive information must be transparent and held accountable for data compromises. Edelman (1992) uses these same characteristics in her research and uses the term "public sphere" to mean "the culture surrounding the *federal* state and the federal legal order" (p. 1548). In essence, Edelman suggests that organizations that are closer to the public sphere are more sensitive to legal environments for many reasons, one of which is they "operate in an environment in which rule-based governance, bureaucracy, and notions of citizens' rights are highly institutionalized (1990, 1992, p. 1549).

The USPS, in particular, stood out as a model for overall PIA implementation across federal agencies based on a historical commitment to the protection of privacy but more specifically because it started conducting PIAs before they were mandated. While this is not a comparative case study analysis, the USPS provided insights as a minor case study in contrast to the predominant focus on the VA. The processes undertaken by both agencies had different contexts and made each approach to policy implementation distinct. These contexts will be further addressed in Chapters 4 and 5. Different characteristics of these processes in each agency reveal the diversity of their respective approaches.

The VA case study is the predominant focus of this research and shows an implementation approach that was different compared to that of the USPS. Its approach to PIA implementation was largely impacted by the data breaches in 2006 and 2007, but also influenced by frequent turnover in leadership held by several CIOs who were political appointees as well as mounting pressures to modernize its IT infrastructure and become more centralized, and growing fiscal pressures and political scrutiny. Data breach, in particular, was a problem that the PIA requirement was intended to address. These critical events and environmental context present an

opportunity to identify patterns in the implementation process aided by a focus on the influence of training, professional expertise, and organizational structure.

The findings show that the USPS approach to implementation was highly centralized, while the VA was decentralized and often fragmented. The USPS approach faced similar pressures to the VA in terms of congressional scrutiny, growing financial crisis, and struggles to adapt to a modernized IT environment. In contrast to the VA, the USPS was also scrutinized by congress and the GAO over privacy concerns throughout the 1990s particularly because it is a quasi-government agency engaged in business-like activities. Therefore, the USPS is subject to different privacy laws that do not apply in the private sector and privacy concerns arise over the use of sensitive personal information such as Social Security Numbers, addresses, and credit card. A pivotal issue was brought to light by a 1996 GAO report regarding the need to protect the privacy of address changes. Specifically, the address correction service provided by the USPS came under question under the Privacy Act in terms of whether or not this service was a "routine use" of data information that would be permitted under the law (Walters, 2008).

The next section describes the data collection process and procedures used in this study.

Data Collection Procedures and Process

This study involved a combination of data collection methods from review and analysis of relevant literature, to elite interviews, and extensive document analysis from the agencies and various government reports and other outside sources. The nature of the data collection afforded flexibility in the types of datum collected from each case within the study, providing for a richer understanding and analysis of organizational behavior and the social processes that cannot be achieved using quantitative research (Yin, 1994). This is particularly true in understanding how organizations respond to their legal environments, as evidenced in Edelman's (1997) research.

Therefore, process data collected through interviews with elite staff enhanced the analysis of how things evolve over time and why they evolve in this way (Van de Ven & Huber, 1990). Process data afforded the ability to learn from stories about events and activities ordered over time. In this way, process data enabled a means for conceptualizing events and detecting patterns among them (Langley, 1999). The most common form of patterns is the linear sequence of "phases" that occur over time to produce a given result (e.g., Burgelman, 1983; Rogers, 1983, in Langley, 1999), another approach that was leveraged in this study. Process research may also deal with relationships between people or with the cognitions and emotions of individuals at they interpret and react to events (Isabella, 1990; Peterson, 1998, in Langley, 1999). The complexity of process data is a reflection of the complexity of the organizational phenomena we are attempting to understand.

The approach to literature, content and document analysis is addressed in the next section.

Content / Document and Literature Analysis

Once the agencies for the case studies were selected, the document analysis could begin. Several types of documents were reviewed in this study ranging from agency documentation, policies and procedures related to the PIA process, as well as GAO reports, FISMA reports, congressional testimony, and content from privacy professional media and advocacy groups. Table 5 outlines and categorizes the range of documents that were consulted and analyzed in this research.

Table 5. Document Analysis

	VA	USPS
Agency Documentation	• U.S. Department of Veterans Affairs (2012). *The VA's battle for privacy protection: Best Practice from the digital front lines.* PowerPoint presentation from the IAPP Conference on March 7, 2012 by John Buck, Director, Office of Privacy and Records Management. • VA History in Brief (n.d.) • U.S. Department of Veterans Affairs U.S. Department of Veterans Affairs. (2010) *2010 Organizational Briefing Book.* Washington, D.C. • U.S. Department of Veterans Affairs (2008) *Eliminating the unnecessary collection and use of Social Security Numbers at the Department of Veterans Affairs*. • U.S. Department of Veterans Affairs (2008). *VA Directive 6507 – Reducing the use of SSNs* • U.S. Department of Veterans Affairs. (2008). *VA Directive 6502 - Enterprise privacy program.* • U.S. Department of Veterans Affairs. (2007). *VA Handbook 6500 - Information security program.* • U.S. Department of Veterans Affairs. (2004). *VA Handbook 2502.2 – Privacy impact assessment.* • U.S. Department of Veterans Affairs Office of Inspector General (2006). *Review of issues related to the loss of VA information involving the identity of millions of veterans.* (Report No. 06-02238-163). • U.S. Department of Veterans Affairs (2006). Directive by the Secretary of Veterans Affairs R. James Nicholson to All VA Supervisors on Information Security. • U.S. Department of Veterans Affairs (2006).VA Secretary Inserts New Leadership in Policy & Planning Office. • U.S. Department of Veterans Affairs. (2008) *Final information quality guidelines* • Putt, Stephania. (n.d.) *Role of the privacy office in VA research.* PowerPoint presentation. • Putt, Stephania. (2009). *Role of the privacy officer on the IRB.* PowerPoint presentation.	• U.S. Postal Service. (2009). I*nformation resource: Business impact assessmen*t. Raleigh, N.C. • U.S. Postal Service. (2007). U.S. Postal Service Annual Report 2007. • U.S. Postal Service. (2006). *Application business impact assessment.* Raleigh, N.C. • U.S. Postal Service (2005). *Handbook AS-353, Guide to privacy, the Freedom of Information Act, and records management*. • U.S. Postal Service. (2005). *Handbook AS-805, Information Security*. • *The United States Postal Service: An American History 1775- 2006.*
FISMA Reports	2004 – 2010	Not Available for USPS (Exempt)
GAO Reports	• U.S. Government Accountability Office (2008). *Privacy: Congress should consider alternatives for strengthening protection of personally identifiable information* (GAO-08-795T). Washington, D.C. • U.S. Government Accountability Office. (2008). *Privacy: Agencies should ensure that designated senior officials have oversight of key functions.* (GAO-08-603). Washington, D.C. • U.S. Government Accountability Office (2007).*Information security: Veterans affairs needs to address long-standing weaknesses.* (GAO-07-532T).Washington, D.C. • U.S. Government Accountability Office (2006). *Homeland security: Guidance and standards are needed for measuring the effectiveness of agencies' facility protection efforts.* (GAO-06-612). Washington, D.C. The report specifically named the VA as requiring guidance and standards for measuring performance in federal government facility protection. • U.S. Government Accountability Office (2006). *Veterans affairs: Leadership needed to address information security weaknesses and privacy issues*. (GAO-06-866T. Washington, D.C. • U.S. Government Accountability Office (2006). ―*Information security: Leadership needed to address weaknesses and privacy issues at Veterans Affairs.* (GAO-06-897T). Washington, D.C. • U.S. Government Accountability Office (2006). *Information technology: VA and DOD face challenges in completing key efforts*. (GAO-06-905T). Washington, D.C.	

	• U.S. Government Accountability Office (2003). Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate. *Privacy Act – OMB leadership needed to improve agency compliance* (GAO-03-304).
OMB Circulars	• U.S. Office of Management and Budget, Executive Office of the President. (2007). *Safeguarding against and responding to the breach of personally identifiable information* (M-07-16), requires agencies to develop and implement a breach notification plan and policy within 120 days. • U.S. Office of Management and Budget, Executive Office of the President. (2006). *Reporting incidents involving personally identifiable information and incorporating the cost for security in agency information technology investments.* (M-06-19), provides guidance to agencies for reporting security incidents involving PII and reminds agencies of existing requirements to protect PII. • U.S. Office of Management and Budget, Executive Office of the President. (2006). *Protection of sensitive agency information.* (Memorandum M-06-16), recommends that federal departments and agencies implement a series of controls to safeguard the remote access, transport, and storage of sensitive information, including PII. • U.S. Office of Management and Budget, Executive Office of the President. (2006). *Safeguarding personally identifiable information*, (M-06-15), re-emphasizes agency responsibilities to safeguard PII and train employees on their privacy responsibilities. The memorandum directs agencies to review their privacy policies and processes and take corrective action, as appropriate, to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, PII. • U.S. Office of Management and Budget, Executive Office of the President. (2005). *Designation of Senior Agency Officials for Privacy* (M-05-08), requests executive departments and agencies to designate a senior official with agency-wide responsibility for information privacy issues. • U.S. Office of Management and Budget, Executive Office of the President. (2003). *OMB Guidance for implementing the privacy provisions of the E-Government Act of 2002*, (M-03-22). Washington, D.C.
PIA Documentation	• Clarke, Roger. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, 25, 123-135. • Federal CIO Council. (2000). *Best practices: Privacy. Internal Revenue Service Model Information Technology Privacy Impact Assessment.* Retrieved from http://cio.gov. • Stewart, Blair. (1999). Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies. *Privacy Law & Policy Reporter*, 5 (8), 147-149. • Numerous PIA guidelines and policies across a broad range of federal agencies were reviewed, including PIA documentation from Canada and the UK, to deepen my knowledge of the PIA process.
Congressional Testimony	• Statement of Ari Schwartz before the Committee on Homeland Security and Governmental Affairs "Protecting Personal Information: Is the Federal Government Doing Enough?" June 18, 2008. http://www.cdt.org/testimony/20080618schwartz.pdf. • Statement of Ari Schwartz before the House Committee on Oversight and Government Affairs Subcommittee on Information Policy, Census, and National Archives "Privacy: The Use of Commercial Information Resellers by Federal Agencies" March 11, 2008 at http://www.cdt.org/testimony/20080618schwartz.pdf. • Statement of Linda D. Koontz before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives, "Privacy: Key Challenges Facing Federal Agencies" May 17, 2006 at http://www.gao.gov/htext/d06777t.html • Testimony of Linda D. Koontz, Director, Information Management Issues, Government Accountability Office, and Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office at a Hearing on the Repeated Failures of VA's Information Technology Management Before the Committee on Veterans' Affairs of the U.S. House of Representatives (June 14, 2006). http://www.gao.gov/htext/d06866t.html • Statement of Michael L. Staley, Assistant Inspector General for Audit, Department of Veterans Affairs at a Hearing on the Repeated Failures of VA's Information Technology Management Before the Committee on Veterans' Affairs of the U.S. House of Representatives (June 14, 2006). • Statement of R. James Nicholson, Secretary, Department of Veterans Affairs, at a Hearing on Failure of VA's Information Management Before the Committee on Veterans' Affairs of the U.S. House of Representatives (May 25, 2006). • Statement of George J. Opfer, Inspector General, Department of Veterans Affairs, at a Hearing on Failure of VA's Information Management Before the Committee on Veterans' Affairs of the U.S. House of Representatives (May 25, 2006). • Department of Veterans Affairs, Statement, *Statement of Secretary of Veterans Affairs R. James Nicholson on the Status of the Veterans' Data Theft* (May 24, 2006). • Department of Veterans Affairs, Statement, *A Statement from the Department of Veterans Affairs Announcing the Loss of Veterans' Personal Information* (May 22, 2006).

This broad range of documentation was analyzed using the lens of Edelman's (2004, 2003, 2001, 1999, 1997, 1992, 1990) research as a continuous thread throughout the study. Relevant literature was identified using electronic table of contents searches, access to academic journals, electronic academic database searches, electronic alerts through numerous selected social science databases using a combination of search terms to capture the work and application of Lauren Edelman, any academic aspect of the PIA as a tool for privacy policy implementation and extensive reviews of the privacy literature across several disciplines. Numerous books were also consulted for this research. Table 6 outlines the books used in this research with supporting explanation.

Table 6. Books Reviewed in this Study

Privacy Policy Broadly	• Bennett, C.J. & Raab, C.D. (2003). *The governance of privacy: Instruments in global perspective.* Burlington. • Solove, D.J. (2008). *Understanding privacy.* Boston, MA: Harvard University Press.
Public Administration & Policy and Privacy	• Etzioni, A. (1999). *The limits of privacy*. Basic Books. • Regan, P. (1995). *Legislating privacy: Technology, social values, and public policy.* University of North Carolina Press. • Regan, P. (1995). *Rethinking privacy: social values, technological change, and public policy*.
Case Study Approach	• Khademian, A.M. (1996). *Checking on banks: Autonomy and accountability in three federal agencies.* Washington, DC: The Brookings Institution. • Khademian, A.M. (1992). *The SEC and capital market regulation: The politics of expertise*. Pittsburgh, PA: University of Pittsburgh Press
Agency History	• Henkin, D.M. (2006). *The postal age: the emerging of modern communications in nineteenth-century America*. Chicago: University of Chicago Press. • U.S. Department of Veterans Affairs. *VA history in brief.* (n.d.) Retrieved from http://www.va.gov/opa/publications/archives/docs/history_in_brief.pdf.

The majority of my research was derived from the following academic journals: *The University of Chicago Law Review, Law & Policy, Computer Law & Security Review, Stanford Law Review, American Sociological Review, The Information Management Journal, American Journal of Sociology, Research in Social Stratification and Mobility, Annual Review of Sociology, Journal of Information Privacy and Security, Public Administration Review, Public*

Manager, Records Management Journal, Academy of Management Review, American Business Law Journal, Berkeley Technology Law Journal, Journal of Management Inquiry, and Ethics and Information Technology.

In my analysis of this documentation, special attention was paid to information that pertained to the PIA process and several influential factors such as training, professional expertise and organizational structure.

Once the documents were reviewed and analyzed to determine general findings, a set of interview questions was developed to guide the discussion with various representatives from the agencies and other relevant privacy experts. The preliminary document analysis also helped to identify key candidates for the interview process.

Interview Process

Interview data was the primary data utilized for my research. Any reference to personal communication in this research is followed by the date of the interview and refers to the data collected through my interviews using the Institutional Review Board (IRB) protocol. Support for elite interviews in conducting case study research is noted by Marshall & Rossman, 1995; and Crabtree & Miller, 1992. Marshall & Rossman (1995) consider the interview to be "the main road to multiple realities.". An interview affords the researcher with insights into policies, history, and future plans within an organization and specifically relevant to the research question. Elite interviewees can serve as "competent informants" and contribute insight and meaning to the interview (Berry, J.M., 2002). These observations resonated in my use of interviews. However, the development of interview questions and the selection of interviewees were critical elements to addressing the research question (Stake, 1995).

The interview questions were formulated for the purpose of answering the research question. Care was taken to select interviewees that had some role in the implementation of the PIA or extensive familiarity with the evolution of the process and influential factors within the organization. These individuals were career civil servants with expertise in records management, privacy, information security, IT, law, and risk management. The interviewees were identified through research on the organizational websites, through referrals from privacy professionals, using the IAPP membership catalog, identification through press media, agency policy materials reviewed online, and in reviewing congressional testimony.

Interviews were conducted following the protocol detailed for Research Involving Human Subjects in the Institutional Review Board (IRB) process utilized by Virginia Polytechnic Institute and State University. Prior to conducting the interviews for this study, I received my Certificate of Completion for Training in Human Subjects Protection on July 31, 2008.[19] The research met the exemption standard because the research was of minimal risk to the subjects, did not involve any special class of subjects, and involved the collection of or study of existing data and documents from sources that were publicly available. Verbal consent was obtained from the interviewees prior to recording the interviews and proper protocol was followed as detailed in the IRB process. The tape recordings allowed for deeper analysis and continual review to identify patterns to support findings and conclusions. The interviewees were not compensated or offered any incentive to participate in this study.

[19] IRB approval was granted effective July 31, 2008.

Table 7 shows the general interview guide that was used with agency officials.

Table 7: Interview Questionnaire / Guide

General

1. Can you please explain to me your role at the VA/USPS?

PIA Process and Implementation

2. What role do you play or have you played in the PIA/BIA process?
3. Please describe your knowledge of the PIA/BIA process to me? Can you provide any examples of PIAs/BIAs?
4. Please described the various stages of the PIA/BIA process?
5. In your view, how does the PIA/BIA process help or hinder your agency to manage information risk and privacy policy requirements?

Change Over Time

6. How has the PIA process within your agency changed over the years?
7. What events or factors influenced any change?

Training

8. What kind of training is necessary to help you perform your role (e.g., education, outside training, internal training, certifications, etc.)?
9. What training/education programs to you have for your staff regarding privacy policies?

Professionalism/Level of Expertise

10. What kind of expertise is required to support the PIA/BIA process?
11. Please describe the responsibilities/functions of various staff throughout the PIA/BIA process?

Organizational Structure

12. How is the organization structured to support the PIA/ (BIA) process?

Commitment/Culture

13. Does the PIA process help to form a culture of privacy in the organization?

Interviewees were initially contacted via email to request participation in the study and to schedule the interview. Upon agreement to participate, interviewees were provided with a list of the interview questions in advance of the scheduled interview. The introductory email soliciting interview participants is attached in Appendix A. The interview questions are outlined in Table 7.

Interview data was collected from October 2008 to November 2011. The interviews were semi-structured and scheduled for 60 minutes. Open-ended and probing questions were also used to provide more leeway in the interview and to reduce predetermined responses from the

interviewees (Crabtree & Miller, 1992; Patton, 1987). This approach also allowed me to establish a rapport with the interviewee which is noted an important facet of the process that can provide advantages to the researcher (Marshall & Rossman, 1995; Patton, 1987).

My data collection was generated by eight interviews with key senior-level civil servants in both organizations that were instrumental to the implementation of the PIA. I conducted two in-person interviews, six telephone interviews, and also obtained responses via email. The supplemental interview with Zoe Strickland on February 18, 2011 was limited to 20 minutes. The tenure of the interviewees ranged was extensive, ranging between 10 and 20 years, or career civil servants.

The interviews were recorded with the consent of the interviewee so that further transcription and analysis of the interviews could be evaluated and information could be further clarified in follow-up discussions or emails. My analysis and findings based on the interviews were summarized and distributed to the various interviewees for their review and comment over a two week time period. My field notes included my observations of both verbal and nonverbal communication. These recordings will be destroyed on December 31, 2012.

All of the datum collected from the interviews was cross-referenced across all of my field notes, particularly to identify common themes related to the PIA implementation process, training, professional expertise, and organizational structure. Many respondents from the VA freely discussed the data breaches of 2006 and 2007 in relationship to the PIA and how the breaches generated changes in organizational structure, leadership, expertise, and training. Respondents also discussed the nature of the political environment characterized by political scandal and scrutiny.

Although interviews offer a robust wealth of information, challenges exist in not only trying to make contact with high-level officials but also in securing time commitments. Some interviewees are simply not accessible. This proved to be the case in trying to reach interview candidates within the USPS and the CISO declined to be interviewed at the recommendation of legal counsel. Persistent efforts to reach additional staff at the USPS were continually met with a referral to only one point of contact.

The interviews for this study provided rich insights into the process of policy implementation that could not be derived from a quantitative model alone. Interviews also afforded contextual value to understanding the broad process of PIA implementation and the influence of training, professional expertise, and organizational structure on this process.

Coding the Data

According to Strauss & Corbin (1990), coding data is necessary to examine and compare information, identify core categories to validate relationships among the data and information, and to help integrate concepts. Creswell (2003) also supports detailed analysis that stems from a coding process that organizes materials into "chunks" and brings meaning to those "chunks." The following describes how the various data collected in this study was organized and coded.

Interview Data Coding

Analysis of my interview data involved a process of reading through the comments and color coding for text related to the PIA process, text that described organizational structure and changes to that structure over time, text that described any training relevant to the PIA and more broadly for privacy and security across the agency, and text that described the professional expertise that was associated with the evolution of the PIA in each agency. My observations of both verbal and nonverbal cues were included in my field notes.

All of the interview data was validated by comparing it with known project data and information and associating the datum with broadly available government reports such as FISMA and GAO reports, Inspectors General reports, and congressional testimony. Little to no conflicting data surfaced from the interviews. Any conflicting data was simply omitted from the study.

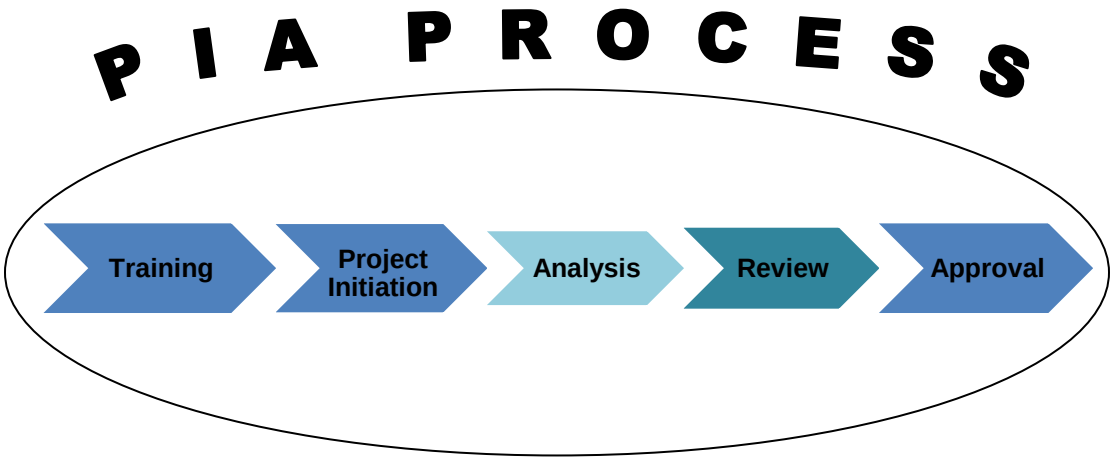
Other text that was coded included references to the VA data breaches, any references to changes or shifts in organizational culture, references to leadership or changes in leadership, references to the political environment, and identification of management challenges in implementing the PIA and privacy policy more broadly in the organization. The range of themes identified in the interview data was condensed into logical and identifiable themes that could be organized into an analysis for each case study. This method included the identification of relevant and supporting examples of the process, of how the influential factors on the PIA process became interdependent, and how these factors may have become integrated over time. This approach allowed me to identify patterns in the PIA process supported by quotations and observations.

Constant themes included the PIA as a process and any datum that contributed to an analysis of the influence of training, professional expertise, and organizational structure on this process. The data was further organized into two time periods, 2002 – 2005 and 2006 – 2010, in order to detect patterns and relationships that emerged from the constant themes.

Coding the PIA as a Process

Figure 3 outlines the stages of the PIA process that were identified in this study. These stages were supported by interview data and document analysis.

Figure 3. Stages of the Privacy Impact Assessment Process



In the analysis in Chapter 5, much of the document and interview analysis was organized first, in terms, of understanding the overall PIA implementation as a process. The central stages of the PIA process were treated in greater detail in that chapter. However, these stages of the PIA process were further used to analyze the extent of influence that training, professional expertise, and organizational structure had on the process. For instance, findings from the analysis show that training was an important factor at the beginning of the PIA process but also supported the analysis stage. Professional expertise was critical to support each stage of the PIA process and frequently emerged in the content analysis in its relationship to organizational structure. The process of the PIA and its evolution was further analyzed with the use of two time periods.

Implementation Time Periods

The use of two separate time periods was particularly useful for the VA case study, allowing me to describe the PIA process in the pre-breach years versus the post-breach years. This proved useful in understanding the considerable amount of change that occurred between 2007 and 2010, and to make inferences about the learning process that took place across the

agency throughout the PIA implementation. The USPS was straightforward to analyze since most of the efforts undertaken were in the early years of PIA implementation; however, a timeline was created to show the vast difference for how the USPS implementation was more front-loaded and robust in the nascent years and the VA actually shows a maturity in the later time period.

The next section provides a more detailed explanation of the treatment of the factors that influenced the PIA implementation process.

Factors that Influence the PIA Process: Training, Professional Expertise, and Organizational Structure

Several factors can influence the PIA process within any organization ranging from the organizational structure, organizational culture, senior level buy-in, resources, training, and education or level of expertise of the agency personnel (professionalism). Extraneous factors also impact the process, however, this study focused on the factors of training, professional expertise, and organizational structure based on a review of Edelman's body of work (2004, 2003, 2001, 1999, 1997, 1992, 1990), the literature on implementation (Pressman & Wildavsky, 1973; Bardach, 1977; Mazmanian & Sabatier, 1983; deLeon & deLeon, 2002; Schofield & Sausman, 2004; O'Toole, 2004), and my preliminary analysis of the PIA process. Clune (1983) also outlines stages of characteristics of the implementation process that include the roles of personnel and activities such as the formulation of policy and the establishment of organizational structure.

Training

First, it was important to understand how other scholars have defined or analyzed training in their research. For instance, Khademian describes a "style of standardized training" in the context of organizational commitments to mission (1996, 127). Khademian (1996) also claims

that training can be used to help understand the management style of an organization. In this study, training was used to help understand the response of the agencies to the law and the role that it played in the implementation process. Training is one means of operationalizing the policy implementation process.

Charles also describes training as a source of expertise. According to Charles, "expertise can be broken up into distinct spheres of knowledge" and the knowledge of any particular sphere comes from people who have the training, skills, and experience to permit them to access that sphere (2000, p. 3). Charles (2000) also notes that another characteristic of experts is they have a "specialized vocabulary."

In this study, several approaches to training emerged from the data. First, training that was specific to the PIA – to its mechanics of how to complete the PIA document, what data to collect, and how to report it. Other references to training were attributed to broad privacy policy training in the agencies to raise the level of awareness in the organization about the importance of protecting PII. Other training was directly related to the professional expertise that was necessary to support the PIA process such as privacy, information security, and records management training. This training was really much more specialized and was supported by professional associations and credentialing programs and therefore, is incorporated into the discussion of professional expertise in the next section.

Training was not only interrelated to professional expertise but also to organizational structure. The approach that each agency took to training became part of the organizational structure and could be seen as evidence of policy enactment based on Edelman's research.

Professional Expertise

The concept of professionalism is not new to the field of public administration (Waldo, 1968; Mosher, 1982). In this study, professional expertise is treated as an independent variable and is understood and analyzed based on prior case study research, such as Edelman (2003), Bamberger & Mulligan (2008), and Khademian (1996, 1992). Edelman (2003, 1992) shows how professionals come together to construct the meaning of the law for the organization. Khademian (1996) describes how organizational commitments can be determined by the primary professional group in a public organization in connection to a particular government mission. Khademian (1992) also addresses the role of expert knowledge in maintaining and amending policy and underscores the influence of expertise in defining options for policy making. Bamberger and Mulligan describe privacy experts as "essential to operationalizing privacy in large decentralized organizations" in their study of specific PIA implementations in the DHS and DOS (2008, p. 102).

In this study, the privacy profession emerged and evolved over time as the primary group that influenced the policy implementation process within the organization, in effect, allowing the professional and organizational priorities to become synonymous – an outcome that Khademian's research supports (1996, 1992). Like Khademian's (1992) study of the SEC, my study reflected a shift in both agencies from a reliance on legal expertise to more specialized privacy expertise for implementing privacy policy.

Edelman's (1999, 1992) research also supports the importance of understanding how professional networks influence the diffusion of new forms of government. The professional networks to support privacy policy were central to the PIA implementation process. The privacy

professional community was particularly influential on this process as evidenced by the support for IAPP membership and the strong encouragement for staff to acquire the CIPP credential.

Professional expertise is also important for understanding how multi-disciplinary management strategies unfold and change over time. For example, Khademian (1996) notes the presence of emergent tensions among disparate professions in the organization as to how the law should be implemented. These tensions became evident in the analysis of the VA and USPS and reflected in interview comments describing tensions between security, IT, privacy, and records management professionals.

The completion of a PIA drew upon this broad range of disciplines but also included operational program and business design skills. The findings showed that privacy expertise is necessary to provide advice and recommendations with respect to relevant program statutes (e.g., Privacy Act, COPPA, FOIA, etc.). But privacy experts are also in tune with current and broad privacy issues, pending legislation, national and international privacy standards, and more.

Legal expertise provides advice and recommendations with respect to privacy and program authorities, institutional oversight mechanisms and potential conflicts where multiple statutes or jurisdictions are involved, etc. Operational program and business design skills is necessary to examine proposals in terms of business flow and context, stakeholder analysis, public/private partnerships, governance structures and feasibility in terms of mitigation strategies, etc. Technology and systems expertise provides technical and systems advice on mainframe and legacy systems, Internet tools and system interfaces, information, security, technical architecture and data flows, etc. Finally, information and records keeping skills are necessary to provide advice on how records are kept and retained.

Finally, records management expertise deserves special consideration as this role has acquired more authority and recognition in organizations. This area of expertise in organizations has grown in stature because of its role in preserving privacy of all types of information in large organizations (Duff et al., 2001). Therefore, the records management function is increasingly critical to the organizational structure supporting the PIA process. But for Hoke (2011), records management also holds the key to transforming information management to information governance.

A relationship between records management and IT is important to collaborate on the impact of the evolution of new technology and applications on organizational recordkeeping. For example, the emergence of cloud computing is a ripe area for collaboration between IT and records management because the records management professionals need to understand how to manage records that are held in the cloud.[20] Another example would include the need for records management to understand how to leverage social media, such as Facebook, for critical functions such as correspondence for e-discovery (Hoke, 2011). It follows that the inclusion of information relevant to systems of record in the PIA requires knowledgeable records management personnel and the ability for IT staff to consult with this staff (Raths, 2010).

In this study, professional expertise is a key ingredient to policy implementation success. However, that success is largely dependent on how that expertise is not only incorporated into the organizational structure but how expertise influences structure. Bamberger and Mulligan state that professional expertise is a "necessary prerequisite for success" in PIA implementation; however, that success is largely dependent on whether or not that expertise becomes part of a "privacy structure" (2008, p. 103). For Khademian (1992), she assumes that the demand for

[20] Cloud computing is the delivery of computing and storage capacity as a service to a community of end-recipients. http://en.wikipedia.org/wiki/Cloud_computing.

expertise is an important independent factor that nurtures the informal and formal institutions that guide agency behavior and policy making. In this way, professional expertise becomes embedded in the internal structures of the agency that plays a key role in determining policy outcomes. But for Edelman (1992), personnel are also a strong determinant in evaluating meaningful organizational response to the law.

Organizational Structure

Organizational structure permeated the entire PIA process and was influenced by numerous factors both internal and external to the agencies. Interview, content, and process data were coded and analyzed to understand the nuances of this factor to understand how the structure changed over time, what factors influenced changes in structure – including training and expertise, and how did changes in structure impact the PIA process over time and vice versa.

In Edelman's research (Edelman 1990, 1992, & Sutton et. al., 1994), she analyzed structure in terms of the creation rates of discrimination grievance procedures and new offices in conjunction with the enactment of the Civil Rights Act of 1964. The PIA could be understood in a similar manner in analyzing the evolution of privacy officers and new structural offices to aid in enacting the PIAs. Edelman was able to show patterns for EEO offices and rules (Edelman & Petterson, 1999). Similarly, organizational structure in relationship to the PIA process reflected patterns in the agency's response to the law over time.

Edelman (2003, 1992) examines changes to organizational structure in response to law, or as a means of showing compliance and describes how compliance officers begin to look like administrative officers. She further shows how the creation of organizational structures can be either substantive or symbolic. In her research (1992), she identifies for types of compliance structure from 1984 to 1989 to assess the effectiveness of the creation of EEO offices and

affirmative action plans. Edelman's (1992) findings found a strong linkage between the creation of EEO offices and the creation of AA recruitment and training programs. In effect, studying the structures for implementing policy can help to analyze policy outcomes by a richer understanding of the managerial behavior, decision making, and other processes within these structures. For instance, decisions to enhance cross-disciplinary interaction, training, and policies and procedures are an indication of managing toward better policy outcomes.

Structures can also become a means of legitimation for organizations to promote a good-faith commitment to policy enactment but also for communicating that commitment within the organization. In this way, structure becomes a vehicle for creating organizational character, or culture, as a policy integration tool and goal (Khademian, 1996). Analyzing structure and its processes and change over time can show us how organizational commitments become manifest, how management styles translate priorities into policy, and to understand the dimensions of the nexus between the mandate from the political arena to the management of the mandate (Khademian, 1996).

Bamberger & Mulligan (2008) also discuss the interrelationship of professional expertise and organizational structure and broaden Edelman's discussion of the creation of new offices. They specifically compare the creation and role of the CPO and the associated organizational structure. Bamberger and Mulligan refer to the existence of an "embedded expert" which becomes manifest in the CPO office and solidified when established as a statutory position (2008, p. 96). The DHS appointed Nuala O'Connor as the first federally appointed CPO. Elevating an expert to this level in the organization established credibility and legitimacy for the organization that stemmed from the respect afforded to an accomplished privacy professional in the privacy community. By comparison, the DOS did not designate a privacy professional to this

status and housed privacy policy in another high-level office held by a career civil servant. This approach to structure subordinated the status of the privacy function, according to Bamberger & Mulligan (2008).

The insights gleaned from Bamberger & Mulligan's (2008) analysis of the interrelationship of expertise and organizational structure shed light onto the data obtained in the case studies of the VA and USPS. Interview data and content analysis showed the positive policy outcomes that were associated with the designation of a CPO within the USPS, whereas, this role was undefined or subordinated in the VA in the early years. As the VA gradually centralized its privacy function, it began to see more positive policy outcomes stemming from an improved process.

The case studies also show how the tensions between areas of expertise can influence organizational structure and impact decision making and policy outcomes. This tension exists between the privacy experts and those in information technology and information security – between the CPOs and CISOs and where these offices are positioned in the hierarchy. The greater the accountability and authority that resides in the CPO, the more privacy-centric the organization will be and where that authority resides in the CISO, the agency will have a more security-centric posture to policy implementation. When one level of the organization wields a greater influence on policy design and implementation, the outcomes will reflect the preferences of the personnel. Khademian (1992) provides a useful analogy in comparing bureaucratic structure and procedure to the rules of baseball, in that, the rules of the game determine which team wins, underscoring that "an agency's structure and decision making are critical for determining who gets what from government" (p., 209).

Validity and Reliability and the Role of the Researcher

Kirk & Miller (1986) describe reliability as the consistency that a measurement process produces repeated solutions. It is possible to have data that is reliable yet inaccurate or invalid; therefore, the researcher must determine the accuracy of the data. Validity, on the other hand, is obtaining the correct answer (Griffin, 1998). Triangulation is one method to ensure validity. Validity was accomplished in this study through extensive review and analysis of agency documentation, relevant government reports, and congressional testimony.

As the sole researcher in this project, I created this project, developed areas of inquiry and identified the research question. It was through my work in gathering, analyzing and identifying relevant data and information and through the interpretation of this data that I was able to draw conclusions in order to answer the primary research question. My approach was cautious to avoid subjective analysis. Using multiple sources to identify and verify the data helped to validate the study and bound any subjectivity (Yin, 1994).

However, this research approach was not without its limitations.

Limitations of Study

One limit of this study may be the research design itself. It is designed to understand only two implementations of the PIA process across a wide universe of agency implementations. Therefore, this study was limited in terms of sample size and by eliminating the feasibility for a comparative analysis. Additional case studies would bear more significant findings and future comparative analysis across multiple agencies could prove valuable.

The results from these case studies are also limited because of the lack of access to key players within the USPS, but also in the VA. In the USPS, access was limited to the privacy officer in consumer affairs who reported to the CPO. Information security and the CISO

declined to be interviewed based on legal advice. In effect, the USPS was not willing to "open the kimono," whereas the VA made itself fully available and forthcoming in all of the interviews. The USPS, though lauded as a privacy pioneer was closed to and protective of its internal practices and operations.

The next chapter provides an introduction to the case studies.

CHAPTER FOUR – INTRODUCTION TO THE CASE STUDIES OF THE DEPARTMENT OF VETERANS AFFAIRS AND THE U.S. POSTAL SERVICE

The United States Department of Veterans Affairs (VA) and the United States Postal Service (USPS) are two very important agencies when it comes to considering how privacy policy is implemented in large organizations. For each agency, the evolution of the process to support privacy impact assessments (PIAs)[21] tells a story about how organizations respond and adapt to ambiguous legal mandates. The sheer size of the constituencies served by each agency makes the management of sensitive personal information a critical task and responsibility that can be accomplished through the PIA process. How each agency responds to this task is unique and varies both historically and culturally. Each agency takes a different approach to policy design and we can better understand this variation by studying the role of training, professional expertise, and organizational structure in policy implementation efforts.

This chapter is designed to provide an empirical introduction to the mechanics of the PIA process within each agency and to explain the relevance of how factors such as training, professional expertise and organizational structure influence this process. This empirical foundation supports the case study analysis that is presented in Chapter 5 derived from interview and process data, document analysis, and theoretical findings based on Edelman's (1999) model of endogeneity.

[21] The PIA process is only one effort used to ensure that personal health information (PHI) and PII is identified early in the project life cycle and that its use is identified and protected via appropriate privacy and security controls. The PIA is not a sole effort to accomplish broader organizational privacy and security objectives (J. Buck, personal communication, November 16, 2012).

United States Department of Veterans Affairs

The treatment and care of U.S. military Veterans dates back to the American Revolution and led to the creation of the United States Department of Veterans Affairs (VA) by Executive Order in 1930.[22] The VA is comprised of three (3) major line organizations: the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). Nearly a quarter of the U.S. population is potentially eligible for VA benefits and services because they are Veterans, family members, or survivors of Veterans.[23]

The VA is a unique case study by the nature of the constituency that it serves and by its public servants who represent a different breed of bureaucrats driven by a sense of duty and moral obligation to Veterans. Many employees are Veterans themselves or perform their jobs out of a deep sense of giving back to those citizens that have served in the military. They are advocates for Veterans and their families as expressed in the VA's mission:

> *To fulfill President Lincoln's promise "To care for him who shall have borne the battle, and for his widow, and his orphan" by serving and honoring the men and women who are America's Veterans*. Retrieved from http://www.va.gov/about_va/mission.asp.

Although the three VA Administrations have very different missions - health, benefits, and memorial affairs, the agency must be able to distinguish among Veterans in order to meet each Veteran's unique needs. In the case of healthcare, mistaken identity could be catastrophic. Therefore, information management and the security and privacy of personal Veteran and employee information is a secondary mission of the agency.

This secondary mission became elevated in May of 2006 when the agency experienced the second largest data breach in American history. It was the biggest breach of Social Security

---

[22] U.S. Department of Veterans Affairs. *VA history in brief.* Retrieved from http://www.va.gov/opa/publications/archives/docs/history_in_brief.pdf.

[23] U.S. Department of Veterans Affairs. (2008). *Eliminating the unnecessary collection and use of Social Security Numbers at the Department of Veterans Affairs*.

numbers ever, putting approximately 26.5 million Veterans at risk of identity theft.[24] Another breach followed in 2007 at the Birmingham, Alabama facility.[25] These data breaches are not the focal point of this study; however, they are relevant as extraneous events that help to frame a deeper analysis of the agency's approach to the PIA process between 2002 and 2010.

The next section outlines the genesis of the PIA, first within the VA and then within the USPS. Each case study is organized to discuss the emergence of the PIA, the participants to the PIA, and to introduce the role of training, professional expertise, and organizational structure in shaping this process. These empirical profiles of the PIA process establish a means for deeper analysis of emergent patterns in the policy process in the next chapter. The case studies are organized and informed by Edelman's research model that analyzes the implementation of EEO/AA policy in organizations, particularly in new offices and rules (policy) that emerge within organizations to respond to uncertainties in the law.

U.S. Department of Veterans Affairs – Emergence of the Privacy Impact Assessment

Prior to the E-Gov Act, the focus of privacy policy within the VA was largely oriented towards the Freedom of Information Act (FOIA), the Health Insurance Portability and Accountability Act (HIPAA) and records management. Privacy officers, prior to 2002, were decentralized and hired strictly to ensure compliance with the Privacy Act, particularly in terms of systems of records notices, computer matching agreements, ensuring PII was protected, and answering privacy related question and concerns. In 1999, privacy officers expanded their focus to the proposed rulemaking for the HIPAA. Hence, the role of the privacy officer was limited in scope before 2002 and no Department-wide privacy office existed though there was a full-time

[24] Pike, G.H. (2008). VA data breach and the Privacy Act. *Information Today*. Retrieved on November 11, 2010 from www.informationtoday.com.
[25] Mosquera, M. (2007, February 6). VA missing hard drive. *Government Computer News*. Retrieved on February 7, 2007 from http://www.gcn.com.

privacy officer, until the creation of the VHA Privacy Office in 2002 (S. Griffin, personal communication, November 19, 2010). Prior to 2002, the respective VA Administrations had privacy professionals assigned by the Director of the facility.

The creation of the VA's Privacy Service represented a shift in the agency's overall focus on privacy policy – one that encompassed a broader mission beyond compliance to one that aimed to protect and preserve the privacy of Veterans and employee personal information. Three other offices worked in concert with the Privacy Service: 1) the Office of the Assistant Secretary for Information and Technology (ASIT), 2) the Office of Information Protection and Risk Management (IPRM), 3) the Office of Privacy and Records Management (OPRM). These offices were created in support of the VA's IT Realigment Plan under Secretary Nicholson and CIO, Bob Howard, a political appointee under the Bush Administration.

This seemingly straightforward response to enabling policy implementation was met with unforeseen complexities as the Privacy Service soon found itself in the role of developing a broad range of programs, products, and VA-wide policies, centrally, although implementing nationally. The creation of the office of the Privacy Service made it possible for the VA to coordinate and centralize the professional expertise necessary to enact the PIA requirement under the E-Gov Act. As noted earlier in Chapter 1, the creation of the Privacy Service was also part of a larger effort by the VA to centralize its operations based on congressional scrutiny and the need to realign its IT infrastructure.

The nature of this expanded scope and broadened privacy policy expectations is expressed by a privacy officer within the VHA who explained how her role changed between 1999 and 2002 from a primary focus on understanding the impact of the proposed HIPAA rulemaking to a focus that became more "global" in nature, reaching beyond a compliance

function with existing privacy laws. Privacy policy became a much more complex and broadened focus across the entire organization. The Privacy Service enabled privacy officers throughout the VA to expand training, resources, and the recruitment of specialists so that their role became more managerial (Personal communication, November 19, 2010).

The background leading to the creation of the VA Privacy Service is important because it marked a pivotal point in the evolution of the organization's response to privacy law and supports Edelman's (1992) claim that personnel are a strong determinant in evaluating meaningful organizational response to the law.

However, Edelman's (1999) model also outlined the creation rates of new offices, rules and/or policies as relevant to understanding organizational response to the law. The creation of the Privacy Service marked one point in the trajectory of a stream of new offices coupled with numerous new policies and directives. Many of these policy directives were issued between 2003 and 2010 as shown in Table 8:

Table 8. VA Privacy Policy Directives between 2003 and 2010

Directive	6502	Privacy Program	06/20/2003
Handbook	6502.1	Privacy Violation Tracking System	3/25/2004
Handbook	6502.2	Privacy Impact Assessment	10/21/2004
Directive	6361	Ensuring Quality of Information Disseminated By VA	09/02/2004
Directive	6500	Information Security Program	08/04/2006
Directive	6504	VA Directive 6504 Rescinded by VA Handbook 6500	09/18/2007
Directive	6502	VA Enterprise Privacy Program	05/05/2008
Directive	6507	Reducing the Use of Social Security Numbers	11/20/2008
Directive	6508	Privacy Impact Assessments (Revises Handbook 6502.2)	10/03/2008
Directive	6509	Duties of Privacy Officers	08/13/2009
Directive	6371	Destruction of Temporary Paper Records	10/29/2010

Source: Department of Veterans Affairs Office of Inspector General. (2006). *Review of issues related to the loss of VA information involving the identity of millions of Americans*. (Report No. 06-02238-163). Retrieved from http://www.va.gov/.

For instance, the VA Directive 6502 - Privacy Program, was issued one year after the creation of the Privacy Service. The Directive did not specify how information should be protected. Furthermore, the 2006 Report by the Office of Inspector General could not identify any policies that were in place prior to May 2006 that established specific requirements for safeguarding protected information.[26] In effect, it appears that the VA's approach to implementing the PIA process began with structural change, or the creation of new offices versus starting with broad organizational policies. A Handbook to support the PIA process was not released until late 2004 and was not revised for another four (4) years in 2008 (U.S. VA Directive 6508 - Privacy Impact Assessments).

The Directive 6508- Privacy Impact Assessments finally did establish a department-wide policy for PIAs in accordance with the E-Gov Act. The Directive expanded upon initial requirements to include not only IT systems, but also *programs* and *projects* that collect PII. It also established criteria for completing mandatory rulemaking PIAs and expanded upon PIA policies that were set forth in the VA Directive 6502 - Enterprise Privacy Program created on May 5, 2008 (a revision of Directive 6502 from 2003).

The policy for PIAs outlined in the VA's Directive 6508 - Privacy Impact Assessments specifies that anyone responsible for a rulemaking, program, system or practice that collects or uses PII must conduct a full PIA. Systems without PII only need to complete Part I of the PIA form to confirm that PII is not collected by that system or that changes have not occurred that require a new PIA. The policy required that a PIA be conducted when a system:

1) Develops or procures any new data capable technologies or IT systems that handle or collect PII;

[26] Department of Veterans Affairs Office of Inspector General. (2006). *Review of issues related to the loss of VA information involving the identity of millions of Americans*. (Report No. 06-02238-163). Retrieved from http://www.va.gov/.

2) Initiates a new collection of PII on 10 or more persons;
3) Revises existing systems – for example, if a program either initiates a new information sharing with another agency or incorporates commercial data from an outside data aggregator; and
4) Issues a new or updated rulemaking that affects PII. The PIA should discuss how management of these new collections or new uses will conform to privacy law, regulations and VA policy.

The VA Directive 6508 further identified staff responsibilities for all of the supporting participants and offices involved throughout the PIA process from the top to the bottom – from the Chief Information Office (ASIT) down to the program managers, project managers, system managers, system developers, and data owners.

The Privacy Service became the centralized authority for reviewing and approving all PIA forms before being submitted to the OMB for review with OMB Circular A-11, Exhibit 300, Capital Asset Plan and Business Case[27] for the applicable fiscal year. The review process was designed to examine whether privacy risks were identified and addressed in all PIAs and to assess PIA content for conformance with privacy and related regulatory requirements. In effect, the review process became a method for managing the security and privacy of all PII held by the VA. The next section introduces the participants to the PIA process and briefly discusses the various offices and expertise that support this process.

Participants in the PIA

The PIA process includes personnel spanning information technology, information security officers, privacy officers, system owners and developers, chief information officer, risk management, records management, project and program managers, inspectors general, and data owners. These various positions and functions are described in Table 9, beginning with the top

[27] U.S. Office of Management and Budget, Executive Office of the President. 2002. *OMB Circular No. A–11, Section 300. Part 7: Planning, Budgeting, Acquisition, and Management of Capital Assets.* Retrieved from http://www.whitehouse.gov/omb/e-gov/docs.

authoritative office held by the ASIT, or the CIO, down to the data owners and project and program managers.

Table 9 – VA PIA Position Responsibilities Per VA Directive 6508

ASIT or Chief Information Officer	(1) Ensure that a mechanism is in place for the review and approval of all PIAs and Exhibit 300s per OMB; (2) Ensure the monitoring of all VA-wide systems for compliance with the security and privacy statements found in the PIAs of said systems; (3) Submit approved PIAs to OMB; and (4) Designate the Associate Deputy Assistant Secretary (ADAS) for Privacy and Records Management, as the principal Department official responsible for ensuring the reporting of all PIAs received.
The DAS, Office of Information Protection and Risk Management (OIPRM)	(1) Perform all PIA duties and responsibilities as designated by the ASIT; (2) Ensure that PIAs are performed as a part of the certification and accreditation and OMB Exhibit 300 processes; and (3) Ensure that completed PIAs are submitted to the ASIT.
The ADAS, Office of Privacy and Records Management (OPRM), Senior Agency Official for Privacy	(1) Perform all PIA duties and responsibilities as designated by the DAS, OIPRM; (2) Ensure that a PIA template and instructions on how to complete a PIA are made available to System Owners; (3) Ensure that guidance and assistance is provided that meets OMB and VA requirements; (4) Ensure that completed PIAs are submitted to the Department CIO; and (5) Ensure that PIAs are published on the appropriate VA web site.
Director, Privacy Service	The Director shall establish department-wide PIA requirements and processes by: (1) Performing all PIA duties and responsibilities as designated by the ADAS, OPRM; (2) Developing a PIA template and instructions on how to complete a PIA; (3) Providing guidance and assistance on meeting OMB and VA requirements; (4) Reviewing and analyzing each PIA received, so that a recommendation for approval can be made to the CIO; (5) Submitting completed PIAs to the Department CIO, as appropriate; and (6) Publishing approved PIAs on the appropriate VA web site.
Director, Records Management Service	1) Perform all PIA-related duties and responsibilities as designated by the ADAS, OPRM; (2) Review Information Collection Requests (ICR) to determine whether the information requested is properly addressed and identified as part of the OMB 83-I Paperwork Reduction Act (PRA) submission, Supporting Statement and collecting instrument in accordance with the PRA of 1995; (3) Review PIAs associated with ICRs; (4) Submit ICRs to OMB on behalf of the Department CIO; (5) Publish Information Collections Notices in the *Federal Register* in accordance with the mandates of the PRA of 1995; and (6) Review Systems of Records Notices (SORN) of systems on which PIAs are conducted.
Inspector General	(1) Provide assistance and guidance to the VA Privacy Service on the oversight and design of PIAs; and (2) Provide recommendations related to VA PIA compliance.
Under Secretaries, Assistant Secretaries, and Other Key Officials	(1) Ensure that Program and Project Managers submit timely and accurate PIAs; (2) Ensure that PIAs are submitted in parallel with the Exhibit 300; (3) Work with the VA Privacy Service to finalize each PIA; and (4) Monitor compliance with security and privacy statements in each PIA for all programs, projects, and systems under their authority.
Program Managers	(1) Work with Project Managers and System Managers to determine whether PIAs are necessary for projects and systems within their programs, and provide this information to their System Managers, Privacy Officers, and Information Security Officers (ISO); (2) Ensure that PIAs are completed in a timely and accurate manner in accordance with the guidance established by the VA Privacy Service; (3) Ensure that PIAs for projects for which they are responsible are verified annually, and updated if major changes take place; and (4) Ensure that each project for which they are responsible is compliant with the security and privacy requirements described in each PIA.
Project Managers	(1) Work with Program Managers, ISOs, Privacy Officers, and System Managers to determine whether a PIA is necessary for their projects and systems; (2) Ensure that PIAs are completed in a timely and accurate manner in accordance with the guidance established by the VA Privacy Service; (3) Coordinate with their Privacy Officers, ISOs, and System Managers, and with the VA Privacy Service to ensure that all PIAs under the responsibility of these officials are

	finalized; (4) Verify PIAs annually, and update if major changes take place; and (5) Ensure that each project or system is compliant with the security and privacy requirements described in each PIA.
System Managers	(1) Work with the Program Managers, Project Managers, ISOs, Privacy Officers, and System Developers to address the system's privacy issues that are revealed through the completion of PIAs; (2) Work with Project Manager in the preparation of PIAs; (3) Obtain the Program and Project Manager's approval of PIA submissions; (4) Submit PIAs to the VA Privacy Service for review and approval; and (5) Serve as points of contact for the system.
System Developers	(1) Ensure that the system design and specifications conform to privacy standards and requirements; and (2) Ensure that technical controls are in place for safeguarding PII from unauthorized access.
Data Owners	(1) Work with the Program Managers, Project Managers, System Managers, ISOs, Privacy Officers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions; (2) Serve as points of contact for questions related to system data; and (3) Respond to questions from Program Managers, Project Managers, System Managers, System Developers, ISOs or Privacy Officers that are related to the submission of PIAs.
Information Security Officers (ISO)	ISOs shall work with their Privacy Officers and System Managers to ensure that security risks are identified and documented in all PIA submissions. In addition, ISOs shall coordinate with their Privacy Officers, their System Managers, and the VA Privacy Service to ensure that the PIA(s) for each system for which she or he is directly responsible is finalized.
Privacy Officers	Privacy Officers shall coordinate with their local ISOs and System Managers to ensure that all data and associated risks are identified and documented in all PIA submissions. In addition, Privacy Officers shall work with their ISOs, System Managers, and the VA Privacy Service to ensure that the PIA(s) for each system in his or her immediate area of operation is of a quality that will reasonably ensure its approval by the VA Privacy Service.

Source: U.S. Department of Veterans Affairs. (2008). *VA Directive 6508*.

Responsibilities for these participants were first outlined in VA Directive 6502 - Privacy Program, issued in 2003. However, this directive morphed into the VA Handbook 6502.2 - Privacy Impact Assessment, released in October 2004, which was later revised in 2008. The Handbook specifically required project managers to complete PIAs promptly and accurately for the ASIT's review and approval.

In order for the project managers to be able to complete PIAs they would require training; however, it is difficult to understand how the training process was implemented because policies, procedures, and memorandums that were issued were not consistent in outlining a specific training program. In fact, there was no consolidated set of policies and procedures issued over several years that employees and contractors could access to ensure all applicable requirements

were being met. The Office of Inspector General (OIG) reached a similar conclusion in its 2006 report that reviewed employee and contractor training on policies and procedures.[28]

Training for the PIA

A review of all security and privacy training modules conducted by the OIG in 2006 found that these modules were difficult to locate and did not provide adequate training. The Report reviewed three (3) online training modules on privacy that were general in nature and not specific to the PIA process (2006). Interviews with VA staff reflected the conclusions drawn by the OIG suggesting that the agency's approach to training for the PIA essentially evolved from "no training" to "what we have now." Today, training is largely centralized in the Privacy Service and performed by two key individuals. Dennis Stewart currently serves as the Assurance Team Lead with oversight for PIAs. In interviews, he was referred to as the "driving force" for reforming the PIA process (J. Buck, Acting ADAS, Office of Privacy and Records Management, personal communication, December 10, 2010).

Training was also described as being "very unique to the agency" and facilitated through the use of online tutorials and user guides. One staff member described training for the PIA as "highly specialized and focused on team-building and supervisory-type things." For example, IT professionals needed to be trained to do non-IT related tasks (J. Buck, Acting ADAS, Office of Privacy and Records Management, personal communication, December 10, 2010).

In an interview with Stephania Griffin, VHA Privacy Officer and Director of Information Access and Privacy Office, she found it hard to describe the role of training to the PIA "because I've been doing it since 1999." She did, however, describe how new specialists were required to go through one week of in-person privacy officer training that was offered once per year. She

[28] U.S. Department of Veterans Affairs Office of Inspector General. (2006, July 11). *Review of issues related to the loss of VA information involving the identity of millions of veterans.*

also referenced a "privacy boot camp" that she conducted in 2007 that was designed for the IT and oversight compliance (ITOC) staff; however, this training was a one-time event and never repeated. She concluded her remarks by stating that [we] "tend to hire privacy specialists who have already been privacy officers in the field so they are familiar with privacy within the VHA" (Personal communication, November 19, 2010).

Training for privacy and security also became mandatory particularly for new privacy officers and information officers in order to familiarize them with the PIA process. The Privacy Service made training for this purpose available twice per year. It also designated one week out of the year as "information protection week" and sponsored an annual "Privacy Day." The Privacy Officer in the Office of Information & Technology (OI&T) also discussed how she supports over 6000 employees and conducts walk-throughs at the VACO campus. Many of the 6000 staff is located throughout the country (Personal communication, November 19, 2010).

A consolidated or comprehensive training program did not seem to appear until the Directive 6508 - Privacy Impact Assessments was issued in October 2008 and commensurate with the hiring of specialized staff (i.e. Dennis Stewart and Christina Pettit). The Directive did outline training for the PIA that was offered to participants of the VA Triumvirate, which is described in the section on organizational structure.

Training was and is a significant component of professional expertise and expertise was necessary to provide training, creating a recursive relationship between these two variables. The next section describes professional expertise for the PIA in the VA.

Professional Expertise and the PIA

The range of professional expertise to support the PIA process in the VA stretches across IT, information security, risk management, records management, privacy professionals, legal

professionals, risk management, auditors, and FOIA experts. It is interesting to note how these areas of expertise unfolded within the VA because interviews referred to expertise as "home grown." For instance, Sally Wallace, former ADAS, Office of Privacy and Records Management, described how she started out in 1990 as an IT program manager for educational benefits and the GI Bill. In 2001 she became the deputy to the Head of Cybersecurity, later became the Chief Architect for VA operations and then moved into privacy and records management (Personal communication, October 10, 2008).

John Buck eventually replaced Sally Wallace as the Acting ADAS upon her retirement. An interim Acting Director unfortunately passed away in between Wallace's retirement and Buck's placement into the position and the title was changed to Director, Office of Privacy and Records Management.

Buck started out at the VBA as the Chief of Administration and Deputy Director of Facilities. In this role, he oversaw records, privacy, FOIA, and building security. In effect, he "wore many hats." He described how the need to conduct a PIA is dependent on relying on the "integrity" of other staff to know when a system changes or a new major or minor application "pops up" so that the need for a PIA is "flagged" by the Privacy Service (Personal communication, October 10, 2008).

Interviews also emphasized that no one individual can complete a PIA, that it requires a team. For example, it is important to have someone on the team that is knowledgeable about Privacy Act Systems of Records Notices (SORNS). It also requires technical expertise from areas such as IT and information security – many of these individuals require training to better understand the privacy needs of information protection and security as they build, manage and oversee the systems that hold PII. The interplay between professional expertise and

organizational structure in this evolution is symbiotic and training emerged as a critical function to support this relationship. The interplay among these factors is illustrated in Figure 4 and is further explored in Chapter 5 – Case Study Analysis.

Figure 4. Interplay among Influential Factors on the PIA Process

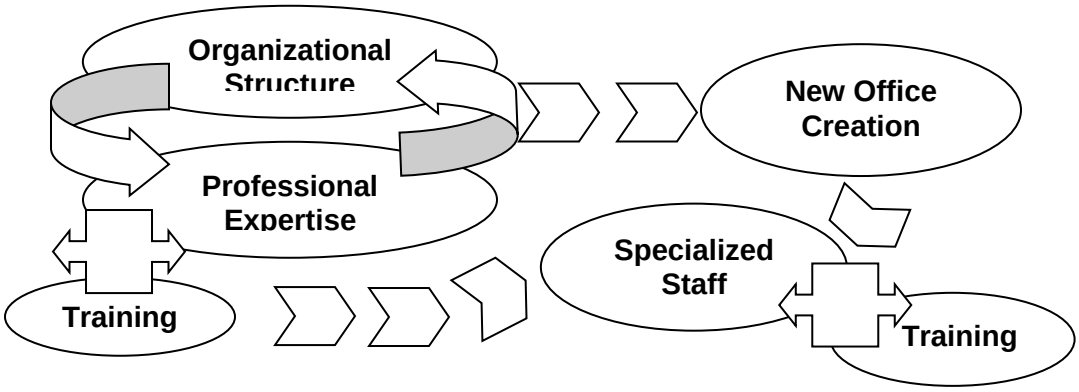


Figure 4 depicts new office creation and specialized staff as components of both professional expertise and organizational structure. The creation of new offices to support policy implementation become an important dynamic of the overall organizational structure and the specialized staff that support these new offices shape the span of the expertise needed for policy implementation. Training is a factor that shapes expertise but is also provided by experts established within the organization.

Organizational Structure and the PIA

A hallmark of the how the VA structured itself to support the PIA process was in the creation of the VA Triumvirate, a structural unit. The Triumvirate brought together a team of professionals–a CIO, Privacy Officer (PO), and Information Security Officer (ISO). Together, these professionals provided the centralized authority and expertise to effectuate the PIA process from initiation to approval. Responsibility for final approval of PIAs was delegated to the Team Lead for Assurance, who reports to the Director of the Privacy Service (Personal

communication, November 19, 2010). Figure 5 illustrates the structure and professional expertise of the VA Triumvirate.

Figure 5. VA Triumvirate

The participants in the Triumvirate are responsible for different aspects of the PIA process represented in the role of the chief information officer, information security officer, and privacy officer.

The Chief Information Officer

The Chief Information Officer, also referred to as the Assistant Secretary for Information and Technology (ASIT), is the single leadership authority for information technology and is the principal advisor to the Secretary on all matters relating to the management of VA's information and technology. Interviews with staff described the CIO as "being up there" and "delegating down." The CIO is primarily concerned with facts and data related to VA data elements and the number of systems that should be reported as this is where his accountability rests.[29] The CIO is

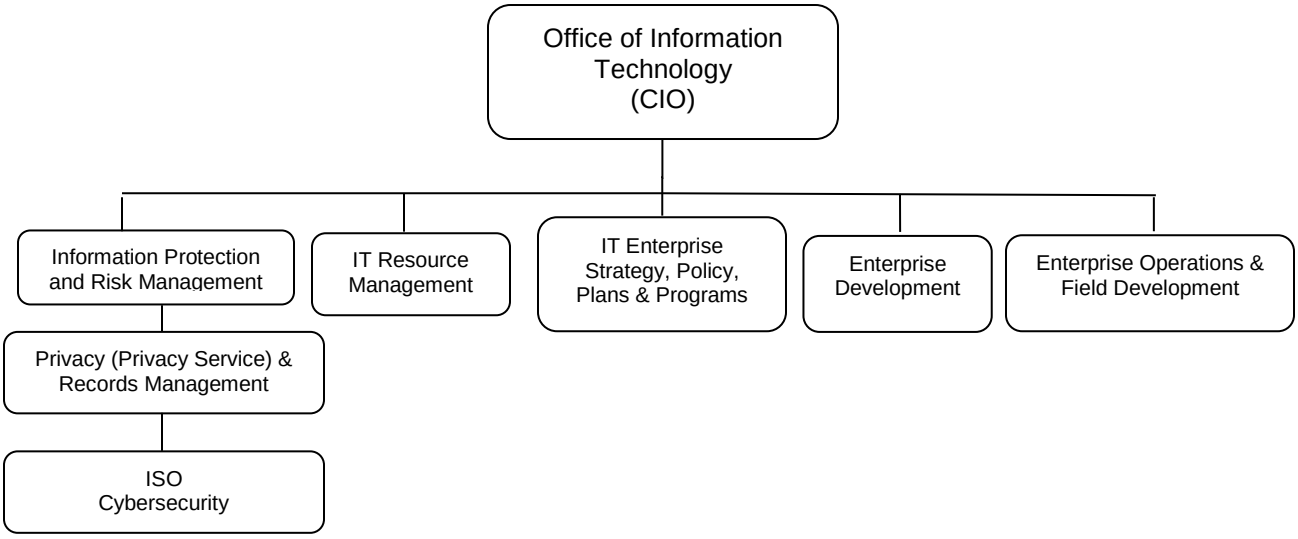
[29] Recall in Chapter 2 that the agencies are required to submit annual reports on their information security under Title III, the Federal Information Management Security Act, of the E-Government Act of 2002.

also the "first person that the media will go to in the event of a problem" (Personal communication, November 19, 2010).

The CIO has oversight of five (5) other offices: the Office of Information Protection and Risk Management (IPRM); IT Enterprise Strategy, Policy, Plans & Programs; IT Resource Management; Enterprise Development; and Enterprise Operations & Field Development. Cybersecurity and Privacy and Records Management fall under the IPRM. The IPRM enacts policies, processes, and procedures that help protect the information and systems across the VA.[30]

Figure 6 provides an overview of the organizational chart for the Office of Information and Technology.

Figure 6. Organizational Chart for the Office of Information Technology



The office also coordinates the Department's implementation of IT requirements for the E-Gov Act and is the primary contact for issues related to OMB E-Government, including compliance with privacy and security laws.

[30] U.S. Department of Veterans Affairs. (2010). *VA Organizational Briefing Book*. Retrieved from http://www.va.gov/ofcadmin/docs/vaorgbb.pdf.

The Office of Information Protection and Risk Management (IPRM) deals with matters related to information protection including privacy, cybersecurity, risk management, records management, FOIA, incident response, critical infrastructure protection and business continuity. The office develops, implements and oversees the policies, procedures, training, communication and operations related to improving how the VA and its' partners safeguard the PII of Veterans and VA employees. Its objective is to assure the confidentiality, integrity and availability of information and information systems.[31]

The Information Security Officer

The role of the Information Security Officer (ISO) in the Triumvirate is to work with the privacy officers and systems managers to ensure that security risks are identified and documented in all PIA submissions. The ISO plays a critical function in supporting the organization's overall security infrastructure and ensuring effective security controls, assessments, training and awareness, and prevention of data breaches. The ISO has the necessary knowledge and understanding of technical systems and technical assets. In addition, ISOs coordinate with their privacy officers, system managers, and the VA Privacy Service to ensure that the PIA for each system for which she or he is directly responsible is finalized.

The Privacy Officer

The Privacy Officer is often characterized as the driving force behind the PIA process; however; the PIA is only one facet of a Privacy Officer's job. Privacy officers are an integral part of the VA's privacy organization and some duties of a general privacy officer may include compliance with Federal privacy laws and regulations and VA Directives; responding to and

[31] U.S. Department of Veterans Affairs. Retrieved from http://www.ois.oit.va.gov/.

reporting privacy complaints and violations such as data breaches; employee and contractor training and education; and cooperation across several agency departments.

A partnership between the ISO, the CIO and the Privacy Officer, is critical to overall information governance and privacy policy implementation and this partnership is reinforced through the Triumvirate. However, this partnership is supported by key areas of expertise such as records management and other areas of expertise.

Records Management

Since records management professionals are responsible for systems of records notices (SORNS) as required under the Privacy Act, they play a key role in the PIA process. Any changes to the data that is being collected by a system require the publication of a SORN or updating an existing SORN to reflect changes in the collection and use of PII as reported in PIAs. Hence, records management is a critical function to any organization to ensuring the proper handling of sensitive information and to the overall maintenance of a system of records. It is highly related to risk management for information systems and often associated with knowledge or content management in organizations.[32]

The increasing role of records management is supported by the expansive growth and volume in electronic records. Its importance to the VA's approach to privacy policy implementation was expressed in staff interviews and reviews of records management journals.

[32] The USVA Records Management programs is under the purview of the Office of Information Enterprise Records & Technology Service. For more information on the USVA's records management program see http://www.rms.oit.va.gov/.

Other Expertise

Peripheral expertise that supports and collaborates with the Triumvirate include the system owner that has responsibility for the system or program under review and information technology experts. Systems owners and related staff may include engineers that design software to incorporate privacy controls for PII.

Summary

In the case of the VA, the emergence of the PIA as a vehicle for broad privacy policy implementation was fragmented and reactive, indicative of an organization paralyzed by legal ambiguity and changing leadership. The VA did increase the creation of new offices to allow for better resource allocation; however, critical events challenged the organization's ability to adapt its structure and policies to build a fluid process. The analysis in Chapter 5 presents a detailed understanding of how expertise and organizational structure shaped the evolution of the PIA.

The next section provides an introduction to the PIA process and approach in the USPS.

United States Postal Service

The United States Postal Service (USPS) also has a rich history based upon its creation on July 26, 1776 in Philadelphia by decree of the Second Continental Congress. It became the Post Office Department in 1792 and was part of the Presidential cabinet. In 1971, the department was reorganized as a quasi-independent agency of the federal government and acquired its present name. The Postal Reorganization Act signed by President Richard Nixon on August 12, 1970, replaced the cabinet-level Post Office Department with the independent USPS. It is often mistaken for a government-owned corporation but is legally defined as an "independent establishment of the executive branch of the Government of the United States," (39 U.S.C. § 201) as it is wholly owned by the government and controlled by the Presidential appointees and the Postmaster General.

Notably, it is the third-largest employer in the U.S. following the Department of Defense and Wal-Mart. The constituency of the USPS is global in reach and serves both the public and private sectors. It is the backbone of a communication network in this country and represents the seeds of basic privacy rights in America in requiring citizens to trust the organization with the stewardship of private citizen information.

This underlying, value-driven mission of the USPS, "*to provide trusted, affordable, universal service*," coupled with its historical context, makes it a harbinger for any study of the enactment of privacy policy in the U.S. The sheer potential for privacy infractions, from the opening of mail (i.e. private communication), to the compilation of vast profiles on citizens, associations, interest groups, affiliations and more, renders this organization as a stand-alone model for assessing the relevance of privacy as a policy and public management matter of interest.

The USPS was also the first Federal agency to elevate the significance of privacy policy by designating a CPO in 2001 to ensure that all projects and departments within the vast 700,000-employee organization meet the requirements of the Privacy Act, the E-Gov Act, and the privacy provisions in Postal Service statutes. This defining event has important implications for the analysis in Chapter 5.

The next section provides a brief historical background to establish a context for the emergence of the PIA process, which is referred to as the business impact assessment (BIA) by the USPS. The following section will also review the key participants in the process and describe the factors of training, expertise, and organizational structure in relationship to the BIA process.

United States Postal Service – Emergence of the Business Impact Assessment

Historically, the USPS has been a pioneer in information privacy. Privacy has been a driving principle since its inception by prohibiting the opening of letters. This principle became manifest in the form of an oath that Ben Franklin made workers take:

> I A. B. do swear, That I will not wittingly, willingly, or knowingly open . . . or cause, procure, permit, or suffer to be opened . . . any Letter or Letters . . . which shall come into my Hands, Power, or Custody, by Reason of my Employment in or relating to the Post Office… (Desai, 2007, p. 563).

This oath was reinforced by laws passed to protect the privacy of the mail and ban it from being opened by unauthorized recipients.

Fast forward to the 21st Century and privacy is still at the center of the USPS mission. Its creation of an office for a CPO in 2001 was a harbinger for broad policy changes in the privacy and information protection landscape. At the time of this announcement, the USPS lauded itself as a world leader in ensuring the secure and private delivery of physical correspondence. It also

reflected a proactive response to emerging privacy problems and attention on Capitol Hill (Personal communication, November 19, 2010).

Zoe Strickland was designated as the first federal agency CPO and was given broad authority for oversight, coordination, development, and implementation of corporate policies, management practices, technologies, and other procedures to foster public trust by protecting personal privacy in its products and services.

Under Strickland's leadership the agency took another preemptive move in administering broad privacy policy by implementing the PIA prior to it being required under the E-Gov Act and regardless of the agency's exempt status. USPS labeled this process as a business impact assessment (BIA) versus a privacy impact assessment.

Underpinnings of the BIA: Leadership, Policy, and Structure

In her role as the CPO, Strickland drove the creation of several organization-wide practices and policies that aligned with the USPS Transformation Plan of 2002 (the "Plan") under Postmaster General Jack Potter. In the Plan, Potter outlined his support for the development of a strong policy program and put Strickland at the helm within the Office for Consumer Affairs and Consumer Advocate. These actions made Potter a recognized leader for driving a strong privacy program that resulted in the USPS being named the most trusted government agency for six consecutive years between 2004 and 2010 in The Ponemon Institute's Government Privacy Trust studies (Fillichio, 2006).

At the time, Strickland reported to Francia Smith, the Vice President of Consumer Affairs, though the predominant trend across government agencies was for privacy officers to report to the CIO or to the legal department. According to an interview, the CPO was housed in

consumer affairs because "it's about the consumer and should come out of consumer affairs" (D. Kendall, personal communication, November 19, 2010).

In its infancy, the CPO coordinated with the corporate information security program to build the privacy office using a two-pronged approach. The first step involved a review of all the privacy statutes that the USPS was subject to: the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach Bliley Act (GLBA), the Privacy Act, and other relevant statutes, including the E-Gov Act. The office would also be attentive to the FTC's Fair Information Practices as previously described in Chapter 2.

This initial coordination effort resulted in the emergence of the BIA through the integration of privacy with corporate security with the objective to support budgeting for the development of new IT systems and to ensure the security of the new system and the presence of proper controls. This structural integration supported a BIA process that was designed to address all aspects of privacy from the tactical (e.g., examination of Privacy Act Systems of Records) to the strategic (e.g., consistent direction for policies and approaches). According to Strickland, this integration was necessary to support a BIA process that would "help drive privacy solutions and considerations in programs and applications" and "foster and facilitate the culture of privacy as part of a proud tradition" (Personal communication, January 21, 2011).

The decision to "marry" privacy and security from the beginning allegedly allowed the USPS to break through the "stove-pipe mentality" of other federal agencies. Strickland decided that it was important to bring IT into the BIA process and outlined the privacy laws that the agency needed to "worry" about. The result was the creation of new sections in the BIA document that addressed all of the relevant privacy laws and jumpstarted the process of

collaboration between these offices, a process characterized as being "joined at the hip" (D. Kendall, personal communication, November 19, 2010).

The IT department assumed responsibility for coordinating meetings to discuss any new IT systems that might require a BIA. The system owner for any new project would need to identify the data that the new system would collect and the intended use of that data. In doing so, the system owner had to collaborate with the CISO and the privacy office.

An example of a particular BIA process to develop a new employee skills bank is helpful to understand the need for collaboration in the process. The first step in this process begins with a request for proposals to develop the new system. Once the contract is in place, the CPO meets with the software provider to gather information about the data being collected by the system and how that data would be used. At this point, the CPO would express their privacy concerns related to the system owner such as data on employee talent, how much data needs to be collected, and how the system would integrate with the USPS's unique identification program for its employees. Integration with this program is noteworthy because it was designed to solve a government-wide problem of collecting and using Social Security Numbers (SSNs) for identification.

Eliminating the use of SSNs was a hallmark of Strickland's broad-based strategy to implementing privacy policy and was launched in 2003. This strategy was borne out of the Unique Identification Program (UIP) housed within the human capital office. This move by Strickland precipitated the same directive that came out of the President's Identity Theft Task Force. Strickland made this effort one of her top priorities as CPO and the agency moved forward with a program and policy to assign unique numbers to employees and to mask any existing SSNs. The result was the implementation of a modern HR system that digitized official

personnel folders (OPFs) which reside with the National Archives and Records Administration (NARA) upon an employee's retirement (D. Kendall, personal communication, November 19, 2010).

Internal policies for privacy and information security were also among Strickland's priorities resulting in the issuance of Handbook AS-353 *Guide to Privacy, the Freedom of Information Act, and Records Management* (the "Handbook") in 2005 and updated in 2009. The Handbook became an internal guide to privacy, the FOIA, and records management and served as a primary source for overall direction and guidance to the organization. It also called out the need for a partnership between the privacy office and information security as well as the need for security of information addressed in separate guidance, *Handbook AS-805: Information Security*. The Handbook was a strategic move in the sense that it supported the goals outlined in the Transformation Plan and set out to ensure the proper collection, use, and protection of customer and employee information. Both handbooks helped to operationalize the BIA for the participants involved in the process.

Participants to the BIA

The key participants to a BIA include information technology (IT), privacy, security and the customer (e.g., supply management, HR, or finance). The roles in the process are described as the Executive Sponsor (developer, system owner, or user) who is responsible for completing the BIA and submitting it to the CPO and CISO for review and approval. The Executive Sponsor is required to sign an acceptance of responsibility document to hold them accountable for accurate information in the BIA. The CPO assists in the completion of the BIA and ensures compliance with the privacy sections and as such, is held accountable for these sections of the BIA. The CISO assists in the completion of the security sections of the BIA as well as

compliance with the USPS's security plan and is accountable for approving the security sections and documenting negotiations (Personal communication, November 19, 2010).

Collaboration from the beginning to the end of the BIA process requires instrumental relationships between diverse areas of expertise and across the organization's structure. Hence, collaboration became a key element that shaped the USPS's ability to integrate training, expertise and organizational structure to support the BIA process. Each of these participants in the BIA process is subject to a range of training and or becomes a credible participant in the process by nature of their area of professional expertise. Let's first turn our attention to the specialized training directly related to the BIA.

Training for the BIA

The USPS offers specialized training to portfolio managers, IT, and new security staff. Face-to-face training is conducted within the headquarter offices, however; training is also made available leveraging the use of various media. This training is initially basic in its nature, but followed by several training modules. All training modules are developed and taught by the manager for strategy and processes in the privacy office, who directly reports to the CPO. In this study, this role belonged to Deborah Kendall, Manager, Strategy and Processes, USPS Privacy Office.

Initial BIA training begins with a comprehensive review the BIA process, objectives, and scope. The scope brings attention to the breadth of the organization's operations both externally and internally, underscoring the vast nature of the information needed to protect. The people, departments, and reporting structure for the entire privacy program are reviewed. The authority held by the CPO and CISO is emphasized. All relevant policies and procedures are reviewed

and cast under the umbrella of the USPS's "business model" as an independent government entity and strategic direction as outlined in the Transformation Plan.

This portion of training is followed by explaining the specifics of the BIA – its description and scope, timing, roles, IT lifecycle, and benefits. The training process walks through each section of the BIA document. The supporting relationships, laws, and policies relevant to each section are reviewed. The training also instructs staff how to complete each section of the BIA using examples of how to populate each section (an automated process) (e.g., sections for development and production information, systems of records, and data management, etc.).

Interviews with the manager for strategy and processes in the privacy office resulted in more information about organization-wide, general privacy training and awareness offered through videos, case studies (for executive staff), email correspondence (e.g., email etiquette), campaigns (privacy and security week), and posters and signs. It was also mentioned that training or messaging addresses the consequences for violating the Privacy Act as well, noting the successful Linda Tripp lawsuit against the Department of Defense for divulging information from her personnel folder (D. Kendall, personal communication, February 13, 2009).

Training within the privacy office also lends itself to the Certified Information Protection Professional (CIPP) credential, which is held by several key staff. Obtaining this credential is encouraged among staff, but not required. The office also helps to develop some of the course work for the CIPP test offered by the IAPP (D. Kendall, personal communication, February 13, 2009). Training for the CIPP is strongly interrelated to expertise, particularly given the expansive growth of the IAPP and the number of CIPP professionals over the last decade.

Records management is another area of expertise that is interrelated to training and is a central factor to the BIA process. The records management officer, like the privacy officer, has grown into a recognized profession. Many colleges and universities offer degree programs in library and information sciences which cover records management. Professional organizations such as the Records Management Association (RMA) and the Institute of Certified Records Managers provide separate, non-degreed, professional certification for practitioners, or the Certified Records Manager designation (CRM). Additional expertise programs are offered in the form of a certificate program through the AIIM International, or the American Records Management Association (ARMA). ARMA outlines generally accepted recordkeeping principles (GARP) which defines the discipline of records management.

Training becomes a key factor that shapes the foundation for the professional expertise that will support a policy implementation effort. In this case, the PIA implementation required training of personnel specific to the PIA process itself, but also personnel for information security, privacy, and records management. Both variables are interrelated in this way as training is a necessary component of developing a profession in a particular area of expertise. Professional expertise, in turn, also influences training, or the training process and content for a particular policy area. In this case, the professional experts became a key source of building and executing the training programs for staff vital to the implementation process. And not only professional experts serve as a source of training, but as we will learn in the next section, professional networks and associations, too.

Professional Expertise and the BIA

Professional expertise to support the BIA process and broad policy implementation is spread across privacy, information security, IT, legal, and records management. However, in

this study, the professional expertise related to the office of the privacy officer and records management emerged as the most influential.

The skill set or expertise required for a CPO have varied and evolved. Legal background or a law degree was typically a prerequisite given the need for deep privacy law knowledge. But a CPO also needs a wide range of skills and expertise related to customer service, to developing and building relationships, operations, IT, and ultimately knowing a company inside and out – knowing its top priorities. The position also requires strong expertise to drive programs and policies (Z. Strickland, personal communication, February 18, 2011).

According to Strickland, "A good privacy professional is engaged in what's going on…privacy changes so much, you need to be listening." She explained this statement in the context of why she launched the effort to eliminate SSNs because they were overused, overdistributed, and causing problems (Personal communication, January 21, 2011).

Staff that work in information security require the requisite knowledge of IT, systems, data flows, etc. Chief Information Security Officers and some of their supporting staff will likely have obtained the Certified Information Security System Protection (CISSP) credential as part of their training.

Expertise in records management plays a critical role in the BIA process as well. A primary consideration for any organization that conducts a privacy audit or assessment is the organization's record-keeping system; in particular; records professionals and their duties related to information used by the organization. The records analyst can and should be a key component to preserving privacy of all types of information in large organizations. Privacy audits, therefore, tend to focus on testing the controls and evaluating the effectiveness of this function (Duff et al., 2011).

A records manager is someone who is responsible for records management in the organization, which can include classifying, storing, securing, and destroying records, i.e., the lifecycle of records. This position may also include a range of broader, strategic activities such as planning the information needs of the organization to creating, approving and enforcing policies and practices regarding records, and coordinating access to records internally and externally (Duff et al., 2011).

Records management has grown as a centralized function of organizations since 2005, in light of new compliance regulations and statutes and scandals such as Enron. Statutes such as the Sarbanes-Oxley Act of 2002[33] have led to more standardization of records management practices within organizations. As such, the role of the records manager has gained much more authority over the course time, shifting from a position that was previously regarded as unnecessary or as a low priority administrative task. The role has also evolved to become closely intertwined with IT management, legal, compliance, and risk (Raths, 2010).

Professional expertise is directly related to the organizational structure and can be understood within the context of the creation of various offices and departments.

Organizational Structure and the BIA

In the USPS, the overall organizational structure to support the BIA and privacy policy implementation is highly centralized. The professional areas of expertise that support this structure include IT, information security, privacy, and records management. The following describes a top-down structure in terms of authority; however, the analysis in Chapter 5 will show an organization that tends to be more flat in its structure largely because privacy policy as a function of an organization has been highly centralized.

[33] This legislation introduced major changes to the regulation of financial practice and corporate governance.

The Executive Vice President and CIO report to the Postmaster General and are responsible for defining and developing business solutions that will enable the USPS to achieve its strategic goals, hence the CIO sits at the top of the organizational structure. This position is highly technical in nature given the responsibility it bears for the daily operations of one of the largest technology networks in the world. The CIO operates one of the world's largest intranets which connect the USPS's processing and distribution centers, bulk mail centers, priority mail processing centers, air mail facilities, and post offices across the country.

Security is another important component of organizational structure and requires expertise in deploying effective controls in preventing security breaches. This expertise usually takes the form of a CISO and dedicated information security personnel. The appointment of a CISO or creation of this office is important for fulfilling the task of developing, implementing, and monitoring the organization's information security program. Other critical tasks for the CISO include establishing security requirements for all third-party and outsourcing vendors; providing education, awareness and training on information security issues and new best practices to personnel throughout the organization (Elson & LeClerc, 2006).

The role of the CPO marks a critical component of the USPS's organizational structure to support the implementation of broad-reaching privacy policy. Former CPO, Zoe Strickland described the creation of this role as a horizontal function. According to Strickland:

> Privacy is like any other new function in an organization, both public and private…a company has to look at what makes sense to bring together, e.g., IT, security, records management, etc. Privacy is a very horizontal function – you're organizing your company around privacy efficiently (Personal communication, February 18, 2011).

Accordingly, Strickland drove an important shift in structure under her leadership by placing Privacy Act responsibility within the records management department, referring to

this as “a natural fit” and noting the trend in privacy officers taking on more records management functionality (Personal communication, February 18, 2011). The integrated nature of this office and expertise will be discussed further in the analysis in Chapter 5.

Summary

The case studies outlined in this chapter provide only an introduction to a deeper understanding of the PIA implementation process and the influence of training, expertise, and organizational structure. Chapter 5 presents this analysis of the implementation process with a picture of two disparate organizations and two unique characterizations of how privacy policy becomes manifest over time.

CHAPTER FIVE – CASE STUDY ANALYSIS

The analysis in this chapter addresses the primary research question to understand how privacy impact assessments (PIAs) have been implemented within the VA and the USPS and how this process has changed over time. The analysis is guided by Edelman's (1992) model for understanding how policy becomes manifest within organizations by examining such factors as the role training, professional expertise, and organizational structure (e.g., creation rates of offices, internal policies and rules). A close look at these factors in relationship to the PIA shows to what extent organizations integrate these factors to manage and implement privacy policy. While these are not the only factors that influence the process of PIA implementation, these factors were the focus of my research to identify characteristics and patterns in the process and the potential consequences for privacy management in public organizations. These factors became my focus based on Edelman's (1992) research, prior literature on implementation, and my own reflections and early analysis of the case studies.

My research generated a lot of process data and limited interview data. The VA is the predominant focus of the two case studies because of the limited interview data that was collected from the USPS. The USPS stands as a minor case study that is useful for making distinctions about different approaches to the PIA implementation and also for understanding the environmental and political context for both agencies that may have influenced the implementation process. The data collected is supported by extensive document review and content analysis. Documentation review and analysis was based on internal agency materials spanning across policies, guidelines, handbooks, reports, presentations, congressional testimony, and Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget (OMB). Other document analysis stemmed from OMB Memorandum,

National Institute for Standards and Technology (NIST) guidelines, and Government Accountability Office (GAO) reports.

The analysis begins with the VA because of the rich data that the analysis yielded and therefore, also resulted in more extensive analysis than the USPS. To manage and enhance the level of analysis, the case studies are structured to examine two time periods: 2002 – 2006 and 2007 – 2010.[34] This approach is most useful for the VA analysis because the first period can be categorized based on the pre-data breach years versus the post-data breach years. The two time periods are also useful to think about implementation in terms the nascent versus mature stages in the process. The USPS implementation process matured very quickly in the early years and did not face disruptive events such as data breach. However, the pace and rigor for which the USPS approached its implementation process was characterized by congressional scrutiny and fiscal pressures forcing it to transform itself quickly to improve both its management structure and ability to comply with privacy laws. Both organizations were influenced by the political environment that was driving the e-government movement and both were under considerable political pressure to realign or transform their IT infrastructures to respond to advancements in technology and increased security and privacy threats. In effect, this approach provides a richer context for describing the evolution of the PIA process, the impact and interrelationship of the factors that influence the process, the role of FISMA reporting (for the VA), emergent trends, and environmental context. This approach was influenced by Edelman's (1992) use of event-history analysis to understand the evolution of EEO/AA policy and the use of "stages" of change is common among most implementation and organizational theories (Clune, 1983).

[34] Recall in Chapter 3 – Methodology the section that explains the use of implementation time periods. The use of time periods also mirrors Edelman's (1992) examination of "stages" of organizational response to the law. However, Edelman's focus is narrowed by its focus on what constitutes compliance and how it becomes institutionalized, which is beyond the scope of this research (p. 1532).

The findings are descriptively theoretical and provide rich insight into how organizations vary in their approach to policy implementation. The findings show that certain processes can lead to learning while other processes may become static and routinized, or fizzle out; revealing that process does, in fact, matter. Edelman's (1992) hypothesis is that organizations can show "gradual growth" (e.g., through the creation of structures) and that this growth is also impacted by political pressure and enforcement efforts (p. 1547). In my study, the VA is indicative of how this gradual growth takes place and how the data breaches made the agency sensitive to political pressures as wells as to enforcement via FISMA reporting. The USPS's approach is better characterized as command and control and largely attributable to its business-like organizational model. Hence, the USPS's approach to implementation was shaped by the use of centralized authority, a reliance on firm policies and procedures, and the need to address an array of problems that it was facing that could negatively impact its overall survival.

It is in studying the various characteristics of implementation processes that we can better understand how policy becomes manifest in organizations and how organizations adapt their processes to respond to change over time. The factors that influence this process and their interrelationships can be interpreted using a case study approach that leverages process data and qualitative analysis of interview data. In effect, these factors shape the focal process of this study, the PIA. The interaction of these factors can affect organizational culture, learning, and leadership but can also drive diverse policy management approaches and outcomes across organizations. These factors are also influenced by the environmental and political context that impacts each organization's distinctive approach to implementation.

Therefore, the process of policy implementation becomes a tool by which organizations come to understand an ambiguous and changing legal environment. The result is a dynamic and

evolving process that unfolds which can be analyzed to understand the need for effective policy management to drive desirable policy outcomes broadly across the organization. For example, the case of the VA, the agency was able to realize gradual improvements in process and policy outcomes over time (e.g., improved ratings in FISMA reports, efficiencies in operations, enhanced coordination, and centralized training). Hence, the efficiencies in process that are gained in response to one particular mandate can be applied to other implementation efforts. The USPS approach aimed at identifying and solving immediate problems posed by the external environment and in its ability to address perceptions of weakness in management and structure and ability to compete in an e-commerce environment. The findings offer valuable insights into the field of public management and public administration not only for expanding our understanding of how policy is enacted, but more broadly for how privacy policy is becoming a pervasive dimension of informative governance in organizations.

This chapter first establishes a context for the case study analyses based on the findings. Each case study is then presented separately, beginning with the VA and organized to address the following attributes of the research: evolution of the PIA, training, professional expertise, organizational structure, patterns and change in policy implementation, and lessons learned.

USPS and the VA – Context for Analysis

The USPS case study reflected a more strategic[35] approach to privacy policy implementation driven by a performance and service-based culture and the designation of a primary leader. In the case of PIA implementation, the USPS employed rapid decision-making and established clear lines of authority. A centralized, layered and procedural approach to

[35] By strategic, I am referring to an approach that had a very strong start with high intensity and highly centralized decisionmaking and authority. Key facets of this approach were centralized leadership that enforced timely and effective implementation of decisions, drove awareness of best practices, and ensured better design of significant policy initiatives. The approach was also strategic in the sense that it was driven by a larger strategic plan outlined by the Postmaster General in the 2002 Transformation Plan as discussed in Chapter 4.

implementation allowed the USPS to create a consistent, proactive, and collaborative approach to privacy policy that could be sustained over time.

This approach was influenced by mounting fiscal pressures and political scrutiny. The USPS was in a defensive position to sustain its independent status, respond to privacy concerns, and modernize its organizational structure. The USPS already had a centralized management structure in place in contrast to the VA's decentralized structure which may explain the agency's ability to rapidly execute its implementation strategy for BIAs.

This centralized approach was solidified through strong leadership and vision that stemmed from the designation of a Chief Privacy Officer to drive the policy implementation process across the enterprise and from beginning to end. Leadership also emerged as key factor to support the organization's need for specialized training and that would support a cadre of professionals that could effectively implement policy directives and norms. The organizational structure and design provided the avenues to coordinate across a diverse group of professional experts that could inform the policy implementation process through information sharing, collaboration, and shared expertise. Recognition by management of the need to bring the right blend of experts together to effectively implement broad policy change was critical to the overall implementation effort.

The VA case study varies widely from the approach taken by the USPS. The implementation process was challenged from the beginning and took more time to get off the ground than the USPS. General uncertainty was a contributing factor to a fragmented and initially decentralized approach to implementation. The VA was challenged to match policy design with clearly defined policy objectives which could partly be attributed to the absence fragmentation of leadership, competing mission objectives, and lack of funding, and staffing

needs. The VA experienced a several changes in political appointee leadership over the course of ten years in the role of the CIO. The overall progress of the implementation process was hindered by what became a reactive stance to the policy environment (e.g., data breaches, changes in reporting requirements, etc.) which only made comprehensive enactment of policy a moving target. In other words, the VA was always moving towards problem resolution in the process. However, as the policy process evolved, the VA was able to learn and adapt to better manage policy outcomes. In many ways, the VA was able to recognize its weaknesses and respond with new management tools contributing to the emergence of a smarter and more innovative organization. In a sense, the VA's approach to implementation was organic, lending itself to an ability to continually recalibrate its design to realize continuous improvement to policy outcomes.

The orientation of these agencies is important because while the PIA serves as a the focus point of this study, other influential factors rendered each agency's approach as unique – one that is influenced by the nature of the organization, outside environmental factors, and the level to which each is able to integrate the factors of training, professional expertise, and organizational structure to adapt to a rapidly changing policy environment.

The VA and the Evolution of the Privacy Impact Assessment

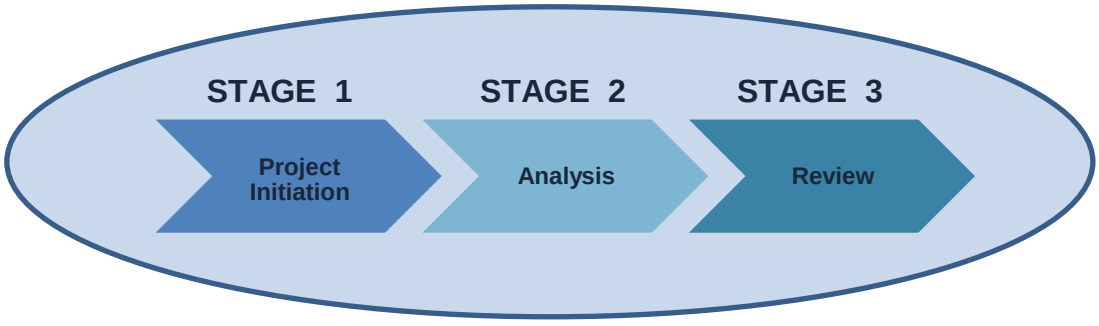
The evolution of the PIA in the VA was a challenging process from the time of the initial requirement set forth by the E-Gov Act. According to staff, their understanding of how the PIA process came about was based on two reasons:

> 1) the process was mandated because government wanted an idea of the systems that contained personal health information (PHI) and personally identifiable information (PII) and to get a handle on the plethora of databases popping up; and 2) the government, in general, said "let's see what these databases contain to decide on the necessary levels of protection" (H. Corbin, personal communication, February 6, 2009).

The second point is important because the PIA became a critical task for all federal agencies by way of its direct link to the federal budgeting process by OMB Circular A-11 Section 300[36], which requires agencies to report on various information systems to obtain operational funding. Corbin interpreted this link to the budgeting process to mean "To get my funding, I have to fill out a PIA" (H. Corbin, personal communication, February 6, 2009). This understanding of the mandate implies a lack of buy-in to the process and points to an unfolding reactionary approach to policy implementation that was exacerbated by an overall lack of guidance from the oversight body (the OMB).

Despite this lack of guidance by the OMB, the key stages of the PIA process remained constant and straightforward across agencies: training, project initiation, analysis, review, approval, and recertification.[37] This study is primarily concerned with the central elements of the process: project initiation, analysis, and review. Figure 7 illustrates the stages of the PIA that are the focus of this study.

Figure 7. Three Stages of PIA Process Analyzed in this Study



Although training is a key stage in the PIA process, it is treated more broadly in this analysis in relationship to the other variables – professional expertise and organizational structure. All of these factors together shaped the PIA process and analysis will show how

[36] See OMB Circular No. A-11, Part 7, Section 300. A PIA is required for all Exhibit 300 submissions, which serve as budget justification and reporting requirements for major information technology investments.
[37] The mechanics of the PIA process are also illustrated in Figure 1 in Chapter 2.

certain combinations or dimensions of these factors may have triggered or shaped changes to the process over time.

As mentioned earlier, the case studies are analyzed according to two time periods: 2002 – 2006 (the pre-breach years) and 2007 – 2010 (the post-breach years). It should be noted that the breaches themselves are not the focal point of the analysis. However, these events presented considerable management challenges and influenced the overall future direction of implementation efforts and policy outcomes. Given that the key driver of PIA implementation was to inventory and protect holdings of PII throughout federal agencies, the 2006 and 2007 data breaches generated a series of significant changes throughout the organization that changed the direction of the policy process.

PIA in the Pre-Data Breach Years: 2002-2006

In its infancy, PIA implementation in the VA was largely unguided and characterized by fragmented policies and internal decision-making. In the absence of consolidated and standardized policies and procedures, analysis of FIMSA reports to the OMB was conducted to inform an understanding of the PIA implementation process between 2004 and 2010.

In its first FISMA Report to Congress in 2004, the VA reported a total of 678 major information systems, out of a total of 8,623 major information systems represented by twenty-four (24) agencies included in this report. The only agencies that reported on more systems were the Department of Defense, the Department of Energy, and the National Aeronautics and Space Administration. But, the number of systems the VA had to report on and develop PIAs for, was staggering and indicative of paramount task before the agency.

Table 10 shows the VA's CIO report of the following metrics in the 2004 FISMA Report to Congress.

Table 10: 2004 Metrics Reported by Agency VA CIO

Effective Security and Privacy Controls (C&A):	14%
Security Costs Included in the System Lifecycle Costs:	86%
Tested Security Controls:	83%
Tested Contingency Plans:	82%
Percentage of Employees Trained in IT Security:	77%
Cost per employee trained:	$12.77

Source: Federal Information Security Management Act (FISMA) 2004 Report to Congress, p. 40.

This early report shows the one-dimensional nature of reporting at the time, largely dependent upon the analysis by the CIO and apparent emphasis on security versus privacy. This narrow focus on security and the resources attributed to IT training, may explain why interviews suggested that there was no real privacy training in the early years. The Office of the Inspector General concluded in the report that the VA approach to PIA implementation was incomplete.[38]

A notable change in FISMA reporting occurred in 2005 that required agencies for the first time, to assign a risk impact level (high, moderate, or low) to their systems. Twenty-five (25) agencies were included in the 2005 report for a total of 10,289 systems, an increase of 19% from 8,623 systems reported on 2004. The VA reported on 585 systems (322 high, 38 moderate, 222 low), lower than the number reported in 2004 which could reflect the nature of this shift from reporting at a *program/project* level to a *systems* level. The focus of training was still narrowly focused on IT security awareness training as reflected in the report showing that of all the 773 employees with IT security responsibilities, all of them received training at a cost of nearly $3 million.[39]

The emphasis on information security in the 2004 and 2005 reports point to a lack of integration of privacy efforts with IT security which is supported by interview data that reflected

[38] U.S. Department of Veterans Affairs Office of Inspector General. (2006, July 11). *Review of issues related to the loss of VA information involving the identity of millions of veterans.*
[39] U.S. Office of Management and Budget. (2005). *FY 2005 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://m.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/reports/2005_fisma_report_to_congress.pdf.

an organizational structure in its nascent stages of trying to coordinate areas of expertise. The original intent in the E-Gov Act's privacy provisions to make the PIA process multidisciplinary had not quite been incorporated into the policy design at this point. In the OMB's review of the 2005 FISMA reporting, it noted only a few agencies failed in their ability to integrate the PIA process across the necessary areas of expertise, the VA was among these agencies.

The 2006 FISMA reporting made changes that, for the first time, outlined privacy reporting in addition to security reporting. The GAO played a key role in fostering this change by issuing recommendations for strengthening the FISMA and for improving overall security weaknesses in federal information systems.[40] The GAO also outlined the key privacy challenges facing federal agencies in May 2006 congressional testimony by Linda Koontz, Director, Information Management Issues.[41]

This shift in reporting to include more privacy specific measures marked a pivotal point to tracking agency progress on PIA implementation and performance. Regrettably, the 2006 FISMA reporting period reflected a record number of security incidents or events, such as data breaches, that could lead to the compromise of sensitive information. Several agencies experienced high level data security breaches in 2006, the most notable being the VA. These breaches were attributed to "internal" problems within the agencies.

[40] U.S. Government Accountability Office. (2005). *Information security: Weaknesses persist at Federal agencies despite progress made in implementing related statutory requirements.* (GAO-05-552). Washington, D.C.
[41] Statement of Linda D. Koontz before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives, "Privacy: Key Challenges Facing Federal Agencies" May 17, 2006. Retrieved from http://www.gao.gov/assets/120/113843.html.

PIA in the Post-Data Breach Years: 2007-2010

The FISMA reporting between 2007 and 2010[42] began to reflect a gradual shift in meeting key privacy performance measures. An important change to the 2007 FISMA reporting included a new question for agency Inspectors General (IGs) concerning the quality of the agency's PIA process. The VA only reflected limited progress and its PIA process was rated as poor, along with only two other agencies. This rating is largely attributed to the data breach events at the VA and other similar cases of PII disclosure reported by other agencies.

The changes in 2007 were also paralleled by the OMB's request for copies of privacy-related policies and plans in conjunction with agencies' FISMA report submission. A significant plan that had to be submitted was one to eliminate the unnecessary use of Social Security Numbers.

The FISMA reports for 2008 through 2010 showed overall improvements in privacy performance measures. The VA improved in its evaluation by the IG and received a rating of satisfactory for its PIA process. However, it should be noted that the 2009 FISMA Report was prepared by an independent accounting firm and was not released to the public because it was considered sensitive information. The report concluded that the VA "continues to face

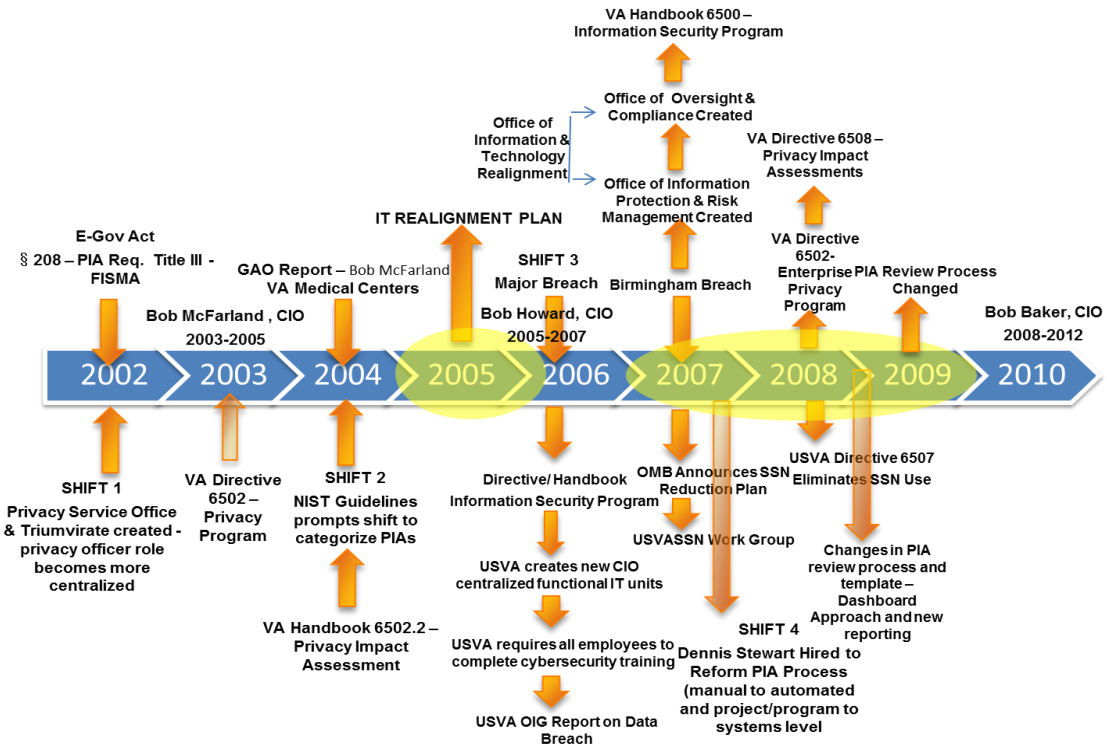
[42]U.S. Office of Management and Budget. (2010). *FY 2010 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf.
U.S. Office of Management and Budget. (2009). *FY 2009 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.
U.S. Office of Management and Budget. (2008). *FY 2008 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/reports/fy2008_fisma.pdf.
U.S. Office of Management and Budget. (2007). *FY 2007 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://m.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/reports/2007_fisma_report.pdf.

significant challenges in complying with the requirements of the FISMA due to the nature and maturity of its information security program" (Lipowicz, 2010).

The VA's progression of improvement is discussed in the following section in relationship to changes that the VA made to its PIA process during this same time period. Many of these changes were triggered by the data breaches in 2006 and 2007. A series of procedural, technical, and design changes to the PIA throughout 2007 – 2009 impacted the overall evolution of the policy implementation and drove other changes in training, professional expertise, and organizational structure. In effect, many policy shifts occurred over the course of the two implementation time periods which were introduced in Chapter 2 but are discussed in more detail in the section on *Policy and Structural Changes* in this chapter.

The timeline depicted in Figure 8 is helpful for understanding the breadth of changes that occurred between 2002 and 2010 in the VA.

Figure 8. Timeline of Privacy Policy Implementation for the VA



Procedural, Technical and Design Changes to the Privacy Impact Assessment

As noted earlier, the FISMA reporting prompted a shift from a project or program level PIAs to a systems level PIA. At this same time, the VA was trying to affect a technical shift from a manual to an automated PIA process. These technical changes prompted additional design changes to the actual PIA document and review templates to make the PIA more user-friendly for the involved participants.

The shift from a project or program level to a systems level PIA was not only driven by changes in FISMA reporting but also by new guidelines issued by the National Institute of Standards and Technology (NIST)[43] in FIPS Publication 199[44] issued in February 2004. The guidelines responded to the objective created under FISMA which tasked NIST with responsibilities for standards and guidelines, including the development of standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency. Hence, these overall procedural, technical and design changes were externally driven and required the agency to adapt its processes.

Analysis of interview data with agency staff reflected the extent of the impact that these guidelines had on the overall PIA process, primarily at the *initiation* and *analysis* stages. A direct impact to the *initiation* stage resulting from the shift to a system level PIA generated the need for the VA to report on over 600 "major" systems in 2008, an increase from 40 PIAs completed at the project level in 2007. In 2008, the staff took on PIAs for the minor applications

[43] Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details. FIPS documents are available online through the FIPS home page: http://www.itl.nist.gov/fipspubs/. Accessed February 1, 2012 http://www.itl.nist.gov/fipspubs/geninfo.htm.

[44] Federal Information Processing Standards Publication No. 199 - *Standards for Security Categorization of Federal Information And Information Systems*. February 2004. Accessed February 1, 2012 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

which amounted to about 400. At the time of this study, 649 PIAs were in cue for 2009 and later analysis will show how the organization adapted to this shift in volume through structural and expertise-based changes. The expanse of systems to report on exerted pressure on the agency to organize itself to better manage the PIA process from beginning to end (Personal communications, October 10, 2008).

Agency staff welcomed this shift and noted the positive benefits of PIAs at the system level, which allowed them to see the types of information being collected, what was being done with that information, and where the information was being stored. It also increased the accountability of the system owner or manager as reflected in the comment "the system manager is on the hook for that system and responsible from the administrative and financial standpoint that the system is reliable" (D. Stewart, personal communication, October 10, 2008). However, a complete collection of PIAs was also necessary to perform any kind of review and analysis.

Subsequently the *review* and *analysis* stage of the PIA process also underwent changes between 2007 and 2008 driven by a shift from a manual to an automated process to provide for quicker analysis and faster correlation. The shift to automation was also viewed favorably by staff, noting that it strengthened the review process by enabling staff to detect what forms were being used, what data types were being collected, and to get an understanding of the quality of information that was being provided in the PIA (D. Stewart, personal communication, October 10, 2008).

In the *review stage* of the PIA process, completed PIAs were submitted to the Privacy Office using a review template that ensured consistency in the review process. Interviews described the 2008 review template as very *subjective* and based on narrative information. In 2009, the review process became more *objective*, incorporating "yes" and "no" questions and

drop down menus to collect information with very little narrative involved. This shift in the review process achieved desirable results according to staff, "we've now learned more about *what* information is collected and *where*" (Personal communication, October 10, 2008).

These changes drove more consistency in the PIA process and had a ripple effect in impacting the *analysis* and *approval* stages as described by staff:

> We did an analysis of PIAs and looked at data types and what systems are collecting what type of information. We analyzed this information and were able to correlate information contained in the PIA to the SORN which [supported] collections forms that OMB had approved for VA use (D. Stewart, personal communication, October 10, 2008).

Stewart described the review process as one that enabled his staff to "detect what forms are being used, what data type and get an understanding of the quality of information that is coming through in the PIA" (D. Stewart, personal communication, October 10, 2008). These observations could indicate that changes to the review process led to an improved management process for the PIA. The process itself became more comprehensive and organized by sectioning out important compliance areas such as SORNS, internal VA guidelines and policies, Privacy Act, COPPA, and agency security controls and risk assessment policies. Note that this change took place in 2008, six years after the USPS took this same approach.

Policy and Management Changes that Influenced Structural Changes

Analysis of interview data also showed that the changes to the PIA process also allowed staff to identify where internal policies were weak and to address these shortfalls to guide the organization toward better policy development. This change is indicative of the emergence of a strong feedback loop in the PIA process represented by a "dashboard" mechanism:

> We notated the shortfalls where enough detail was not provided [in the PIA] and we prepared a response or what we call a 'dashboard' that is given to the system

> owner to show them what parts they are having trouble with and includes a second page that contains comments from the reviewer This is sent back to the team – the Triumvirate that created the PIA is then put in touch with the reviewer and a call can be set up to review the process with them to help them complete the PIA so that Dennis' group can approve it (D. Stewart & S. Wallace, personal communication, October 10, 2008).

This dashboard approach and awareness of the need to reform internal policies and procedures led to enhanced communications supported by the creation of new organizational structures, focused professional expertise, and more consistent policies. Interviews also suggested an increased level of buy-in at very high levels of the organization pointing to a more centralized approach to overall policy implementation (J. Buck, Acting ADAS, Office of Privacy and Records Management, personal communication, December 10, 2010).

The increased level of buy-in was represented by a new monthly reporting program to the Deputy Secretary about the progress in the PIA process. The reporting was structured to reflect improvements in the process through color ratings (e.g., red, green, or blue). Buck described the process as "more involved and more detailed" than in the past. Changes to organizational structure brought together the necessary areas of expertise to produce these reports by the creation of the VA Triumvirate in 2002 (J. Buck, Acting ADAS, Office of Privacy and Records Management, personal communication, December 10, 2010).

In 2008, the VA Directive 6508 consolidated the policies and procedures to support the structural changes between 2006 and 2008. This Directive morphed through a series of policies and handbooks that were developed over the course of 2003 to 2008 as depicted in Table 8 in Chapter 4. This key policy captured the magnitude of the change that was taking place within the agency. The Directive expanded on the existing roles and responsibilities of all of the participants to the PIA. These cumulative policy changes were directly related to overall changes in organizational structure.

The PIA and Organizational Structure

As described in Chapter 4, the VA Triumvirate was created in 2002 for the purpose of developing PIAs. The Triumvirate includes a privacy officer, a local CIO in each facility and a security officer to represent the different perspectives on information: records related information, System of Records Notification information (SORN), and security information. The Triumvirate established a centralized mechanism for facilitating collaboration across all of the disciplines necessary to support the PIA process. The term "team" was frequently used in interviews to characterize the Triumvirate. The Privacy Officer for the Office of Information and Technology, explained the relevant areas of expertise captured by the Triumvirate:

> The system owners should know how many systems he or she has within their organization. They have to know that. The Information Security Officer (ISO) has to be present because they have to make sure all of those security controls are satisfied. The Records Office should be there because we talk about the System of Records. The System Owners are not going to know about the System of Records. And then the Privacy Officer, who looks at COPPA, System of Records makes sense, make sure OMB number is there, security controls, how does the law tie into the system, and how has the program been funded (Personal communication, November 19, 2010).

The Triumvirate fulfilled the organizational objective to combine security and privacy expertise. The Privacy Officer for the OI&T commented "security and privacy work hand in glove you can't have one without the other it's just impossible." She also underscored the importance of the records manager to the Triumvirate, "without the record you're not going to have security and you won't need privacy. So you have to have the records officer there" (Personal communication, November 19, 2010). This observation points to the interrelationship between organizational structure and professional expertise.

The primary driver of this team mentality was provided by the creation of the Privacy Service as a function of the OI&T led by the CIO. The Privacy Service became responsible for

reviewing and approving all PIA forms – the final step before PIAs were provided to the OMB for review for the applicable fiscal year. This structural change centralized the PIA process mainly into the roles of two key individuals, Christine Pettit and Dennis Stewart, described as the "PIA Team within the Privacy Service" (Personal communication, November 19, 2010).

The structural changes within the VA were not without challenges and sometimes faced resistance from various participants to the PIA process. The Privacy Officer, OI&T, explained "there's a lot of pushback sometimes because the system owner feels that you don't need a PIA in the infancy of it [the PIA]." The Triumvirate and the Privacy Service were put in place to ensure that privacy was not an afterthought in the policy process, that it was placed "upfront" (Personal communication, November 19, 2010).

The Privacy Service played a predominant and supportive role to the Triumvirate through the consolidation of expertise and policy to support the PIA process. Dennis Stewart became the hub of PIA expertise and was responsible for "getting a list together of all systems" (Personal communication, November 19, 2010). At the time of the interview there were 6000 systems within the VA that the Privacy Service had knowledge of and Dennis Stewart identified the systems that he believed required a PIA. Understanding the number of systems that required a PIA was an important management need and critical to the FISMA reporting process and privacy performance measures.

Once all of the systems that require a PIA have been identified, the Triumvirate is brought in to analyze the dynamics of the data and information in the system. Once the Triumvirate has completed the PIA template for a system, the PIA is submitted to the VA's SMART database (Security Management and Reporting Tool). Another individual is responsible for pulling the PIAs for review. The Privacy Officer, OI&T, noted that this person pulls PIA s

and reviews them "all day long." Their responsibility is to ensure that the PIA is complete and accurate, "that it makes sense" and references the appropriate OMB number, SORN notice, types of data elements, and all of the security controls (Personal communication, November 19, 2010). The reviewer for the PIAs was assigned to Christina Pettit who works directly with Dennis Stewart.

If any problems are identified with the PIA, it is sent it back to the Triumvirate team for additional information or verification. Upon approval, the team decides what portions of the PIA can be published on the Internet as required by the law, however, some PIAs may not be published due to the sensitivity of the information that it contains. The Privacy Officer, OI&T, emphasized "We publish [PIAs] to show the public we have nothing to hide. These are our systems and this is what we have on those systems and this is how we hold the information" (Personal communication, November 19, 2010).

The Privacy Service ultimately became the glue that holds all of these various structures together in support of the PIA process. Its strategic decision to operate as a team fulfilled its objective to bring together a disparate group of departments and expertise to support the critical task of completing PIAs, which also manifested into an overall attitude or set of norms for the way the VA thinks about privacy policy broadly.

Analysis of interview data showed that many structural changes and the creation of new departments were the direct result of the data breaches. Hal Corbin described the period of 2007 to 2009 as witness to departmental change in "leaps and bounds" (Personal communication, February 6, 2009). Corbin himself was part of this change and became the Regional Director for the Office of IT Oversight and Compliance (ITOC), an office created as a direct result of the breaches that reported directly to the CIO. This reporting structure or level of autonomy was

"necessary to give his office some teeth"…because the CIO is the "key person in charge" (Personal communication, February 6, 2009).

It is interesting to note that Corbin characterized the biggest problem in information protection as the culture. He described a culture of information protection that was present before the breach, "but to a greater extent now." He elaborated that shaping the culture was influenced by broad policy training and awareness programs across the organization, from public service announcements (PSAs), posters, etc. He emphasized the importance of reminding people (employees) broadly, but for managers and senior managers, "these are the people on the hook, so the mentality is pervasive throughout everything they do" (Personal communication, February 6, 2009).

The next section addresses the role of professional expertise in the PIA evolution.

The PIA and Professional Expertise

As the VA's PIA implementation process evolved over the years, analysis of interview and process data shows that the lines that traditionally segmented security, IT, privacy, records management or other areas, began to blur and that some expertise migrated from one area to another. For example, in an interview with Sally Wallace, then ADAS in the Office of Privacy and Records Management, she described her evolving role since joining the VA in 1990 where she began as an IT program manager heavily focused on the Y2K project. She began her role as the deputy to cybersecurity in 2001, within two years became a Chief Architect for VA operations and then moved into privacy and records management and assumed responsibility for privacy programs, records management, e-discovery and FOIA. In this role, the Acting Director of the Privacy Service reported to her and "became the driving force for reforming the PIA process" (Personal communication, October 10, 2008).

The Acting Director, Dennis Stewart,[45] was asked to join the Privacy Service in 2007 and to "reform the PIA process." Dennis reported having a twenty (20) year history in privacy and security in various government agencies. He explained the first year of his position as

> Trying to change and better the process and improve the process. PIAs are a key task. We deal with compliance issues and oversight of privacy issues within the VA. I think I bring a wealth of information to the VA when I joined them (Personal communication, October 10, 2008).

According to Wallace, a key motivation for changing the process resulted from the grade of "poor" by the IG in the 2007 FISMA Report. Sally explained that she and her boss "realized that they could improve a lot and Dennis' expertise has helped them to reform that process and fix what the IG told us to fix" (Personal communication, October 10, 2008).

Professional expertise for the highest levels in the organization included IT and management – represented by the CIO. The case studies point to the significance of the CIO as the primary leadership authority for IT and having a direct linkage to the top of the organizational structure. In the USPS this is the Postmaster General, in the VA this is the Secretary.

Privacy and legal were clearly the responsibility of a CPO which has emerged as a critical managerial role for the implementation of privacy policy in organizations. It should come as no surprise to learn that the CPO also plays an integral role in shaping and driving the PIA process.

Finally, the role of records management was an interesting twist in the research that drove further examination of the profession. The records management function is critical to IT

[45] It should be clarified that Dennis Stewart joined The Privacy Service as a federal employee and rotated as acting director along with others during the absence of the Director. The PIA effort was only one of many tasks earmarked for Stewart (Personal communication, November 16, 2012).

systems design processes and to the development and implementation of electronic information systems (Raths, 2011). Despite the critical nature of this role, federal agencies have not had a strong history of creating the basic infrastructure of a records management program, according to Raths (2011) who cited a NARA Survey Report:

> Without dedicated records management staff, clear policy directives and proper training, these agencies are at high risk of mishandling their information…they may find it difficult to meet their legal and operational needs, and their lack of coherent recordkeeping may inhibit Congressional oversight and public accountability (p. 30).

The case studies also support a transformation in the level of authority granted to records management professions particularly in policy implementation and their significant role in the PIA. Hoke points to a transformation in records management to "information governance" (2011, p. 3).

The PIA and Training

Many interviews with staff spoke highly of the training that was required and made available at the VA from the internally and locally developed training programs to the general privacy awareness training. Many of the comments linked expertise to the presence of CIPP professionals in the organization. In a 2008 interview, the respondent emphasized that the VA was "leading the government now for the number of people trained and certified for the CIPP/G (a Certified Information Privacy Professional with specialized expertise in government organizations)" reporting 66 CIPPs in 2008, clearly expressing pride in these numbers (Personal communication, October 10, 2008).

At the time, the VA also reported plans to develop an internal privacy certification program for staff that did not obtain the IAPP credential, which was mostly attributed to turnover. Interviews explained that sometimes employees were unable to take the CIPP test due

to extenuating circumstances creating a need to develop adequate training for staff to perform their jobs (Personal communication, October 10, 2008).

The importance of the CISSP credential was also linked to discussions of training in the interviews. Sally Wallace explained that when she was in security, "the CISSP was 'pushed.'" Sally Wallace and Dennis Stewart both had the CISSP credential, but Stewart was also a CIPP/G (Personal communication, October 10, 2008).

Patterns and Change in the Policy Implementation Process

The biggest pattern that gradually unfolded over the entire implementation period was the shift from decentralization to centralization. This was largely prompted by external environmental and political pressures driving the VA to pursue an overhaul of its IT infrastructure under Secretary Nicholson. The IT Realignment Plan was the result of decentralized budgetary discretion that was detached from the VA's system-wide IT strategy. The offices and structures created to support the PIA implementation process, together with broader privacy and security goals, began in 2002 with the creation of the Privacy Service and the Triumvirate, a structural change that centralized the expertise necessary to support PIA implementation process. The Privacy Service enabled the expansion of training and resources and the recruitment of specialists. Its creation also expanded the role of the privacy officer, making this role more managerial and responsive to a broader mission beyond compliance with privacy laws.

A pattern of fragmentation became evident in the development of policy that was not synchronized with structural changes. For instance, VA Directive 6502 – Privacy Program,[46]

[46] U.S. Department of Veterans Affairs. (2003). *VA Directive 6502 - Privacy program.*

was issued following the creation of the Privacy Service and the Triumvirate. In effect, the VA began the implementation process with the creation of new offices or with structural changes in the absence of broad organizational policies which would have helped to standardize the approach taken. This also contributed to a lack of communication, more broadly, to the organization about the impending shifts in privacy policy.

A reactive pattern also characterized the course of the PIA implementation process. The organization generally found itself in a position where is was continuously reacting to changes in the law, changes in reporting requirements, changes in technical standards, GAO or IG reports, or critical events such as breaches. The breaches catalyzed extensive structural and policy changes between 2005 and 2009 not only to the PIA process but also the implementation of broad privacy policy and information protection values. The breaches did, however, have a positive impact on process but also on widely held beliefs among key professional staff.

For instance, when discussing the 2006 breach, Sally Wallace said "she was in the dark as much as anyone." She was new to her position and the current CIO, Bob Howard, was appointed in an "acting" position after the departure of former CIO, Bob McFarland. This was a particularly disruptive point in the evolution of the VA's implementation process because Howard was appointed just as the 2005 contractor's assessment of the VA's IT organizational realignment was being completed and prepared to implement. The IG began to ask questions about the ramifications of an event that Veterans' information was exposed and how the VA would respond to such an event. The incident became very public and subjected the agency to a high level of scrutiny that prompted the agency to make immediate changes such as the reorganization of IT under the CIO, which were previously in the VBA and VHA (where all the data resides) (Personal communication, October 10, 2008).

Historically, the VA has been an organization characterized as resistant to change. This became evident in the 1990s as the VA underwent major restructuring. Resistance emerged because of threats to expertise of specialized groups, threats to established resource allocations, and threats to established power relationships (Dudley & Raymer, 2001; Chenoweth et al., n.d.). Despite its struggles with change over the years, the VA has certainly evolved and diminished its resistance to change and in fact, has transformed itself to embrace change and establish itself as a learning organization reflecting the ability to continuously adapt and change and make growth and improvement part of its culture (Robbins & Judge, 2009).

Lessons Learned

Analysis of interview and process data, supported by broad document analysis, reflected that the breaches clearly had valuable lessons for the VA. The organization had to get a handle on what they were doing–who held the data and policies needed to be enforced because they were not being followed. This is where political appointee and CIO Howard took more of an active leadership role and empowered all CIOs to be responsible for enforcing the rules. Hence the emphasis on directives, in other words, "this is the policy and you will follow it" (Personal communication, October 10, 2008). In this interview, it was noted that Wallace's boss, Adaire Martinez and Howard were "trying to change the culture, create solutions and hold people accountable."

The data breach experience was a hard lesson in terms of the costs that it imposed on the agency. Analysis of interview data suggested that the OMB did not support the need for the VA to offer free credit reporting to the Veterans impacted by the breach because of the expense and in light of pending lawsuits. One mailing, alone, of breach notification letters to Veterans cost the agency $8 million. The event was described as "an administrative nightmare that required

coordination with the SSA to determine those Veterans that were deceased or who had a change of address" (Personal communication, October 10, 2008).

Conclusions

The data breaches experienced by the VA are indicative of "situational" evidence that had both direct and indirect effects on the policy process in organizations (Wilson, 1989). Wilson (1989) argues that situation matters, or the situational mandates of the work being done by an organization. It follows that situations color an agency's response to how to implement policy and in this case, the data breaches had a direct effect on the PIA process within the VA and the factors to support this process. However, in the midst of these data breaches, the VA was also in the process of adopting a new IT Realignment Plan that would transform the organizational structure from one that was decentralized and fragmented to one that was centralized. This transformation was not only for the purpose of executing consistent policy implementations but also to drive more transparency and accountability in its budgetary operations. Other situations that may have influenced the evolution of the VA implementation of PIAs were the frequent turnover in political appointees that assumed the role of CIO, which was the top authority overseeing the IT infrastructure reform. Wilson's (1989) construction of organization mission also provides a useful lens for understanding the role of organization culture and its relationship to policy implementation. Although an analysis of organizational culture is not within the scope of this research, it does help us to think about how agency culture defines agency mission, assuming that agency mission in some form, shapes the policy implementation process. The mission of the VA was also impacted by the need to respond to a secondary mission to protect sensitive information and to incorporate broad privacy and security protections into its overall IT management structure.

The USPS provides a good case study for understanding the role of culture and mission in the implementation process and for drawing conclusions about how the disparate cultures and missions of public organizations can lead to different approaches to policy implementation leading to different policy outcomes.

United States Postal Service (USPS) and the Evolution of the BIA

The BIA process within the USPS is a critical element to continuing its progress of protecting communications privacy. While the USPS is not required to comply with Section 208 of the E-Gov Act, it does so voluntarily through its BIA which was created prior to 2002. These reports are made available to the public with limitations. However, the USPS is not subject to FISMA reporting as the VA is, so the same level of analysis based on this reporting was not possible. The trajectory of the BIA process for the USPS was fully detailed in the previous chapter and introduced the role of training, expertise and organizational structure on this process. These were factors that the USPS deemed important to the policy implementation process at the front end of its design. How the dimensions of these factors influenced and became part of the implementation process varies from that of the VA.

For instance, analysis of interview data showed that the USPS recognized the importance of a multidisciplinary approach early in its implementation design which, in turn, led to a coordinated effort to integrate privacy with corporate security to both support budgeting for the development of new IT systems and to ensure the security of the new systems and the presence of proper controls. This structural integration of professional expertise supported a BIA process that was designed to address all aspects of privacy from the tactical (e.g., examination of Privacy Act Systems of Records) to the strategic (e.g., consistent direction for policies and approaches). In this sense, the approach was holistic in its design. Former Chief Privacy Officer (CPO), Zoe

Strickland described this integration as "necessary to support a BIA process that would help drive privacy solutions and considerations in programs and applications and foster and facilitate the culture of privacy as part of a proud tradition" (Personal communication, January 21, 2011).

This multidisciplinary and structural approach to implementation was also influenced by external environmental and political factors. The USPS was under political pressure to first address its fiscal crisis but also to improve its management structure for e-commerce products and services which is also closely related to pressures to address concerns over the agency's compliance with the Privacy Act and other related privacy laws. Many of these privacy concerns stemmed from e-commerce considerations related to the use of sensitive customer information such as SSNs, addresses, and credit card information. The USPS has to move swiftly to show that it was addressing congressional concerns but also to reinforce its ability to compete in the marketplace as a communications service provider. The USPS was challenged to demonstrate decisive action and a consistency of effort.

The decision to "marry" privacy and security from the beginning also allegedly allowed the USPS to break through the "stove-pipe mentality" of other federal agencies. Strickland made the decision that it was important to bring IT into the BIA process and outlined the privacy laws that the agency needed to "worry" about. The result was the creation of new sections in the BIA document that addressed all of the relevant privacy laws and jumpstarted the process of collaboration between these offices, a process characterized as being "joined at the hip" (Personal communication, November 19, 2010).

While integration of processes was a central goal of policy implementation, another important goal of the USPS was to solve larger problems such as the elimination of SSNs, to generate standardization, to achieve operational efficiencies. The USPS was one of the initial

agencies that developed an alternative internal identifier for its 600,000 + employees referred to as the Employee Identification Number (EIN) in order to reduce the use of employee SSNs when dealing with personal issues such as payroll administration and tracking of training requirements. This approach to integration was driven by the performance-based culture and distinctive nature of the USPS's as a quasi-governmental organization that competes in the marketplace. Furthermore, a service-oriented mission influenced an approach that placed emphasis on leadership and authority based on a long tradition of what has been a command and control style agency. This command and control style placed emphasis on executive-level buy-in to implement sweeping policy change and a robust privacy program was no exception in this case. To drive strategy, under the direct of the Deputy Postmaster General, the USPS consolidated leadership and authority for policy implementation in its designation of the first federal-level Chief Privacy Officer (CPO) and decided that the CPO should report to the Office of the Consumer Advocate versus IT or legal (D. Kendall, personal communication, November 16, 2012).

This designation supported a privacy management structure with a senior designated privacy official (SAOP) long before guidance was issued by the OMB in 2005[47] and before the 2008 GAO report that recommended agencies give their SAOPs full oversight over all privacy-related functions.[48] This approach underscored the critical need for multidisciplinary expertise such as privacy, IT, information security, and records management. This recognition of the value of expertise underpinned the agency's support for broad training efforts and particularly,

[47] U.S. Office of Management and Budget, Executive Office of the President. (2005). *Designation of Senior Agency Officials for Privacy* (M-05-08). Washington, D.C.
[48] U.S. Government Accountability Office. (2008). *Privacy: Agencies should ensure that designated senior officials have oversight of key functions.* (GAO-08-603). Washington, D.C.

support for privacy expertise evident in its strong affiliation with the International Association for Privacy Professionals (IAPP) and its credentialing program.

The USPS's approach to privacy policy implementation was highly centralized and strategic from the very beginning. The entire policy design had a starting point that began with broad strategic direction outlined in the 2002 Transformation Plan.[49] In contrast to the VA's efforts to modernize its IT infrastructure, the USPS developed its strategy much earlier, recall that the VA did not unveil its IT Realignment Plan until 2006 in the wake of a major data breach. The business model approach of the USPS began with the identification of problems and long-term objectives. Once a plan was in place, the agency could operationalize its approach which became manifest in the creation of effective leadership, authority, and a supporting policy infrastructure.

Organizational Structure and the BIA

The organizational structure to support the BIA in the USPS was quite different from that of the VA. The USPS approach was more business-like with an emphasis on authority and hierarchy, reflective of its command and control style. This idea for developing a broad privacy and security program was seeded by a former "marketing guru" at the USPS who decided that the agency needed to worry about privacy and suggested that they consider getting a privacy officer and develop a privacy program. It is interesting to note the seeding of broad privacy objectives within marketing. However, this evolution makes sense in understanding the nature of how the USPS operates like a business and has to protect vast customer information. The origins from marketing may also indicate awareness by the USPS of the public-facing nature of protecting customer information and the need to convey its efforts to the broader public, to its

[49] U.S. Postal Service (2002). *2002 Transformation plan*. Washington, D.C. Retrieved from http://about.usps.com/strategic-planning/transform.htm.

employees, and to Congress. In effect, the USPS had to concern itself with its "brand" as part of its larger implementation efforts. The emphasis on authority and hierarchy led to the creation of an office for a Chief Privacy Officer (CPO) as early as November 2000 (D. Kendall, personal communication, February 13, 2009).

Furthermore, as the Postal Service advanced in its development of usps.com and other technologies, it saw that the privacy field was also evolving. The Postal Service has always had a trusted brand with its customers and wanted to maintain that brand into the future. According to Deborah Kendall "Without customers, the USPS could not sustain itself since it became an organization in 1972 funded not by tax dollars but by revenue from the stamp-buying public" (Personal communication, November 16, 2012).

Deborah Kendall, Manager, Privacy and Consumer Policy Office, described the infancy of this process as it stemmed from a meeting with the corporate information security program which resulted in the decision to "build an office to show that we are complying with all privacy laws" (Personal communication, February 13, 2009). Hence, the process began with an identification of the key privacy statutes that the USPS had to comply with such as COPPA, the Gramm-Leach Bliley Act (GLBA), FOIA, the FTC's Fair Information Management Practices, and more. The USPS was not required to comply with the E-Gov Act, although it voluntarily agreed to do so. In effect, the beginning of the policy implementation process in the USPS embedded two areas of expertise together – privacy and security based on the assumption that the system the agency is responsible for is ultimately a customer system and the agency was tracking people for marketing purposes which added an element of risk that required mitigation efforts.

The decision to locate the privacy function in the Office for Consumer Affairs and Consumer Advocate is worthy of discussion as previously noted. Locating the privacy function in this office helped to widely broadcast the agency's commitment to protecting privacy and to continuously communicate its efforts to support this goal. Upon Strickland's appointment, she reported the Vice President of Consumer Affairs and she had formerly worked in the Office of General Counsel, which likely explains the early compliance focus of the BIA implementation process and the identification of all relevant privacy laws. According to an interview, the CPO was housed in consumer affairs because "it's about the consumer and should come out of consumer affairs" (Personal communication, November 19, 2010). These actions made Postmaster General Potter a recognized leader for driving a strong privacy program that resulted in the USPS being named the most trusted government agency for six consecutive years(2004 – 2010) by the Ponemon Institute (Fillichio, 2006).[50]

Strickland's position actually expanded in 2003 to include, in her designation as CPO, Manager, Consumer Policy and Strategy. With this additional function, Strickland was given responsibilities to address all policies and procedures in addition to privacy, that impact consumers and small businesses. At this time, Strickland directly reported to the Vice-President and Consumer Advocate, a fitting function for privacy, but also had a dotted line directly to the Office of the Postmaster General (Personal communication, February 18, 2011).

Within Strickland's office, 12 people were focused on privacy-related areas such as privacy programs (including policies, processes, training, and employee and customer communications); records management; strategies and research; and Privacy Act and FOIA

[50] The Ponemon Institute is a research organization dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. Each year, The Ponemon Institute conducts an annual *Privacy Trust Study of the United States Government.*

compliance. A cross-functional privacy board was created in conjunction with the privacy office. The privacy board is responsible for vetting all privacy policies and processes for the organization, and our office educates them on emerging privacy trends. The board expanded over the years to include information security and other functions such as marketing, human resources, communications, government relations, legal, and the postal inspection service. In the field, in 85 districts, Consumer Affairs Managers were designated to serve as coordinators for privacy and FOIA throughout the country (Personal communication, February 18, 2011).

A factor that is critical for a strong program and implementation process is the need to have the buy-in and support of the top of the organization, as well as from management and peers, something that the VA struggled with. The USPS took a structural approach to ensure adequate executive buy-in and to ensure effectiveness by building a framework based on the "4Ps": People: identify and involve the right people in the organization; Policies: establish policies based not only on laws but also your brand; Processes: create processes for compliance with all policies; and Publication: communicate effectively internally and externally (Carter and Goel, 2005).

Other factors that are important to support a privacy program include sufficient resources in terms of staffing and a sufficient budget – one that can support the necessary training, the acquisition and development of subject matter experts, and privacy-oriented technologies and systems. In this case, the IT department likely has the higher budget so it is important to have a strong relationship with IT and to have that department be open to the input of the privacy office regarding vendor solutions that impact both privacy and security.

What is difficult to understand about the agency's decision to marry the functions of privacy and security at the front end of the BIA implementation process is the functions and role

of IT and security. In my interviews, it was explained that IT functions were previously broken down into portfolios managed by a portfolio manager. For instance, one portfolio may handle HR, supply management, and facilities. New system changes under this previous portfolio structure required the portfolio manager to work with someone from information security, and quite possibly, also someone in the consumer advocate or legal department. In my discussions with USPS staff, it seems that much of the discretion for making decisions about BIAs fell with the Information System Security Officers who were part of the corporate information security office reporting to Peter Stark, the CISO – who directly reports to the CIO. The information security function is all housed in Raleigh, NC which is where incident response is handled as well (Personal communication, February 13, 2009).

Unlike the VA's creation of the Triumvirate to coordinate its PIA process, the USPS placed responsibility within the IT department to identify and discuss any new IT systems that would require a BIA. Recall that this responsibility was housed within the Privacy Office and a designated expert was assigned to the PIA process and coordination. In the USPS, the IT department assumed responsibility for coordinating meetings to discuss any new IT systems that might require a BIA. The system owner for any new project would need to identify the data that the new system would collect and the intended use of that data. In doing so, the system owner had to collaborate with the CISO and the privacy office. It makes sense now that in interviews with the USPS, they reported some resistance from IT, particularly when the responsibility had to become shared between privacy and security (Personal communication, February 13, 2009).

The sharing and integration of responsibilities and expertise at the USPS made relationships a critical component to support collaboration for the BIA process, to pull the bench strength, so to speak, from a range of disciplines and expertise. From the beginning to the end of

the BIA process requires instrumental relationships between diverse areas of expertise and across the organization's structure. Hence, collaboration became a key element that shaped the USPS's ability to integrate training, expertise and organizational structure to support the BIA process.

Another important facet of organizational structure is the need to establish policy priorities and communication of those priorities. The capacity to accomplish this task was driven by the leadership and vision of the CPO. Strickland exceled at this and created a solid policy framework to support implementation by creating internal policies for privacy and information security, such as the Handbook AS-353 *Guide to Privacy, the Freedom of Information Act, and Records Management* (the "Handbook") that was issued in 2005 and updated in 2009.[51] The Handbook became an internal guide to privacy, the FOIA, and records management and served as a primary source for overall direction and guidance to the organization. It also called out the need for a partnership between the privacy office and information security as well as the need for security of information addressed in separate guidance, *Handbook AS-805: Information Security*.

The Handbook was a strategic move in the sense that it supported the goals outlined in the 2002 Transformation Plan and set out to ensure the proper collection, use, and protection of customer and employee information. Both handbooks helped to operationalize the BIA for the participants involved in the process.

Eliminating the use of SSNs was a hallmark of Strickland's broad-based strategy to implementing privacy policy and was launched in 2003. This strategy was borne out of the Unique Identification Program (UIP) housed within the human capital office. This move by Strickland precipitated the same directive that came out of the President's Identity Theft Task Force – reflected her leadership ability to anticipate trends. Strickland made this effort one of

[51] Handbook AS-353 *Guide to Privacy, the Freedom of Information Act, and Records Management.* Retrieved on February 14, 2009 from http://www.usps.com/cpim/ftp/hand/as353/welcome.htm.

her top priorities as CPO and the agency moved forward with a program and policy to assign unique numbers to employees and to mask any existing SSNs. The result was the implementation of a modern HR system that digitized official personnel folders (OPFs) which reside with the National Archives and Records Administration (NARA) upon an employee's retirement (D. Kendall, personal communication, November 19, 2010).

Another important technology aspect of organizational structure was the development of the USPS's Enterprise Information Repository to support the BIA process. The repository enables the agency to manage all of its IT systems (over 1000 applications run by the USPS as reported in 2009). The USPS also implemented a significant technological undertaking to transition to digitized records for its employees. This effort resulted in over 700,000 Office of Personnel Files (OPFs) being digitized with security and quality control (D. Kendall, personal communication, November 19, 2010). This is an important point to note because the VA was much slower to innovate in terms of creating a central database – its SMART database. However, the USPS was also driven to move faster in developing this infrastructure based on congressional pressure for the agency to create a structure for managing and categorizing its e-commerce products and services, which was also closely tied to its needs to comply with a range of privacy laws.

What becomes difficult to ascertain is how the USPS's BIA process and privacy program, particularly in terms of structure, has evolved over the years given its major accomplishments in the early years before 2006. In the early stages, the focus was on developing policies, processes, and networks. As this process matures, the focus tends to shift to compliance, training, and auditing. Certainly, at some point, new policies may be needed and often as a result of new technology as a driver. Examples for the Postal Service include policies for

intelligent mail services, cameras in lobbies, and records retention for both hard and soft copy data. Intelligent mail is a particularly sensitive topic as it operates like global positioning systems using standardized barcodes on each piece of mail and mail container. Intelligent mail refers to capture and sharing of information to the mailer about each piece of mail throughout the system from point of origin to destination.[52]

Other developments in the marketplace may exert pressure on the USPS to evolve such as the FTC's 2012 Privacy Report[53] which will require a code of conduct for application developers that support mobile technology. As the USPS expands its services to the mobile platform, the privacy challenges increase exponentially. The agency is also currently operating under extreme budget constraints and is challenged by competitive market forces.

Professional Expertise and the BIA

Professional expertise to support the BIA process and broad policy implementation is spread across privacy, information security, IT, legal, and records management. However, in this study, the professional expertise related to the office of the privacy officer and records management emerged as the most influential.

In an interview with former CPO Zoe Strickland, she explained how the skill set or expertise required for a CPO has varied and evolved. Legal background or a law degree was typically a prerequisite given the need for deep privacy law knowledge. But a CPO also needs a wide range of skills and expertise related to customer service, to developing and building relationships, operations, IT, and ultimately knowing a company inside and out – knowing its top

[52] See the USPS website for more on intelligent mail https://www.usps.com/business/intelligent-mail.htm.
[53] U.S. Federal Trade Commission. (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.* Washington, D.C. Retrieved from http://ftc.gov/os/2012/03/120326privacyreport.pdf.

priorities. The position also requires strong expertise to drive programs and policies. According to Strickland, "A good privacy professional is engaged in what's going on…privacy changes so much, you need to be listening." She explained this statement in the context of why she launched the effort to eliminate SSNs because they were overused, overdistributed, and causing problems (Personal communication, February 18, 2011).

An important consideration in how the structural role of the CPO relates to professional expertise is the office's reliance on advice from others in the organization. The CPO often has to weigh questions for which there are no clear answers, particularly where laws intersect with each other or with industry practice. Other considerations include weighing your organization's tolerance for risk, so the CPO must analyze policy and compliance options and consequences. In this sense, it is critical for a CPO to turn to others for advice to improve their decisionmaking but to also help generate buy-in to support decisions among stakeholders in the process.

A CPO and their staff may turn to external resources to seek further expertise through consulting with the IAPP and leveraging its extensive network of privacy professionals. Expertise can also be leveraged from cross-industry groups such as the Center for Information Policy Leadership (CIPL)[54] and the Responsible Information Management (RIM) Council.[55]

Based on analysis of interview and process data, a key task of the CPO is to stay abreast of emerging trends and to bring these issues back to the organization to generate engagement and dialogue on those trends. Hence, the staff that supports the privacy office should perform ongoing analyses of media stories, privacy studies and surveys, federal and state legislative and

[54] The Centre for Information Policy Leadership develops initiatives that encourage responsible information governance necessary for the continued growth of the information economy. For details see http://www.informationpolicycentre.com/.

[55] The RIM Council is based on ethics-based framework and long-term strategy for managing personal and sensitive employee, customer and business information. It is a select group of privacy, security and information management leaders from multinational corporations that is managed by The Ponemon Institute. For details see http://www.ponemon.org/rim-council.

regulatory activities, and enforcement actions via courts or regulators. As mentioned earlier, this is another reason to establish strong ties to the privacy professional community through groups like IAPP, CIPL, and the RIM Council. But for the Postal Service, it also joined workgroups like the one that the OMB sponsors for agency privacy professionals. Expertise can also be sought using advocacy groups such as the Center for Democracy & Technology (CDT) and the Electronic Privacy Information Center (EPIC). And some publications might include Evan Hendrick's *Privacy Times* and Alan Westin's *Privacy & American Business*.

Staff that work in information security require the requisite knowledge of IT, systems, data flows, etc. Chief Information Security Officers and some of their supporting staff will likely have obtained the Certified Information Security System Protection (CISSP) credential as part of their training.

Expertise in records management plays a critical role in the BIA process as well. A records manager is someone who is responsible for records management in the organization, which can include classifying, storing, securing, and destroying records, i.e., the lifecycle of records. This position may also include a range of broader, strategic activities such as planning the information needs of the organization to creating, approving and enforcing policies and practices regarding records, and coordinating access to records internally and externally (Raths, 2011).

Records management has grown as a centralized function of organizations since 2005, in light of new compliance regulations and statutes and scandals such as Enron. Statutes such as the Sarbanes-Oxley Act have led to more standardization of records management practices within organizations. As such, the role of the records manager has gained much more authority over the course time, shifting from a position that was previously regarded as unnecessary or as a low

priority administrative task. The role has also evolved to become closely intertwined with IT management, legal, compliance, and risk (Raths, 2011).

Training and the BIA

The first source of training for the BIA begins with the *Handbook AS-353 - Guide to Privacy, the Freedom of Information Act, and Records Management* issued in 2005. Strickland called for the development of this handbook as a premise to support all relevant staff training. Previously, this handbook served only as an administrative support systems manual for IT and security (D. Kendall, personal communication, February 13, 2009).

Training for the BIA begins with a comprehensive review the BIA process, objectives, and scope. The scope brings attention to the breadth of the organization's operations both externally and internally, underscoring the vast nature of the information needed to protect. The people, departments, and reporting structure for the entire privacy program are reviewed. All training modules are developed and taught by the manager for strategy and processes in the privacy office, who directly reports to the CPO. In this study, this role belonged to Deborah Kendall, Manager, Strategy and Processes, USPS Privacy Office.

Kendall described the specialized training that she provided to portfolio managers, IT, and new security staff to include face-to-face training in the headquarter offices and training made available more broadly using various media. She described the training as basic in nature, but followed by several training modules developed by herself (Personal communication, November 19, 2010).

The scope of the BIA training brings attention to the breadth of the organization's operations both externally and internally, underscoring the vast nature of the information needed to protect. The people, departments, and reporting structure for the entire privacy program are

reviewed. The authority held by the CPO and CISO is emphasized. All relevant policies and procedures are reviewed and cast under the umbrella of the USPS's "business model" as an independent government entity and strategic direction as outlined in the Transformation Plan (Personal communication, November 19, 2010).

This portion of training is followed by explaining the specifics of the BIA – its description and scope, timing, roles, IT lifecycle, and benefits. The training process walks through each section of the BIA document. The supporting relationships, laws, and policies relevant to each section are reviewed. The training also instructs staff how to complete each section of the BIA using examples of how to populate each section (an automated process) (e.g., sections for development and production information, systems of records, and data management, etc.) (Personal communication, November 19, 2010).

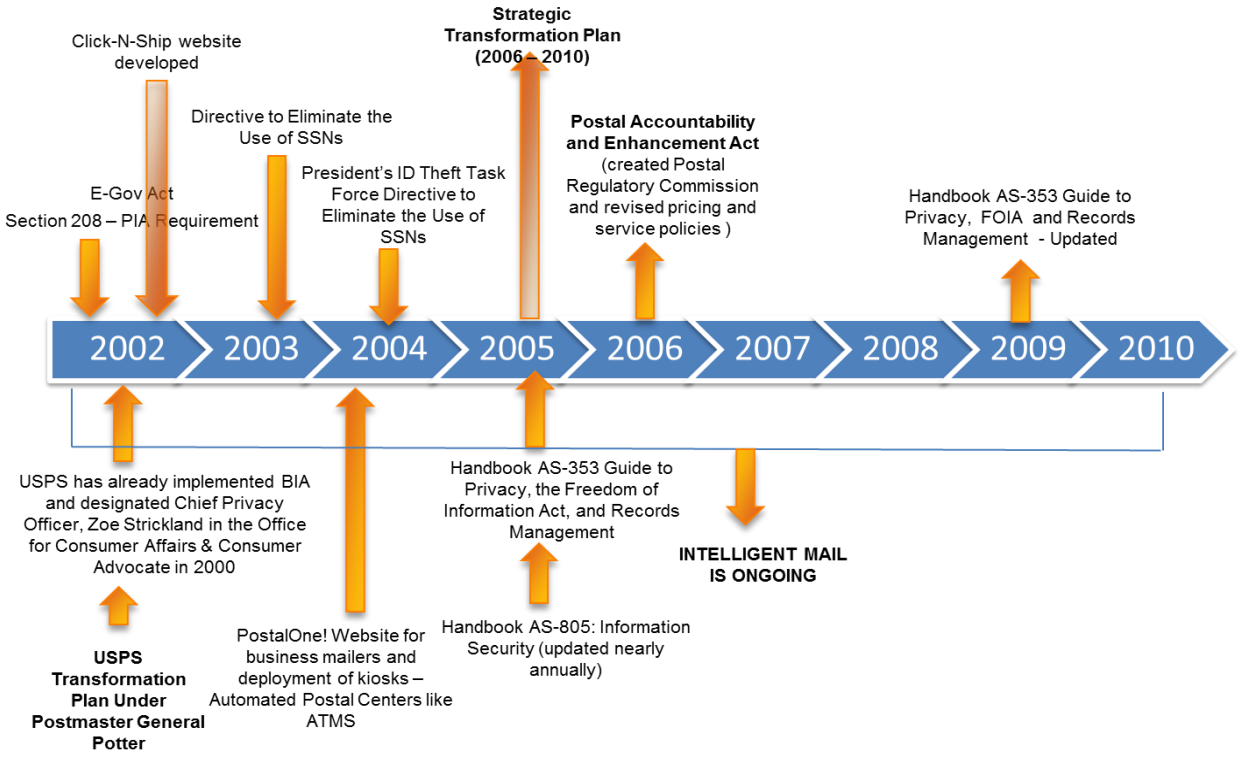
Kendall also discussed general, organization-wide privacy awareness training offered through videos, case studies (for executive staff), email correspondence (e.g., email etiquette), campaigns (privacy and security week), and posters and signs. It was also mentioned that training or messaging addresses the consequences for violating the Privacy Act as well, noting the successful Linda Tripp lawsuit against the Department of Defense for divulging information from her personnel folder (Personal communication, February 13, 2009).

Training within the privacy office also lends itself to the Certified Information Protection Professional (CIPP) credential, which is held by several key staff. Obtaining this credential is encouraged among staff, but not required. The office also helps to develop some of the course work for the CIPP test offered by the IAPP (Personnel communication, February 13, 2009). Training for the CIPP is strongly interrelated to expertise, particularly given the expansive growth of the IAPP and the number of CIPP professionals over the last decade.

Records management is another area of expertise that is interrelated to training and is a central factor to the BIA process. The records management officer, like the privacy officer, has grown into a recognized profession. Professional organizations such as the Records Management Association (RMA) and the Institute of Certified Records Managers provide separate, non-degreed, professional certification for practitioners, or the Certified Records Manager designation (CRM).

It becomes apparent that training shapes professional expertise, but that professional expertise, in turn, shapes the training within the organization as demonstrated by the extensive training that largely resides with the privacy office and officer. Figure 9 provides an overview of the BIA implementation process between 2002 and 2010.

Figure 9. USPS BIA Timeline



Summary

In the nascent stages of the PIA implementation process, the VA had a reactive approach. However, despite the many challenges posed to the agency throughout the process, those interviewed were forthcoming and candid about the problems that they faced. This willingness to share their stories and be so open about the process translated to a sense of commitment toward not only the process, but to policy outcomes. An assumption could be made that an organization with a fragmented and challenging implementation process would be less likely to share their story, to publicize visible problems, and to perpetuate a negative image. Instead, the openness of the VA staff led me to conclude that this was an organization willing to embrace change and to learn, an organization that weathered the implementation process as an evolution – subject to experimentation and to trial and error.

The USPS seemed more prone to resting on its laurels as a pioneer, less willing to reveal any management and implementation challenges. However, the USPS also has to protect its internal processes and brand image due to the nature of its independent status and its competitive position in the marketplace. The message that was conveyed in my interviews with the USPS was that things were done the right way from the very beginning period. The way the BIA process was explained to me in my interviews lacked the emotion that emanated in my conversations with the VA staff, other than the excitement that described the accomplishments of Zoe Strickland as the first CPO (Personal communications, November 19, 2010, and February 13, 2009). Based on my interviews, the USPS portrayed an image of being fail-safe and free from error in its approach to implementation. The process was very black and white and linear, whereas the VA revealed many more grey areas in its process, points of experimentation, and a

"learn as we go" approach. The USPS was more determined to get it right from the very beginning – to bake privacy into its overall policy design and implementation process. For this reason, the agency was ahead of its time and nearly ten years before the broad acceptance of PrivacybyDesign principles (Personal communications, November 19, 2010 and February 13, 2009).

Another characteristic that led to such disparate approaches in policy design lies in the orientation of the two agencies. For the USPS, in particular, its orientation toward profitability and business model design resulted in a different strategy design that started with the identification of the big privacy problems out there in the marketplace and the negative consequences that could impact the agency's bottom line and reputation. This awareness of risk and consequences may also explain the unwillingness of the USPS to be more transparent about their approach. Both organizations, or any organization for that matter, is subject to reputational risk and legal ramifications; however, the way that each organization responded to the presence of this risk was very different.

Conclusions: Disparate Approaches to Policy Implementation

Bamberger and Mulligan (2011) in their review of Smith's research provides a useful framework for explaining the diversity in the process of PIA implementation between the USPS and the VA. Smith's research in Bamberger and Mulligan, distinguished between a proactive and strategic privacy policymaking process versus "wandering and reactive" policy-making process. These disparate approaches easily characterize the approach of the USPS versus the VA, respectively.

Smith's research, like mine, reflects how the CPO was integrated into senior management – on the front-end in the USPS and gradually within the VA. And what flows down from these

executives are policies and practices intended to manage privacy cohesively and consistently throughout the organization. Such mechanisms in turn send powerful signals about the importance of privacy to the rest of the organization. These developments alone are worth notice, as they provide the indicia of strong management commitment—in the form of "corporate policies, organizational structure, measurement and control systems . . . and organizational culture" (Murray, 1976, p. 7, in Bamberger & Mulligan 2011).

Centralized coordination of issues across business units, moreover, can help ensure that these issues are not marginalized and avoid "silo" behavior in which locations and divisions are principally focused on maximizing their own accomplishments, harming the organization as a whole (O'Dell & Grayson, 1998; Gioia & Thomas, 1996, in Bamberger and Mulligan, 2011, p. 24). The decentralized approach to PIA implementation by the VA contributed to a lack of ownership in the policy process by key professionals. This lack of ownership or autonomy in the organizational structure hindered the capacity to manage the implementation process to improve outcomes.

The 2006 Report of the Department of Veterans Affairs, Office of Inspector General (OIG Report), supports conclusions reached based on my interviews. The Report indicated a lack of consolidation or standardization for VA policies and procedures for safeguarding information and data. This perpetuated the decentralized and reactive approach to policy implementation because consistency in following all applicable requirements in a similar fashion was not ensured among all employees, particularly through the availability of training. The OIG Report found that VA employees and contractors were not adequately trained and reminded of the policies and procedures to follow to safeguard personal or proprietary information.

In my research of the VA's internal policies, practices and procedures, I found it very difficult to identify a consistent method or any direct correlation between policies and the implementation process, meaning policies and procedures were issued at irregular intervals over a long period, and in separate guidelines, memoranda, directives, and handbooks, and in response to various laws and other legal requirements. As such, there was no consolidated repository of instructions and requirements that employees could research and follow, nor was there an adequate method for ensuring that all policies and procedures issued by VA were current. These findings are also supported by the OIG's 2006 Report.

The fragmentation of VA policies and procedures issued over a long period, and the issuance of numerous local policies and procedures issued independently by each administration within VA, contributed to many of the procedural and control inconsistencies that are noted throughout this report. With respect to training, the OIG was able to obtain limited memoranda to support training for privacy policy in the form of memorandums from the ASIT in early 2006. The OIG further found that there was no consolidated and current set of policies and procedures that employees and contractors could access to ensure all applicable requirements are being met. VA employees that wanted to learn about privacy and cybersecurity policies met various challenges to accessing such information on the intranet and there was no direct link on the main VA home page to VA-wide directives. The OIG findings further reflected the need for multiple time-consuming searches and sort through tens of thousands of "hits" before locating pertinent directives, which mirrored my own research efforts.

Both case studies reflect a direct relationship between CPOs and privacy policy and PIA training and education. The privacy officers or "advocates" in these case studies also indicated the influence of the IAPP as a source of training and expertise, but also the reverse influence of

the privacy experts in both agencies on the IAPP and its certification process. The IAPP has emerged as a recognizable source of expertise and training and provides a space for networking and information sharing among privacy professionals. The creation of an association for privacy professionals generates a sense of culture across the profession – this culture has a strong presence at these professional conferences.

CHAPTER SIX – ADVANCING IMPLEMENTATION

The literature surrounding privacy is extensive and largely rooted in the legal field. Despite the expansive nature of the privacy literature, the treatment or study of privacy policy and management in the field of public administration and policy is scarce. Even more scarce is any research on the process of privacy policy implementation.[56] While there may be numerous approaches for analyzing the process of privacy policy implementation, the scope of this research is narrowed by way of examining a particular approach to policy implementation—the privacy impact assessment (PIA). In this way, this study focuses on *process* implementation[57] and makes a unique contribution to the vast implementation literature (Pressman & Wildavsky, 1973; Bardach, 1977; Mazmanian & Sabatier, 1983; deLeon & deLeon, 2002; Schofield & Sausman, 2004; & O'Toole, 2004) in public administration and policy. By focusing on the process of implementation, this study responds to Pressman & Wildavsky's (1973) message that policy conception must account for the whole picture – from conceptualization to where the rubber meets the road, or where policy becomes reality in how it is being done and who is being held accountable for what is being done. Understanding the underlying process of implementation introduces a way of thinking about implementation also encouraged by Bardach (1977) by "looking at the players…their strategies and tactics…and the nature of communications among the players and the degrees of uncertainty surrounding the possible outcomes" (56).

[56] The study of implementation is a complex endeavor and challenging to define. Fixsen et al. define implementation as "a specified set of activities designed to put into practice an activity or program of known dimensions," which is a useful definition for understanding implementation in this study (2005, 5).

[57] Fixsen et al. set forth several categories of implementation based on implementation literature that discusses the purposes and outcomes of implementation attempts – paper implementation, process implementation, and performance implementation. They define process implementation as "putting new operating procedures into place to conduct training workshops, provide supervision, change information reporting forms, and so on," (2005, 6).

The research design is informed using the sociology of law literature rooted in Lauren Edelman's (1992) model for investigating how implementation becomes understood within organizations. Edelman (1992) contends that the factors that influence the policy implementation process are endogenous, or internal to the organization, and therefore, provide a means for analyzing overall impacts and changes to the implementation process over time. This can be done by examining factors that operationalize the process, such as training, professional expertise, and changes to organizational structure as reflected in the case studies of the U.S. Postal Service (USPS) and U.S. Department of Veterans Affairs (VA) in this study.

Edelman's (1992) model, as used in this research, becomes a vehicle for understanding the *process* by which agencies implement ambiguous law and policy and adapt the law to fit their own interests. Further analysis based on Edelman supports conclusions that outline the relationship between policy implementation and privacy policy outcomes and identifies relevant management challenges. Understanding policy implementation from this perspective can bridge the divide between public administration and law using the lens of the sociology of law literature to understand the need for better public management of information privacy and how better management can be achieved. The next section provides a fuller explanation of Edelman's (1992) model.

Edelman's Model

Edelman's research is largely focused on the realm of civil rights law and the adoption of equal opportunity laws and procedures within organizations. What is important to note is that her research begins with the assumption that law is ambiguous and uncertain, or that the "rules that regulate organizations tend to be broad and ambiguous" (1992, p. 1532). This ambiguity limits our understanding of the process by which organizations respond to the law. This study

acknowledges the work of other scholars to address the relationship between policy ambiguity and implementation (Matland, 1995; Offerdal, 1984; Lowi, 1979); however, this study is limited in scope to understanding implementation as a process.[58] Like Edelman (1992), this research begins with the assumption that privacy laws are ambiguous and therefore, seeks to address the uncertainties surrounding the enactment of privacy policy vis-à-vis the PIA process by understanding some of the factors that impact this process and policy outcomes.

Edelman (1990) also contends that organizations vary in their responsiveness and sensitivity to the legal environment. This variation in responsiveness and sensitivity can be affected by a range of factors such as the size of the organization, its legal experience, or its proximity to the public sphere (Edelman, 1992).[59] Other internal factors can shape and influence this response to how organizations enact policy, such as the role of professions and changes to the organizational structure (Edelman, 1999, 1992, 1990). These factors further influence the rate at which organizations create complex organizational structures (1992, 1990). All of these factors were considered in the case studies that were selected for this study and examined in detail in Chapters 4 and 5.

Edelman's (1999, 1992) model uses event-history analysis to model the creation rate of EEO/AA offices and internal EEO/AA rules in order to examine the process of change over time in response to EEO/AA law. She uses this method and contends that "legal environments exert continuous pressure on organizations…and event-history analysis allows for changing values

[58] Matland, (1995) addresses the theoretical significance of ambiguity and its impact on implementation. He presents an ambiguity-conflict model as an alternative model for reconciling existing findings on implementation.
[59] Edelman (1992) uses these same characteristics in her research and uses the term "public sphere" to mean "the culture surrounding the *federal* state and the federal legal order" (p. 1548). In essence, Edelman suggests that organizations that are closer to the public sphere are more sensitive to legal environments for many reasons, one of which is they "operate in an environment in which rule-based governance, bureaucracy, and notions of citizens' rights are highly institutionalized (1990, 1992, p. 1549).

and changing effects of exogenous variables over time, which is important because the climate of EEO/AA law and civil rights has changed considerably over the years" (1551).

My study does not employ event-history analysis to understand the legal environment for privacy law and policy. However, my research leverages Edelman's (1999, 1992) model and takes a modified approach to understand how certain variables change over time in relationship to the law. This is done through the analysis of a specific process, the PIA. Identifying stages in this process over time also allows for further analysis of the influence of particular events on the process, such as the creation of new offices, changes to organizational structure, new policies, and critical events such as data breach which dramatically change the climate for privacy law for any organization. In effect, the PIA process can be better understood as a means of privacy policy implementation by assessing the influence of training, professional expertise, and organizational structure on this process. Like Edelman (1999, 1992), I analyze the interplay among these factors to better understand the how organizations design customized approaches to the implementation of privacy policy and to a larger extent, how organizations respond to the need for information governance as a central task of the enterprise.

This analysis provides special consideration to *how* the agencies have customized and /or adapted this process to meet unique challenges such as data breach and a changing legal and regulatory landscape. These approaches to policy enactment may become ready models for other organizations. Edelman (2004) supports this proposition through research (Edelman 1999, 1992, 1990, and Sutton et. al., 1994) where she looks at the creation rates of discrimination grievance procedures that were slow the first few years after the Civil Rights Act of 1964 was enacted, but then these rates increased dramatically during the mid-1970s as the process of implementation became more familiar. Edelman showed that similar patterns hold for EEO offices and rules

(Edelman & Petterson, 1999). Similarly, the patterns by which the agencies create offices and rules (policy) to support the PIA implementation process can be evaluated using the factors of organizational structure and professional expertise, which are closely intertwined.

This study identifies patterns in the policy implementation process by first breaking the PIA process into stages and then organizing the case studies by time periods.[60] The use of two time periods for the analysis is particularly helpful in the case of the VA because the time frame can be organized to evaluate the PIA process in the pre-breach years versus the post-breach years and include analysis based on FISMA reports to understand how policy outcomes change over time. The USPS case study helps to create a context for the interpretation of the VA's PIA implementation process over time, since the USPS was a pioneer in enacting broach-reaching privacy policy before it was mandated. Similarly, Edelman (1992) identifies patterns based on the creation of EEO/AA offices and rules over time across 346 organizations between 1964 and 1989. Her results show that patterns are different for offices versus rules. For instance, her research shows that the presence of personnel departments lead to higher rates in the creation of rules, my case studies show similar patterns consistent with the presence of a privacy office or privacy officer, and the presence of strong leadership (1992, p. 1565).

Edelman's study also shows that new offices can be created without the simultaneous creation of rules, "the existence of one structure does not affect the formation rate of another" (1992, p. 1561). In other words, sometimes structure precedes rules and vice versa. The USPS is indicative of the former, affected by the creation of the office for the Chief Privacy Officer, who subsequently issued a host of new rules and policies. In contrast, the VA showed a tendency to begin with a patchwork of policies and rules that were not consistent with the

[60] Mazmanian and Sabatier note that "the implementation process normally runs through a number of stages" and that "the crucial role of implementation analysis is to identify the factors which affect the achievement of statutory objectives throughout this entire process" (1983, p. 541).

creation of new offices or related structural changes. This study does not judge whether one approach was better than the other but rather seeks to show how organizations respond to ambiguity in privacy mandates through their approach to implementation – to show that the implementation process in both cases provides an opportunity to learn new methods or to reach new goals (Offerdal, 1984 as cited in Matland, 1995). Offerdal sees implementation as a testing ground for principles, visions, and technological knowledge (199 as cited in Matland, 1995).[61] The findings also support conclusions about the implementation process that there is no quick fix about how to implement public policy and that sustained attention is important to successful implementation.[62] The evolving quality of the implementation process warrants managerial strategies that can accommodate adjustment and learning.

The case studies show two distinctive approaches to PIA implementation. The variation in these approaches and the processes lead to different policy outcomes. Changes in organizational structure over time is a particularly useful approach to understanding these variations in approaches and is supported by Edelman's research (1992) that contends organizations initially respond to ambiguity in law with formal structures. Hence, organizational structure is a key facet of her model that helps to paint a picture of process (1992, p. 1532). However, organizational structure is largely influenced by the professionals within an organization and both factors are influenced by the expanse and strength of training that is offered to drive an efficient process of policy implementation.

[61] Matland argues that "the degree of ambiguity inherent in a policy directly impacts the implementation process in significant ways…[by] influencing the ability of superiors to monitor activities, the likelihood that the policy is uniformly understood across the many implementation sites, the probability that local contextual factors play a significant role, and the degree to which relevant actors vary sharply across implementation sites" (1995, p. 159).
[62] This research does not seek to define "successful implementation" but acknowledges previous attempts to do so by scholars such as Ingram & Schneider (1990).

Organizational scholars have long pointed to the importance professionalism has as an important institution for mediating uncertainty in the face of environmental ambiguity (Edelman 1992; Arrow 1963, as cited in Bamberger & Mulligan, 2011). For Edelman (1992), professions fulfill a "filtering role" in the implementation process. She identifies tendencies among actors within organizations and how various professionals influence the process based on their area of expertise. In this way, Edelman (1999, 1992, 1990) expands upon previous implementation research[63] by digging deeper into the participants in the process – who they are, what their expertise is; the structures that they create or support as part of the implementation process (e.g., new offices, new rules, etc.), how they coordinate activities and policy goals, to how they obtain their expertise and information.

Specifically, Edelman shows how personnel and affirmative action professions play a critical role in helping an organization to understand ambiguities in the law and convey interpretations of the law that become integrated with the organizational structure to influence an "institutionalization" process (1992, p. 1546). While the treatment of institutionalization in organizations is outside of the scope of this study, the institutionalization process is a useful lens for examining the importance that privacy, security, and records management professionals play in the PIA implementation process and the evolution of broader privacy policy efforts within organizations. This process of institutionalization driven by professionals also takes shape in the form of professional workshops, conventions, workshops, and accredited credentials and professional affiliations that lend credibility to a particular field (Edelman, 1990; Edelman, Abraham, & Erlanger, 1992). The role of accredited credentials and other forms of professional

[63] Previous implementation research discusses participants in the process – their number and intensity, the role of hierarchical integration, and the assignment of implementing agencies or officials committed to statutory objectives (Pressman & Wildavsky, 1973; Bardach, 1977; Mazmanian & Sabatier, 1983).

experience were treated in the case study analysis in Chapter 5, reflecting the significance of CIPP, CISO, and records management professional credentialing.

These professionals play a vital role in conveying their interpretation of the law and certain areas of expertise tend to coalesce to drive the policy implementation process. My research design leverages Edelman's (1992, 1990) approach to understand how professional expertise or professionals shape the process of policy implementation. Findings show how professional expertise is related to changes in organizational structure and to the course of training throughout the organization to support policy implementation. These findings are supported by Edelman's (1997) claim that "law if often 'enacted' at a fairly local level, with intraorganizational professional constituencies playing a significant part in determining which institutional norms and scripts get reflected in organizational structures and practices" (Scheid-Cook, 1992 as cited in Edelman et al., 1997, pp. 479-515).

Empirical evidence on the filtering role of professions suggests that professional activities can either dampen or amplify the impact of law, depending on circumstances (Edelman et al., 1997). In referring back to the case studies, it becomes evident that the filtering role of professionals, namely privacy professionals, drove an amplified impact on PIA design and implementation in both agencies. However, the ability for these professionals to exert influence on the policy implementation process is closely linked to organizational structure in order to drive effective policy outcomes. For example, consider that privacy professionals within the VA were not able to drive the PIA implementation process forward and make sweeping policy design changes until the data breaches amplified the need for attention to privacy policy. Significant changes across professional expertise, organizational structure, and training occurred following the breaches of 2006 and 2007.

Accordingly, this research set out to uncover the relevant professional constituencies within the VA and USPS that could positively or negatively influence the impact of law within the organization and thus, the relevant impact on the PIA process. Identifying the professional constituencies or necessary areas of expertise and their relationship to organizational structure allowed for the identification of patterns of policy enactment in each case study.

Privacy Impact Assessment in the Literature

Since the PIA is the focus process being explained in this research, it was helpful to survey the extant literature on PIAs. The work of Bamberger & Mulligan (2008) (also influenced by Edelman) in the legal literature was relevant to this research to support findings and conclusions derived from the analysis of the PIA process in each agency. Bamberger & Mulligan (2008) introduce noteworthy research in their examination of the "digitization of administration" and raise questions about decisions that are made about the use of technology in public management and their impact on the protection of personal information and privacy policy. Hence, Bamberger & Mulligan (2008) take a technology focused approach to understanding privacy policy implementation at the program level within agencies. In doing so, they are able to show the inconsistencies in policy approaches across agencies and between programs within a single agency.

Their biggest contribution to understanding these inconsistencies is in their exploration of the PIA within the Department of State (DOS) and the Department of Homeland Security (DHS). Bamberger & Mulligan (2008) drill down into the actual PIAs conducted to support two very, specific programs, ePassport and US-VISIT, respectively.[64] They narrow their focus even further by their study of the adoption of specific technology, or radio frequency identification

[64] Bamberger and Mulligan (2008) describe the ePassport and US-VISIT programs in more detail in their research.

(RFID)[65], a highly controversial technology among privacy advocates (Magid, Tatikonda, & Cochran, 2009; Wasieleski1 & Gal-Or, 2008; and Mulligan & Perzanowski, 2007 as cited in Bamberger & Mulligan, 2008).

By comparing the PIAs in these two programs, they reveal the importance of agency structure, culture, personnel and professional expertise as important mechanisms for ensuring bureaucratic accountability to the secondary privacy mandate imposed by Congress. Their study further explores the relationship between independence, agency culture, expertise, alternative forms of external oversight, interest group engagement and management of privacy commitments within federal agencies (Bamberger & Mulligan, 2008).

In *Privacy on the Books and the Ground*, they help to expand the understanding of the impact that professionalism and expertise have on policy implementation (Bamberger and Mulligan, 2011). Privacy "on the ground" is the approach they take to conducting an inquiry into how corporations manage privacy and what motivates them to do so. Although the study is focused on the private sector, its findings correlate to the public sector because they study the role of the Chief Privacy Officer as industry leaders – a role that is present in both the public and private sector and a role that is analyzed in this research for its impact on the PIA implementation process and policy outcomes. Bamberger & Mulligan (2011) make the case for the rise and increasing influence of the privacy professional and its direct relationship toward meeting the management challenges of implementing privacy policy in organizations.

---

[65] Radio-frequency identification (RFID) is a technology that uses communication through the use of radio waves to exchange data between a reader and an electronic tag attached to an object, for the purpose of identification and tracking. It is possible in the near future, RFID technology will continue to proliferate in our daily lives the way that bar code technology did over the forty years leading up to the turn of the 21st century bringing unobtrusive but remarkable changes when it was new.

Privacy in the Public Administration Literature

Research in information privacy and its administrative implications, let alone general privacy concepts, is scarce among public administration and policy scholars (Nelson, 2002; Regan, 1995; Etzioni 1999).

In *Public Administration and Review,* Nelson (2002, 2004) used a rhetorical analysis to raise the level of awareness in the academic community about the inconsistencies between the rhetoric of public policy solutions post-September 11 and the philosophical and legal framework of American democracy. She explores the post-September 11 imbalance between individual privacy and the common good and posits that a better understanding of the theoretical framework of democracy and constitutional doctrine will advance the debate towards policy solutions.

Nelson (2002, 2004) challenges public administration scholars to meditate on the unprecedented age of information and see how it has altered our notions of privacy. This research responded to that challenge and represents a meditation on the nexus of the power of advanced technology and our notions of privacy; however, the focus is predominantly on the policy implementation process, relevant management implications, and policy outcomes. My aim was to understand the process that supports privacy policy implementation by focusing on one specific process, the PIA. This allowed me to analyze the PIA as a policy enabling vehicle using Edelman (1992) as a theoretical anchor and model for my analysis.

While very little law and society scholarship considers the intersection of law and organizations (Selznick, 1969 and Macaulay, 1963 are notable exceptions), the same can be said of public administration scholarship in terms of addressing the imbalances among administration, technology, law and policy, or the existence of policy vacuums (Edelman, 2003).

Studying processes for policy implementation from within organizations can help to

address problems that result from policy vacuums. Data breaches, in particular, are one indication that a policy vacuum may exist within an organization.

Further studies on the effects of the ambiguities of the law on the policy implementation process in conjunction with the internal factors that shape this process can lead to a better understanding of how policy vacuums are created and to assuage the unintended consequences. Such an approach would also lend itself to studies of policy implementation as a process of legitimation in organizations, in other words, how organizations translate ambiguous laws through their design of policy implementation processes that are intended to influence perceptions of the organization's behavior as credible and authentic. Edelman (1992), in particular, says that the quest for legitimacy is a primary motivation for structural elaboration and supports this claim by understanding how structures become a means of legitimation to promote good faith commitment to policy enactment but also for communicating that commitment within the organization (p. 1544). In this way, structure becomes a vehicle for creating organizational character, or culture, as a policy integration tool and goal (Khademian, 1996).

Edelman expands her claim that policy implementation is a process of legitimation in organizations by drawing upon her theory of legal environments to explain organizational response to general legal norms and extends that theory to address organizational response to direct legal mandates. Edelman claims:

> Law creates an 'illegal environment' that consists not only of the law and the sanctions that are built into it, but also of societal norms and culture associated with the law. Organizations that are sensitive to their legal environments develop forms of governance that conform to legal norms in order to achieve legitimacy. Over time, some organizations responses to the legal environment may diffuse among organizations and become institutionalized. Thus by influencing organizations' environments, law has an important indirect effect on

> organizational behavior that goes significantly beyond the direct effect of law and legal sanctions (1992, p. 1535).

Edelman concludes that "the conflict between EEO/AA law and managerial interests poses a dilemma to organizations: they must demonstrate compliance in order to maintain legitimacy and at the same time they must minimize the law's encroachment on managerial power" (1990 in 1992, p. 1535). Organizations' formal structures are more visible to the outside world than their internal structures. As a strategy for achieving legitimacy, organizations adapt their formal structures to conform to institutionalized norms; the structures are symbolic gestures to public opinion, the views of constituents, social norms, or law (Meyer & Rowan, 1977 as cited in Edelman, 1992).

Organizations seek to appear legitimate for a number of reasons: organizations that appear sensitive [to EEO/AA] law are less likely to provoke protest by protected classes of employees within the firm or community members who seek jobs, they are more likely to secure government resources, and they are less likely to trigger audits by regulatory agencies (Edelman, 1992). A review of the organizational legitimacy and its impact on implementation is outside of the scope of this study; however, the broader literature is acknowledged (Powell & DiMaggio, 1991 - organizational survival depends perceived legitimacy; Pfeffer & Salancik, 1978 - organizational legitimacy is controlled by those outside the organization, Suchman, 1995, 574;[66] Dowling & Pfeffer, 1975, in Patel & Xavier, 2005).[67] Patel and Xavier also note that "organizational legitimacy is a summative reflection of the relationship between an organization

[66] Suchman (1995) defines organizational legitimacy as the "generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within a social system" (p. 574). He argues that organizations can manage legitimacy through a number of strategies and outlined a series of phases to gain, maintain, and repair legitimacy within the three different types of pragmatic, moral and cognitive legitimacy.

[67] Patel and Xavier (2005) respond to a gap in the organizational legitimacy literature by seeking to understand the strategies that an organization uses to manage legitimacy over time. They define legitimacy, its phases and types, and exploring the strategies used by an organization to repair organizational legitimacy.

and its environment" and refer to Weber (1968) stressed the importance of legitimacy with his belief that legitimate order guided social action; Parsons (1960) argued that organizations that pursue goals in line with social values have a legitimate claim on resources; Dowling & Pfeffer (1975) continued this line of thought and argued that organizational legitimation efforts help explain organizational adjustment to the environment; Meyer & Rowan, 1977 as cited in Ruef & Scott, 1998, p. 878) were among the first to 'call attention to the ways in which organization seek legitimacy and support by incorporating structures and procedures that match widely accepted cultural models embodying common beliefs and knowledge systems' (2005, p. 2).

Therefore, although EEO/AA law does not specifically require it, organizations respond to the law by creating new offices, positions, rules, and procedures (which I will call EEO/AA structures) as visible symbols of their attention to EEO/AA issues and their efforts to comply (Edelman, 1992). Edelman contends that the "quest for legitimacy is a primary motivation for structural elaboration" (1992, p. 1544). Based on my findings, I contend that this quest for legitimacy can be learned through the policy implementation process and that certain combinations of variables, or characteristics of the implementation process, can lead to different policy approaches and outcomes. In a world where the law is grey and policy is continuously changing, we need a learning approach or one that strives for continuous improvement.

Edelman brings the public administration field one step closer to a deeper understanding and analysis of the process of policy implementation and what this means for public management. The import of distinguishing implementation efforts as substantive versus symbolic can drive future research into legitimizing the process of policy implementation. For example, in her research, Edelman characterizes implementation as being either "symbolic" or "commitment-oriented" (1992). Similarly, Chapter 7 of this study discusses conclusions about

each PIA implementation and draws generalizations about whether implementation represents a "check-box" or "baked-in" approach to policy implementation. In other words, the former presupposes that the implementation process has become part of the overall organizational culture and social norms of the organization, whereas, the checkbox approach designates a process that may be more expedient for an organization.

Furthermore, by analyzing the impact of a certain factors that influence the PIA process, assumptions can be made about whether or not the organization has taken a symbolic or commitment-oriented approach to policy implementation. In this study, I use the terminology "checkbox" versus "baked-in" (a.k.a., Privacy by Design) approach to describe the implementation process. For instance, Edelman (1992) points out that the creation of organizational structures, such as new offices, can be indicative of evidence of policy enactment. Such changes in structure can create the perception of action and attention to policy implementation, when in fact these changes may only be symbolic and done to advance the perception that the agency is responding to legal mandates. The mere creation of new structures to support policy implementation does not necessarily mean that agencies are actually committed to the process, but may only be "window-dressing."

Edelman's (1999) model of endogeneity says that *diffusion patterns* reflect a rationalization and institutionalization of symbolic structures of policy enactment. Over time, these structures come to be seen as evidence of policy enactment, even though nothing in the statutory language would suggest that organizations must (or even should) create them (Edelman & Petterson, 1999). Similar "diffusion patterns" stem from the PIA implementation process in the USPS and VA and provide insight into broader privacy policy management issues and policy outcomes. Other diffusion patterns become apparent in the way that both organizations are

structured to develop privacy directives and respond to the need to complete PIAs, to the quality of information that is contained in the PIAs, to the training that may be available to staff to enhance privacy awareness, or the creation of a cadre of professionals within each agency.

Broadly speaking, the PIA is a component of privacy policy and sensitivity to the process of implementing PIAs is amplified by such things as an organization's constituency, size, transparency, and mission. The nature of information use by organizations and the need for trust in the public eye makes organizations more or less sensitive to the law and to its implementation. In this research, the presence of data breaches rendered the VA even more sensitive to the legal environment and drove key changes throughout the organization. Edelman (1999) claims that endogeneity theory explains how law may produce significant social change in subtle, indirect and unexpected ways by altering conceptions of what constitutes good management and organizational fairness. In effect, organizational structures can become vehicles or obstacles for the transmission of legal principles into policy design and implementation processes.

CHAPTER SEVEN - CONCLUSIONS

Privacy policy is characterized by a dynamic and multifaceted nature that is subject to frequent rule changes that present significant challenges for public managers. The evolution of privacy policy implementation within organizations can be impacted by any number of external factors, such as public perception, changes in regulatory expectations, and changes in reporting requirements. The legal environment has also created new expectations by the public and has required federal agencies to not only adjust how they manage information but also how they govern it. The result has led to broad inconsistencies in both process design and implementation across organizations. These inconsistencies often stem from ambiguity in the legal mandates and a lack of guidance from the oversight authority which can create policy vacuums. Despite these challenges to implementation, organizations can learn in their approach to responding to uncertainties in the law. This study seeks to enrich our ability to understand privacy mandates in the context of PIA implementation. The analysis and findings are discussed in this chapter as a means to suggest key takeaways in terms of theoretical findings, real-world mapping, and future recommendations for practice. Table 11 outlines these key findings from the study.

Table 11. Research Findings

Theoretical	• Sociology of law literature informs field of public administration and can be used as a lens for understanding policy implementation as a process. • Edelman's research can help us to understand how policy is enacted and changes over time by focusing on implementation. • Inconsistences in implementation can be explained by a focus on process and certain characteristics that influence the process. • Policy implementation process itself can become a tool to enhance policy design and outcomes. • A learning approach to implementation is encouraged in a world where policy mandates are uncertain and changing.
Real-World Mapping	• PIA can be used as a management tool. • Integration and collaboration across multidisciplinary teams is integral component to achieving desired policy outcomes throughout the policy implementation process. • PrivacybyDesign principles (i.e., "baked-in" approach). • Current legislative environment supports stronger privacy policy (e.g.,

	Privacy Bill of Rights, FTC's Final Privacy Report). • Increasing incidents and threats of data breach are a policy imperative driving stronger privacy management. • Value of embedded experts to guide the organization through the implementation process. • PIA implementation process led to greater transparency in the IT infrastructure and management of information in both organizations. • What is the degree to which consultants are engaged by agencies for large-scale policy implementation?

Theoretical Findings

Edelman (1992) says that our understanding of the process by which organizations respond to law is very limited. Likewise, I contend that the field of public administration and policy is limited in its understanding of the implementation (Pressman & Wildavsky, 1973; Bardach, 1977; Mazmanian & Sabatier, 1983; deLeon & deLeon, 2002; Schofield & Sausman, 2004; O'Toole, 2004) process and more broadly, in understanding the nature and complexity of privacy policy in organizations. Theories developed by the sociology of law literature can inform the public administration and policy field, particularly in understanding how organizations enact policy and how inconsistencies in policy implementation can be explained by focusing on process.

Empirical research that analyzes the PIA implementation process in two large organizations has valuable import for understanding the evolution of the policy implementation process, critical factors that influence the process, and patterns that emerge over time. This leads to a richer understanding of how organizations change in tandem with the implementation process and how they manage and operate in a world where the law if often grey and the policy landscape continuously changes. These pressures on the organization force it to adapt and to recalibrate policy design to realize desired policy outcomes.

Not only do organizations respond by altering their approaches to implementation but they can also change in terms of their character. Because the implementation process is dynamic

and emergent, it can have unintended effects as supported by Clune's 1983 analysis of implementation and Burke's 1988 study of organizational response. The unintended effects of implementation can be studied by looking at some of the characteristics of the process and how they change over time. For instance, the social actors as well as their motivations may change over time. These changes can influence or be influenced by structural changes. Throughout this process of change, training becomes a vital tool that not only influences the quality of the implementation process but also can cultivate broader changes to organizational culture.

Clune (1983) also shows us that actual implementations tend to exhibit distinct trends or stages – that cycles or bundles of interactions at one stage become the prelude to a new type of interaction at the next stage. In other words, there is long-run development for implementations that allows for a development history that may be "evolutionary" in the sense that trial and error leads to improvement. In the case of the VA, I characterize the evolutionary development of the PIA implementation as a learning approach because it continually recalibrated its design to refine processes, to refine characteristics of the implementation, to increase the effectiveness of its policy design, and to reach a type of "dynamic equilibrium" (Clune, 1983, p. 75). In this way, implementation becomes recursive in Clune's (1983) sense because the process becomes circular and changes over time.

Edelman (1992) also adds to our understanding of implementation in the context of the PIA in studying how organizations conform to legal norms to achieve legitimacy – a particularly valuable insight for public administration. Implementation becomes not only a management challenge but also a governance challenge given the broad discretion that is passed on to administrative agencies. Bamberger and Mulligan (2008) call attention to the difficulty in forcing groups to include new priorities in their program goals that is discussed in a broad span

of decisionmaking in organizations literature. The requirement to implement the PIA across federal agencies was a new priority for agencies and therefore, disruptive to existing structures, expertise, and rules. This creates further internal challenges in terms of overcoming resistance to change in existing priorities in larger organizations (Bamberger & Mulligan, 2008).

The literature and empirical findings from this study show us that organizations can use certain tools for designing policy implementation such as training, professional expertise, and organizational structure. For instance, the USPS case study showed the critical value of having "embedded" expertise in the form of a Chief Privacy Officer (CPO). For Bamberger and Mulligan, an embedded expert establishes a "respected individual" from the privacy community and leads to legitimacy of the position and the establishment of a new policy direction as an organizational priority (2008, p. 97). Experts can also help to manage the state of ambiguity and guide the organization through a learning process as it finds its way in translating law into actionable policy and effective outcomes.

The PIA implementation process itself can become a tool – for raising the level of attention to privacy or the level of commitment within an organization, as an accountability mechanism, and as a tool for bringing greater transparency to IT development and information management within organizations (FISMA and GAO reports are analyzed to support this claim). Edelman (1992) brings the public administration field one step closer to a deeper understanding of the process of implementation by analyzing the tools of the process in order to characterize organizational approaches as "symbolic" or "commitment-oriented." In this research, the case studies can be analyzed to draw similar generalizations about whether an organization took a "check-box" or "baked-in" approach to policy implementation. In other words, the former presupposes that the implementation process has become part of the overall organizational

culture and social norms of the organization, whereas, the check-box approach designates more of what is deemed to be expedient for an organization.

Furthermore, by analyzing the impact of certain factors that influence the process of PIA implementation assumptions can be drawn about whether or not an organization has taken a symbolic or commitment-oriented approach to policy implementation. For instance, Edelman (1992) points out that the creation of organizational structures, such as new offices, can be indicative of policy enactment. While these changes in structure can create the perception of action and attention to policy implementation, these changes may only, in fact, be symbolic and done to advance the perception that the agency is responding to legal mandates. The mere creation of new structures to support policy implementation does not necessarily mean that agencies are actually committed to the process. These structures are, in effect, only "window-dressing."

The factors that influence the evolution of the policy implementation process also change over time both internally and externally to organizations. These factors can help to characterize an organization's approach or stance to policy implementation – in how it internalizes assigns meaning to the process. The trend toward a larger policy goal of information governance is an example of a policy outcome that goes beyond what is required by mandate, beyond compliance requirements and leading to more of a committed and value-driven approach versus a check-box approach. The trend toward an information governance orientation also indicates that the process of implementation has become more familiar to the organization, which in turn, can drive better policy design.

Policy implementation has a context and what sets privacy policy apart from other policies is that organizational practices and responses to privacy policy implementation are

characterized as *information governance* – a term that is growing in popularity across the privacy profession and across organizations both public and private. It's no longer information protection or information assurance but has evolved to something larger and more significant and central to the core competencies of any organization.

The patterns and trends that emerge from the implementation process run counter to Edelman's (1992) approach that is more heavily focused on the compliance posture of organizations. Edelman (1992) refers to law as creating an "illegal environment," but my findings suggest that implementation of complex legal mandates can lead organizations to grow, to innovate, and to learn in response to the law, treating the law as an opportunity versus a threat. The VA case study is indicative of this approach, turning the law into an opportunity for the organization to strive toward continuous improvement both in terms of policy outcomes but also in terms of its policy posture. In this sense, I mean that the implementation process became a transformative experience for the VA, empowering the agency to strive for excellence in information governance and privacy policy more broadly. Its implementation approach became one that was embedded with norms, not an approach that was strictly about conformance with legal norms as Edelman would frame it (1992, 1999, 2004).

While organizational response to legal mandates may initially be negative and compliance-focused, my study shows that law can be good and that organizations can learn and that process matters. Edelman (2004) contends that the law can indirectly influence organizational behavior, whereas I suggest that organizational behavior can influence the law and shape the future direction of policy.

Based on expansive document analysis and research, it can be concluded that the implementation of PIAs across the federal government has certainly been evolutionary and

unevenly implemented across agencies. However, a learning process has occurred over time from a legislative, regulatory, and organizational perspective. Over the years, Congress has enhanced the legislative mandate to incorporate better measures of privacy performance objectives intended under the E-Gov Act and the FISMA. The gradual incorporation of more privacy benchmarking versus an initial focus on security, has improved FISMA and the quality of reporting by agencies. From an organizational perspective, agencies have responded to changes in the legal mandates and reporting requirements to improve their stance on privacy policy and demonstrate enhanced implementation and positive outcomes (such as reduced breach events or better management of data collection and information flows).

When PIAs were first required under the E-Gov Act in 2002, they were an independent assessment, not tied to anything else in the law. This changed over the years, particularly as the PIA was tied to FISMA by the OMB. This marked a big change in the PIA requirement and implementation process. This change was likely influenced by the large number of breaches that were being seen across government organizations. The OMB tying the PIA to FISMA only showed that privacy was a much more visible issue that it was paying attention to and that it wanted the agencies to provide more substantial reporting.

The FISMA reports for the VA were very helpful in evaluating some of the downfalls of the VA's PIA process. A key element of success may have been the agency's recognition of the need to balance privacy and security, something that the USPS did from the very start of its implementation process. However, the USPS was driven by external pressures and congressional scrutiny to focus on compliance with privacy laws much earlier in the timeline of both agencies' PIA evolution. The USPS also had to balance its focus on privacy with a focus on security in light of the anthrax attacks in a post-9/11 environment. The USPS approach was

also largely characterized by delegating responsibility and leadership to a careerist with extensive privacy and legal expertise. The VA, on the other hand, was more narrowly focused on security in the early stages of the policy implementation process. This focus was largely attributable to the VA's challenge of a complete overhaul of its IT infrastructure driven by political appointees with primarily military and IT background. Training to support the VA implementation was scarce and contributed to a fragmented policy approach – one that perpetuated the ambiguity of the policy objectives and hindered an effective design. But training was also expensive as reflected the FISMA reports and discussed in Chapter 5. The prohibitive cost of training and lack of resources to support comprehensive training could have contributed to this fragmented policy approach.

However, the VA's fragmented approach evolved into one that was emergent and changing which can be understood within the context of mutual constitution. The notion of mutual constitution implies that social orders (structures, institutions, routines, etc.) cannot be conceived without understanding the role of agency in producing them, and similarly, agency cannot be understood 'simply' as human action, but rather must be understood as always already configured by social conditions. The ongoing nature of this constitutive relationship indicates that social regularities are always 'in the making,' that is, they are ongoing accomplishments (re) produced and possibly transformed in every instance of action (Gherardi, 2006; Reckwitz, 2002 as cited in Feldman & Orlikowski, forthcoming, p. 6). This is reflective of the VA in its approach to implementing PIAs; whereas, the USPS distinctively outlined what its structure would be to support policy implementation, the VA's approach was more emergent and changing. If a particular structure was not working, the VA changed and made adjustments. In my analysis of the USPS, it was hard to conclude that its process could be characterized as

emergent because of limited interview and process data. Its implementation was "full steam ahead" in the early years but its approach can be better understood by looking at some of the factors that motivated the USPS in its approach as well as environmental factors.

The USPS was a necessary agency to study in the context of PIA implementation not only because of its historical orientation towards privacy but also because the factors that influenced its approach were different from those of the VA. Historically, the VA has always had a commitment to protecting privacy in the U.S. mail system as a function of a democratic communications network. This point of distinction is important because this historical orientation towards privacy may help to explain why the USPS located its privacy management function in the Office of Consumer Affairs. Because the USPS is an independent agency that often operates as a business, marketing is a function of the agency that is not often seen in other government agencies. Placing the privacy function in consumer affairs helped to integrate the goals of broad messaging that the agency placed a high value on privacy and protecting both citizen and employee information but also the goal of achieving transparency in its operations in light of mounting fiscal pressures and changing markets.

The USPS "take charge" approach to implementation was also in response to need to modernize its technology infrastructure and support the movement towards e-commerce. The agency was criticized throughout the 1990s for its inability to effectively structure and manage its e-commerce products and services. Claims of having a weak management structure prompted a long-term transformation plan by the Postmaster General. A linchpin in this transformation plan involved putting in place a solid management structure that would allow it to categorize its e-commerce products and services and respond to compliance with applicable privacy laws.

The USPS's approach is largely based on an organizational model that has often by characterized as command and control and top-down. This may explain some of the reported initially resistance by other departments, such as IT and information security, to collaborate with consumer affairs on privacy policy implementation. Because the USPS was also facing competitive market pressures to develop new e-commerce and enhanced technological services, the BIA implementation and need for enhanced privacy controls, may have been met with resistance by product developers who were eager to bring new products to market and may have perceived privacy controls as a barrier to development.

In studying the evolution of the PIA implementation process in two agencies, organizational culture also emerged as a key element shaping the policy process. Some agencies may have a predisposed orientation towards privacy, in general. This was evident in the USPS case and derived from a historical orientation towards privacy in terms of protecting the mail. While the VA was also predisposed to a culture of privacy in protecting Veterans' personal information, from a policy perspective, this culture became more integrated as the law drove several different professional groups to work together to solve serious privacy challenges, such as data breach.

The USPS clearly shows the importance of assigning autonomy and authority to a privacy expert or the Chief Privacy Officer (CPO). When a CPO is given wide latitude to shape an organization's privacy policy agenda, then he or she can ensure a level of consistency throughout this uncertain and ambiguous process at both the policy and implementation levels. Clearly defined leadership can also shape organizational culture.

The beauty of the USPS case study began with the appointment of Zoe Strickland as CPO and taking this function out of the legal department. Keeping this function in the legal

department would have narrowed the focus of implementation to a compliance exercise, or a check-box approach. Housing the CPO in Consumer Affairs definitely established a privacy-centric approach versus a security-centric approach had the CPO been placed under the CIO or CISO leading to a policy design that could overlook the need for broad organizational training and awareness programs and preventative measures to protect against insider use of data. Privacy policy must be placed under a senior executive policy officer, one who subscribes to norms of information governance and data stewardship.

Strickland's role was reinforced by her vision and methodical approach to privacy implementation. She came into the position with a pre-established notion of what the policy implementation process should look like and was able to articulate that notion with consistent methods. Strickland's role is so vital to this study because her efforts substantiate the role of professional expertise in policy implementation. Good privacy policy and management is not possible without privacy professionals. In general, executive-level privacy professionals have been forward-looking and aimed at identifying solutions. They are able to accomplish positive policy outcomes and solutions through the establishment of firm organizational structures that build privacy principles in from the very beginning.

Despite the privacy officer's stature, autonomy, and strategic role in organizations, external events can complicate their management tasks; however, the interplay between professional expertise and organizational structure can result in a policy environment characterized by a continual process of learning. This environment of learning, if shaped by strong privacy leadership, can lead to the cultivation of an organizational culture that supports privacy policy and principles.

This study could also have implications for bridging the public administration field with that of knowledge management vis-à-vis the importance and relevance to expertise in records management as part of implementing privacy policy and an overall information governance strategy and program in organizations. It is vital that information and records management becomes incorporated into the overall operational and cultural fabric of an organization.

The establishment of a basic infrastructure of records management is the foundation to building effective privacy programs and effective implementation. Without a dedicated records management staff, proper training and clear policy directives, the agency increases its risk of mishandling their information and more importantly, sensitive personal information.

The Value of Integration in Policy Implementation

The policy process is not an exact science, it is an art form. The process of implementing policy requires the assembling of a type of orchestra that takes its cues from a conductor in order to harmonize and deliver a delightful experience for the audience. No one person or department can unilaterally implement broad sweeping policy stemming from ambiguous legal mandates. It requires exceptional skill, vision and coordination. How policy gets enacted can tell us a lot about an organization and if studied or monitored using certain factors that influence the process of policy implementation. These factors can be studied to understand how some may be adjusted to enhance or change the process at any time. Having a process that can be flexible and adaptive is important to realizing desired policy outcomes.

The need for integration in the policy implementation process is a critical factor that can lend itself to flexibility. The VA initially lacked integration of privacy efforts with IT security. This calls attention to the need for management to focus on how to approach integration challenges in the early stages of policy design. Integration is largely dependent on creating a

multidisciplinary approach to policy implementation. The USPS case study showed how the PIA is a powerful tool for integrating across the organization, for ensuring good data management practices, and protections, and in providing an added layer of protection for the citizen or customer.

In these case studies of PIA implementation, the integration process was advanced by re-designing the mandate and its reporting requirements to include privacy benchmarking as well as security. Agencies that did not integrate privacy and security from the beginning may have realized better policy outcomes had this been part of the original mandate. So, while it may be important for agencies to be able to recalibrate their policy design, the laws should also be recalibrated from time to time to enhance policy outcomes. Building strong benchmarking into policy mandates is important so that agencies have a barometer of their progress to help identify where the process may need improvements.

Leveraging technology to support a more efficient implementation process is also important and can lead to positive policy outcomes. The VA incorporated several technological innovations into its PIA implementation approach represented in the shift to an automated process and to creating a centralized database to aid with reporting. The centralized SMART database greatly enhanced the agency's ability integrate and automate its reporting requirements under FISMA and enhanced the evolution of the PIA process. The SMART database also represents a point of innovation for the VA that allowed it to improve its compliance and reporting processes. This enhanced capability also added a significant amount of accountability to the PIA process.

The USPS, on the other hand, is in the business of technology innovation to deliver mail services and privacy is always a consideration in building any new system or product. Experts

are able to incorporate knowledge of privacy-enhancing technologies early on in the design phase of any new product.

In recent years, the VA's approach to PIA implementation has morphed into a best practices and collaborative approach, collaborative both within the organization and across government. This kind of approach lends itself to learning and flexibility but also to transparency in its processes. Some of the VA's best practices have been the implementation of greater IT controls and enhanced training. The agency has set a course to balance transparency and collaboration with data protection and management leveraging its people, policy and process, technology, training, governance and oversight, and through technical enforcement (J. Buck, IAPP PowerPoint presentation, March 7, 2012).

One particular innovation that the VA has embraced is the use of SharePoint 2010 for secure collaboration and storage of sensitive data. SharePoint has allowed the VA to audit document libraries, sites, forums, and communities, to prevent data breaches, to comply with relevant privacy laws, and to enhance brand integrity. This best practice approach by the agency led the organization to conduct an assessment of overall enterprise content from electronic and paper documents, to email, to social collaboration, external and internal websites, and more. The VA discovered that eighty percent (80%) of its content is unstructured and growing at thirty-six percent (36%) a year. This finding led the agency to decide to make "control" part of its process and to better measure itself in terms of compliance to lead to better policy outcomes such as minimizing the risk of data loss or misuses or to minimize the impact of data loss or theft (J. Buck, IAPP PowerPoint presentation, March 7, 2012).

Real-World Mapping and PrivacybyDesign

The E-Gov Act is no exception to perpetuating the ambiguity of how federal agencies implement privacy policy through the PIA. For some agencies, this ambiguity is circumvented by a simple and straightforward approach to implementing PIAs in that the approach taken in akin to "checking a box" on a checklist. While other agencies take a "Privacy by Design" (PbD)[68] or a "baked-in" approach that is based on a model of implementation that continually evolves and strives for improvements and efficiencies over time to achieve policy goals. This approach can be described as "commitment-oriented" whereas the former can be characterized as more of a symbolic approach as described in Edelman's (1992) research.

The emergence of PbD has become an important facet of privacy policy implementation and is now internationally recognized by resolution at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem.[69] Anne Cavoukian, Ph.D. and Information & Privacy Commissioner, Ontario, Canada is credited with introducing this concept. This concept espouses that as new technologies enable the collection of greater amounts of data online, it is essential that companies consider privacy at each stage of product development. Because the PIA process is essentially a management tool assessing the privacy risk of existing and new IT systems, it should not require a huge leap to recognize the import of PbD principles into the PIA process as a means to ensure that privacy is considered from the beginning to the end of systems design and data collection methods and practices. As described by Cavoukian, "Privacy by Design asserts that the future of privacy cannot be assured solely by compliance

[68] As described by Anne Cavoukian, "'PrivacybyDesign' asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation"

[69] http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011---9--Privacy-by-design, Accessed on January 7, 2012.

with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."

The approach taken in this study to examine the PIA process by looking at the factors of training, professional expertise, and organizational structure shows how PbD can be operationalized in organizations and integrated into organizational culture adhering to Anne Cavoukian's claim that it is a "philosophy of embedding privacy proactively into technology itself."[70] This concept and its influence on PIA implementation and process is treated more fully in the analysis and conclusions in Chapter 5.

The PbD approach is significant to the findings of this study because the Obama Administration has embraced this approach as reflected in the Privacy Bill of Rights and in the Federal Trade Commission's (FTC) Final Privacy Report released in March 2012.[71] The FTC's Privacy Report marks a huge step forward in supporting the principles of PbD. But it is not only that PbD has influenced the current regulatory environment but that the environment is also changing and evolving as evidenced by the increasing attention to privacy almost on equal footing now with security protection. The evolution of the role of the FTC as a forum for shaping a collective understanding of privacy among advocates, industry, academics, and regulators is an important development. The FTC has expanded its scope by developing a cross-field understanding of privacy through workshops, fact-finding investigations, and other soft-law techniques to flesh out the meaning of an ambiguous privacy mandate. This evolution will be a factor to continue to monitor in terms of how external events and bodies can influence the privacy policy implementation process within organizations.

[70] http://privacybydesign.ca/about/, Accessed on January 7, 2012.
[71] U.S. Federal Trade Commission. (2012, March). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.* Retrieved from http://ftc.gov/os/2012/03/120326privacyreport.pdf.

The regulatory environment is also a hotbed of activity today with an increased focus on privacy, cybersecurity, and data breach. The recent HITECH Act ramped up data breach reporting and notification requirements for the healthcare industry and the banking regulatory agencies have their hands full with updating guidance for securing electronic transactions and the movement of money.

The Department of Commerce (DOC) is also playing a larger role in this unfolding environment, prompted by its 2012 white paper, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*. In this paper, the DOC has acknowledged that digital technology linked by the Internet has enabled large-scale collection, analysis, and storage of personal information. These tools enable service options and capabilities but also create risks to individual privacy. Therefore, the department has also embarked on an initiative to establish norms and ground rules for uses of information that allow for innovation and economic growth while respecting consumers' legitimate privacy interests. The white paper also influenced the creation of the Privacy Bill of Rights which sets out to establish baseline consumer privacy protections that are based on the Fair Information Practices but seek to expand upon those practices.

Future Research – In Other Areas

The possibilities for future research into privacy policy implementation are vast. Future research could expand upon this study and its focus on the PIA implementation by examining agencies based on the number of systems that each has to report on and analyze how the expanse of systems may pose management challenges. Furthermore, a comparative study of FISMA reporting over time for a group of agencies could be analyzed to understand each organization's

approach to training, professional expertise, and organizational structure and how these factors correlate to the FISMA reports.

Future research could also leverage the model I have developed in this study to study the impact of external groups on the policy implementation process and whether or not external groups are able to effect or influence the process in a positive or negative manner. These groups would include the use of consultants to aid in implementation efforts. Surprisingly, in an era characterized by an increased use of contracting out services, this element did not emerge in this study. Future research could examine the degree to which consultants are engaged for large-scale policy implementation or realignment efforts such as those driven by the e-government and IT modernization movement. Other groups that impact the implementation process include external groups. In the case of privacy policy implementation, it would be helpful to understand the influence of various advocacy groups such as the Electronic Privacy Information Center and the Center for Democracy and Technology, among others.

Wilson's construction of organization mission supports a sub-theme throughout these case studies. Future research could incorporate these dimensions into the study of policy implementation to show how agency culture defines agency mission, or vice versa. Another dynamic to policy implementation is the relevance of "situation." Wilson says that "situation" also matters or the situational mandates of the work being done. Privacy policy is subject to the nature of situational mandates but also situational external events such as data breach. In this case, data breach management as a component of privacy policy implementation would further enhance the fields understanding of the policy implementation process. For instance, the VA data breach had both negative and positive effects on the policy implementation process. One positive outcome could be seen in terms of how the data breach triggered the desire by the

agency to be viewed as having a legitimate privacy policy infrastructure - one that supports a larger public management goal of information governance across public organizations.

Finally, it would be interesting to see future studies on the process of implementation consider theories of technology and the scope for human agency, leveraging the work of Feldman & Orlikowski, forthcoming. This work could be used to better understand how humans adapt technologies to affect policy outcomes, to better understand how technology is viewed within organizations around a particular policy process, and how users recurrently enact technology structures or "technologies in practice" which is consequential for shaping of organizational outcomes (Feldman & Orlikowski, forthcoming).

This research can also be leveraged to inform other areas of compliance, such as diversity to show that as new mandates emerge and present new implementation challenges for organizations, the process can be understood by focusing on certain qualities of the process. These qualities can be used to develop an approach to policy design and implementation using them as goals, or treating them as malleable to improve process, decisionmaking, and outcomes.

I offer two suggestions to developing a typology. The first approach would select a group of agencies based on an agency's historical perspective on privacy and how this historical perspective applies to broader privacy policy implementation within the organization. Agencies could be analyzed not only by their historical predisposition to privacy issues but also by their sensitivity to privacy issues (e.g., high, medium, low or susceptibility to data breach). Second, a typology could be based on an agency's ability to integrate functions across the policy implementation process. Certain factors that influence the level of integration could include examining collaboration across departments, the creation of multidisciplinary teams, the role of technology in enhancing integration, or the role of leadership and expertise.

Recalibrating Policy Management for Achieving Success

The process of policy implementation alone, lends itself to one that allows organizations to come to understand an ambiguous and evolving legal environment. Insights into the process and lessons learned throughout, can shape stronger policy design. A better understanding of the process can help public managers *recalibrate* an existing process to adjust for errors – to be innovative throughout the process and become better at *policy architecting*.

This research has shown that although technology has made life simpler, it has also brought the notion of privacy to the forefront. Privacy in the contemporary context does not solely deal with an individual's relationship with government, but rather, privacy in contemporary terms encompasses an individual's relationship with government, with civil society, and their relationship to technology. Therefore, protecting privacy may mean more than development of new laws, it may entail developing new ways people think and deal with others. In a sense, the design of the policy approach can be a measure of an organization's fidelity to privacy expectations. These case studies show that this can be done from the inside out within organizations. Changing the mindset within the organization to mirror the intent of law can promote transference of policy values to society or outside of the organization.

Privacy policy will prove to be one of the biggest policy challenges to government in this century. The problem can be characterized using the analogy, "privacy is to the information age as the environment was to the industrial age" (Bamberger & Mulligan, 2011). Abusive environmental practices can be compared to abusive data collection and management practices. The resulting wasteland conjures up notions supported by popular science fiction alluding to Big Brother and a surveillance society. The potential to mismanage privacy policy is significant as technology advances faster than government can keep pace. A movement has emerged to truly

address the present day challenges of privacy policy and the need for ethical information governance.

Ethical information governance and privacy practices can aid public organizations in their quest for legitimacy and can be learned through the policy implementation process. In a world where the law is grey and ever-changing, we need a learning approach and one that strives for continuous improvement.

BIBLIOGRAPHY

Addison, H.J. (2009). Is administrative capacity a useful concept? Review of the application, meaning and observation of administrative capacity in political science literature. Research Paper. Retrieved on September 12, 2012 from http://personal.lse.ac.uk/addisonh/Papers/AC_Concept.pdf.

Bamberger, K.A. & Mulligan, D.K. (2008). *Privacy decisionmaking in administrative agencies. Chicago Law Review*, 75(1), 75-107.

Bamberger, K.A. & Mulligan, D.K. (2011). Privacy on the books and on the ground. *Stanford Law Review, 63*. (UC Berkeley Public Law Research Paper No. 1568385), 75(1), 75-107.

Bamberger, K.A. & Mulligan, D.K. (2011). New governance, chief privacy officers, and the corporate management of information privacy in the united states: an initial inquiry. *Law & Policy*, 33(4), 477-508.

Bardach, E. (1997). *The implementation game: What happens after a bill becomes law*, MIT Press, Cambridge.

Bennett, C.J. & Raab, C.D. (2003). *The governance of privacy: Instruments in global perspective*. Burlington.

Berry, J.M. (2002). Validity and reliability issues in elite interviewing. *PS: Political Science & Politics*, 35(4), 679-682.

Best, S.J., Krueger, B.S. & Ladewig, J. (2006). The polls-trends: Privacy in the information age. *Public Opinion Quarterly*, 70(3), 375-401.

Carter, V.E. & Goel, R. (2005). *Preparing for privacy: A module for marketing educators in an era of electronic commerce.* Proceedings of the Annual Meeting of the Association of Collegiate Marketing Educators. Retrieved on September 23, 2012 from http://www.sbaer.uca.edu/research/acme/2005/06.pdf.

Charles, K.K. (2000). Diversity: The demand for differential expert opinion. Working paper. Retrieved on July 22, 2012 from http://www.fordschool.umich.edu/research/papers/PDFfiles/00-013.pdf.

Chenoweth, J., Criddle, R., Jeffery, N. & Miller, S. (n.d.) *The United States Department of Veterans Affairs: Veterans Health Administration organizational analysis.* (Research paper). Pacific Lutheran University.

Clark, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, 25(2), 123-135.

Clune, W.H. (1983). A political model of implementation and implications of the model for public policy, research, and the changing roles of law and lawyers. *Iowa Law* Review, 69 (47), 86-95.

Crabtree, B. and Miller, W. (Eds.). (1992). *Doing Qualitative Research* (3rd ed.). Newbury Park: Sage Publications, Inc.

Creswell, J. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks: Sage Publications.

Dao, J. (2009, August 21). At V.A., scrutiny over abuses and $24 million in bonuses, *New York Times*. Retrieved on October 29, 2012 from http://www.nytimes.com/2009/08/22/us/22vets.html.

Denzin, N.K. and Lincoln, Y.S. (Eds.). (2005). *The SAGE Handbook of Qualitative Research* (3rd ed.). Thousand Oaks: Sage Publications.

Desai, A.C. (2007). Wiretapping before the wires: The post office and the birth of communications privacy. *Stanford Law Review*, 60(2), 553-594.

Doig, J.W., and Hargrove, E.C. (Eds.). (1987). *Leadership and innovation: Entrepreneurs in government*. Baltimore: John Hopkins University Press.

Dowling, J. B. & Pfeffer, J. (1975). Organizational legitimacy: Social values and organizational behavior. *Pacific Sociological Review, 18*(1), 122-136.

Dudley, L. and Raymer, M. (2001). Inside organizational change: puzzling across permeable boundaries. *Public Administration Review*, 61(5), 620–624.

Duff, W.M., Smieliauskas, W, & Yoos, H. (2001). Protecting privacy. *The Information Management Journal*, 35(2), 14 – 30.

Edelman, L.B. (1990). Legal environments and organizational governance: The expansion of due process in the American workplace. *American Journal of Sociology*, 95(6), 1401-40.

Edelman, L.B. (1992). Legal ambiguity and symbolic structures: Organizational mediation of civil rights law. *American Journal of Sociology*, 97(6), 1531-76.

Edelman, L.B. and Suchman, M.C. (1997). The legal environments of organizations. *Annual Review of Sociology*, 23, 479-515.

Edelman, L.B. and Petterson, S. (1999). Symbols and substance in organizational response to civil rights law. *Research in Social Stratification and Mobility* 17: 107-135.

Edelman, L.B., Uggen, C., and Erlanger, H.S. (1999). The endogeneity of legal regulation: Grievance procedures as rational myth. *American Journal of Sociology*, 105(2), 406-54.

Edelman, L.B., Fuller, S.R., & Mara-Drita, I. (2001). Diversity rhetoric and the managerialization of law. *American Journal of Sociology*, 106(6), 1589-1641.

Edelman, L.B. (2003). *Law at work: An institutional approach to civil rights*. (Working paper).

Edelman, L.B. (2004). Overlapping fields and constructed legalities: The endogeneity of law. To appear in *Bending the Bars of the Iron Cage: Institutional Dynamics and Processes*, edited by Walter P. Powell. University of Chicago Press.

Edelman, L.B. and Suchman, M.C. (2007). *Introduction to the legal lives of private organizations.* (The International Library of Essays in Law and Society). Burlington, VT: Ashgate Publishing Limited. Retrieved from http://web.mit.edu/~ssilbey/www/pdf/Silbey_I_fnl.pdf.

Edelman, L.B., Kreiger, L.H., Eliason, S., Albiston, C.R., & Mellema, V. (2008). (Working paper). When organizations rule: Judicial deference to institutionalized employment structures. Retrieved from http://www.stanford.edu/~mldauber/workshop/Edelman.pdf.

Elson, R.J. and LeClerc, R. (2006). Customer information: protecting the organization's most critical asset from misappropriation and identity theft. *Journal of Information Privacy and Security*, 2(1), 3 – 15.

Etzioni, A. (1999). *The Limits of Privacy*. Basic Books.

Federal Chief Information Officer's Council (2000). *Best practices: Privacy – Internal Revenue Service model information technology privacy impact assessment.* Washington, D.C. Retrieved from http://www.cio.gov.

Feldman, M.S. and Khademian, A. M. (2002). To manage is to govern. *Public Administration Review*, 62(5), 541-554.

Feldman, M.S. and Wanda J. Orlikowski. Forthcoming. Theorizing practice and practicing theory. *Organization Science,* Special Issue Perspectives on Organization Science: The First 20 Years. Retrieved on July 22, 2012 from http://socialecology.uci.edu/faculty/feldmanm/.

Fillichio, C.A. and Potter, J.E. (2006). A public servant who really drives. *Public Manager,* 35(3), 63-67.

Fixsen, D.L., Naoom, S.F., Blasé, K.A., Friedman, R.M., & Wallace, F. (2005). *Implementation research: A synthesis of the literature*. University of South Florida.

Goggin, M., et al. (1990). *Implementation theory and practice: Toward a third generation.* Scott, Foresman, Little, Brown, Glenview, Illinois.

Goodchild, J. (2008, December 1). CPO and CISO: A Comprehensive Approach to Information. *CSO Security and Risk*.

Hase, S. and Galt, J. (2011). Records management myopia: a case study. *Records Management Journal*, 21(1), 36-45.

Henkin, D.M. (2006). *The postal age: the emerging of modern communications in nineteenth-century America*. Chicago: University of Chicago Press.

Hoke, G. (2011, January). Records management evolves to information governance. *KMWorld*.

Huber, G.P. and Van de Ven, A.H. (1995). (Eds.) *Longitudinal field research methods: studying processes of organizational change*. Thousand Oaks, CA: Sage Publishers.

Hult, K.M. and Walcott, C.E. (1990). *Governing public organizations: Politics, structures, and institutional design*. Pacific Grove, CA: Brooks/Cole Publishing Co.

Information Security and Privacy Advisory Board. (2009). *Toward a 21st Century Framework for Federal Government Privacy Policy* (Report).

Ingram, H. and Schneider, A. (1990). Improving implementation through framing smarter statutes. *Journal of Public Policy.* 10(1): 67-88.

Kayworth, T., Brocato, L. and Whitten, D. (2005). What is a chief privacy officer? An analysis based on Mintzberg's taxonomy of managerial roles. *Communications of the Association for Information Systems*, 16, 1.

Khademian, A.M. (1992). *The SEC and capital market regulation*. Pittsburgh, PA: University of Pittsburgh Press.

Khademian, A.M. (1996). *Checking on the banks*. Washington, D.C.: Brookings Institution Press.

Khademian, A.M. (2002). *Working with culture: The way the job gets done in public programs*. Washington, D.C: CQ Press.

Kirk, J. and Miller, M. (1986). *Reliability and validity in qualitative research*. (Vol. 1). Newbury Park: Sage Publications.

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, 24(4), 691-710.

Lewis, D.E. (2008). *The politics of presidential appointments: Political control and bureaucratic performance*. Princeton, NJ: Princeton University Press.

Lipowicz, A. (2010, May 7). VA faces major hurdles to comply with FISMA, audit finds. *Federal Computer Week.* Retrieved on August 16, 2010 from https://fcw.com.

Lowi, T. (1979). *The end of liberalism*. New York: W. W. Norton & Company.

Manning, J., Mohan, M., Tatikonda, V. and Cochran, P.L. (2009). Radio frequency identification and privacy law: An integrative approach. *American Business Law Journal*, 46 (1).

Matland, R.E. (1995). Synthesizing the implementation literature: The ambiguity-conflict model of policy implementation. *Journal of Public Administration Research and Theory*, 5(2), 145-174. Retrieved on September 10, 2012 from http://links.jstor.org/sici?sici=1053-1858%28199504%295%3A2%3C145%3ASTILTA%3E2.0.CO%3B2-Z.

May, P.J. (2003, Eds.). Policy design and implementation. In *Handbook of Public Administration.* (Ed. B. G. Peters and J. Pierre). London: Sage Publications.

Mazmanian, D.A. and Sabatier, P.A. (1983). *Implementation and public policy*. Scott, Foresman, Glenview, Illinois.

Meyer, J.W. & Rowan, B. (1977). Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, 83, 340-63.

Mosher, F. (1982). *Democracy and the public service*. (2nd ed.). New York: Oxford University Press.

Mosquera, M. (2007, February 6). VA missing hard drive. *Government Computer News*. Retrieved on February 7, 2007 from http://www.gcn.com.

McElhatton, J. (2012, January 3). USPS memo highlights privacy violations. *The Washington Times.* Retrieved on October 29, 2012 from http://www.washingtontimes.com/news/2012/jan/3/usps-acts-to-avoid-customer-privacy-violations/?page=all.

Mulligan, D.K. & Perzanowski, A.K. (2007). Embedded RFID and everyday things: a case study of the security and privacy risks of the U.S. e-passport. *BerkeleyTechnology Law Journal*, 22, 1157.

Nelson, L. (2002). Protecting the common good: Technology, objectivity, and privacy. *Public Administration Review*, 62, Special Issue, 69-73.

Nelson, L. (2004). Privacy and technology: Reconsidering a crucial public policy debate in the post September 11 era. *Public Administration Review*, 64(3), 259-269.

Northouse, C. ed. Foreword by Barquin, R. and Fishkin, J. (2005). *Protecting what matters: Technology, security, and liberty since 9/11*. Brookings Institution Press and the Computer Ethics Institute.

O'Brien, D.M. (1979). Freedom on information, privacy, and information control: A contemporary administrative dilemma. *Public Administration Review*, 39(4), 323-328.

O'Sullivan, E. and Rassel, G.R. (1995). *Research methods for public administration*. (2 ed.). White Plains: Longman.

O'Toole, L.J. (2004). The theory-practice issue in policy implementation research. *Public Administration*, 82(2), 309-29.

Parsons, T. (1960). *Structure and process in modern societies*. Glencoe, IL: Free Press.

Patel, A. & Robina, X. (2005, July 4-7). *Legitimacy challenged: James Hardie Industries and the asbestos case.* Presented at The Annual Meeting of the Australian and New Zealand Communication Association. Christchurch, New Zealand.

Pfeffer, J. & Salancik, G. (1978). *The External Control of Organizations: A Resource Dependence Perspective*. New York: Harper and Row.

Pike, G.H. (2008). VA data breach and the Privacy Act. *Information Today.* Retrieved on November 11, 2010 from www.informationtoday.com.

Powell, W. & DiMaggio, P. (1991). *The new institutionalism in organizational analysis*. Chicago: University of Chicago Press.

Pressman, J. & Wildavsky, A. (1973). *Implementation: How great expectations in Washington are dashed in Oakland.* University of California Press, Berkeley.

Price, D.K. (1962). Administrative leadership. In S. Graubard & G. Holton (Eds.), *Excellence and leadership in a democracy* (pp. 171-184). New York: Columbia University Press.

Raths, D. (2011). Many federal agencies struggle with records management. *KMWorld,* 30-31.

Regan, P. (1995). *Legislating privacy: Technology, social values, and public policy.* University of North Carolina Press.

Regan, P. (1995). *Rethinking privacy: social values, technological change, and public policy*.

Robbins, S.P. & Judge, T.A. (2009) (Eds.) *Organizational behavior* (13th Ed.). Prentice Hall.

Ruef, M. & Scott, W. R. (1998). A multidimensional model of organizational legitimacy: Hospital survival in changing institutional environments. *Administrative Science Quarterly*, *43*(4), 877-904.

Schoenbrod, D. (1993). *Power without responsibility: How Congress abuses the people through delegation.* New Haven, CT: Yale University Press.

Schofield, J. & Sausman, C. (2004). Symposium on implementing public policy: Learning from theory and practice: introduction. *Public Administration*, 82(2), 235-48.

Scott, W. R., Ruef, M., Mendel, P. J. & Caronna, C. A. (2000). *Institutional change and healthcare organizations*. Chicago: The University of Chicago Press.

Simon, A. & Xenos, M. (2000). Media framing and effective public deliberation. *Political Communication, 17*, 363-376.

Selznick, P. (1957). *Leadership in administration: A sociological interpretation*. Evanston, IL: Row, Peterson.

Solove, D.J. (2008). *Understanding Privacy.* Boston, MA: Harvard University Press.

Stake, R. (1995). *The art of case study research*. Thousand Oaks: Sage Publications, Inc.

Steinberg, J.B., Graham, M. & Eggers, A. (2003, September). *Building intelligence to fight terrorism*. Brookings Institution. Retrieved from http://www.brookings.edu/comm/policybriefs/pb125.htm.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, CA: Sage Publications, Inc.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review, 20*(3), 571-610.

Tolbert, C.J. & Mossberger, K. (2006). The effects of e-government on trust and confidence in government, *Public Administration Review*, 66, 354-368.

The Ponemon Institute. (2007, February 15). *Privacy trust study of the United States government*.

U.S. Senate Subcommittee before The International Security, Proliferation & Federal Services Subcommittee of the Committee on Government Affairs. (2002). *The Postal Service in the 21st century: the USPS Transformation Plan.* 107th Cong., 2nd Sess. Washington, D.C.: Government Printing Office. Retrieved on October 29, 2012 from http://www.gpo.gov/fdsys/pkg/chrg-107shrg80598/html/chrg-107shrg80598.htm.

U.S. Federal Trade Commission. (2007, April). *Combating identity theft: A strategic plan.* U.S. Federal Trade Commission. A Report of the President's Identity Theft Task Force.

U.S. Federal Trade Commission. (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for businesses and policymakers.* Washington, D.C. Retrieved from http://ftc.gov/os/2012/03/120326privacyreport.pdf.

U.S. Department of Veterans Affairs. *VA history in brief.* (n.d.) Retrieved from http://www.va.gov/opa/publications/archives/docs/history_in_brief.pdf.

U.S. Department of Veterans Affairs. (2003). *VA Directive 6502 - Privacy Program.*

U.S. Department of Veterans Affairs. (2004, October 21). *VA Handbook 6502.2 - Privacy Impact Assessment.*

U.S. Department of Veterans Affairs Office of Inspector General. (2006, July 11). *Review of issues related to the loss of VA information involving the identity of millions of Veterans.*

U.S. Department of Veterans Affairs. (2007, September 18). *VA Handbook 6500- Information Security Program.*

U.S. Department of Veterans Affairs. (2008, April). *Eliminating the unnecessary collection and use of Social Security Numbers at the Department of Veterans Affairs*.

U.S. Department of Veterans Affairs. (2008, October 3). *VA Directive 6508-Privacy impact assessments.*

U.S. Department of Veterans Affairs. (2008, November 20). *VA Directive 6507- Reducing the use of Social Security Numbers.*

U.S. Department of Veterans Affairs. (2008). *FY 2008 E-Government Act Report.*

U.S. Department of Veterans Affairs. (2010). *2010 Organizational briefing book.* Retrieved from http://www.va.gov/ofcadmin/docs/vaorgbb.pdf.

U.S. Department of Veterans Affairs. (2011). *Strategic plan refresh FY 2011-2015.* Office of the Secretary. Washington, D.C. Retrieved on September 21, 2012 from http://www.va.gov/ofcadmin/docs/vaorgbb.pdf.

U.S. Government Accountability Office. (1996). *USPS improved oversight need to protect privacy of address changes*. Washington, D.C.: Government Printing Office.

U.S. Government Accountability Office. (2003, June). Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate. Privacy Act – *OMB leadership needed to improve agency compliance* (GAO-03-304).

U.S. Government Accountability Office. (2005, July). *Information security: Weaknesses persist at Federal agencies despite progress made in implementing related statutory requirements.* (GAO-05-552) Washington, D.C.

U.S. Government Accountability Office. (2008, May). *Privacy: Agencies should ensure that designated senior officials have oversight of key functions*. (GAO-08-603) Washington, D.C.

U.S. Government Accountability Office. (2008, June). *Privacy: Congress should consider alternatives for strengthening protection of personally identifiable information*. (GAO-08-795T). Washington, D.C.

U.S. Office of Management and Budget, Executive Office of the President. (2002). *OMB Circular No. A–11, Section 300. Part 7: Planning, Budgeting, Acquisition, and Management of Capital Assets.* Retrieved from http://www.whitehouse.gov/omb/e-gov/docs.

U.S. Office of Management and Budget, Executive Office of the President. (2003). *OMB guidance for implementing the privacy provisions of the E-Government Act of 2002.* (M-03-22). Washington, D.C.: Government Printing Office. Retrieved from http://www.whitehouse.gov/omb/memoranda_m03-22.

U.S. Office of Management and Budget. (2005). *FY 2005 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://m.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/reports/2005_fisma_report_to_congress.pdf.

U.S. Office of Management and Budget, Executive Office of the President. (2005). *Designation of Senior Agency Officials for Privacy* (M-05-08).

U.S. Office of Management and Budget, Executive Office of the President. (2006). *Safeguarding personally identifiable information*, (M-06-15).

U.S. Office of Management and Budget, Executive Office of the President. (2006). *Protection of sensitive agency information*. (M-06-16).

U.S. Office of Management and Budget, Executive Office of the President. (2006). *Reporting incidents involving personally identifiable information and incorporating the cost for security in agency information technology investments.* (M-06-19).

U.S. Office of Management and Budget, Executive Office of the President. (2007). *Safeguarding against and responding to the breach of personally identifiable information* (M-07-16).

U.S. Office of Management and Budget. (2007). *FY 2007 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://m.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/reports/2007_fisma_report.pdf.

U.S. Office of Management and Budget. (2008). *FY 2008 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/reports/fy2008_fisma.pdf.

U.S. Office of Management and Budget. (2009). *FY 2009 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.

U.S. Office of Management and Budget. (2010). *FY 2010 Report to Congress on implementation of the Federal Information Security management Act of 2002*. Retrieved fromhttp://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf.

U.S. Postal Service. (n.d.). *Handbook AS-805, Information security*. Retrieved on February 14, 2009 from http://about.usps.com/handbooks/as805/welcome.htm.

U.S. Postal Service. (2002). *2002 Transformation plan*. Retrieved from http://about.usps.com/strategic-planning/transform.htm.

U.S. Postal Service. (2005). *Handbook AS-353: Guide to privacy, the Freedom of Information Act, and records management*. Retrieved on February 14, 2009 from http://www.usps.com/cpim/ftp/hand/as353/welcome.htm.

Walters, J. (2009). Transforming information technology at the Department of Veterans Affairs. *Governing Magazine*. Retrieved on October 28, 2012 from http://www.isaca.org/Knowledge-Center/cobit/Documents/WaltersVAReport-June09.pdf.

Wasieleski, D.M. & Gal-Or, M. (2008). *Ethics and Information Technology*. An enquiry into the ethical efficacy of the use of radio frequency identification technology. Dordrecht, 10(1).

Waldo, D. (1968). Scope of the theory of public administration. *In Theory and practice of public administration: Scope, objectives, and methods*, edited by James C. Charlesworth, 1-26. Philadelphia: American Academy of Political and Social Science.

Weber, M. (1968). *Economy and society: An interpretive sociology*. New York: Bedminister Press.

Wilson, J.Q. 1989. *Bureaucracy.* Basic Books

Yin, R.K. (1994). *Case study research: Design and methods* (2nd ed.) Thousand Oaks: Sage Publications, Inc.

APPENDICES

APPENDIX A: Agency Interview Recruitment Emails

VA Recruitment Email
Subject: Virginia Tech PhD Dissertation regarding Privacy Impact Assessments

I am writing to request an interview with you to better understand the U.S. Veterans Administration's approach to managing privacy compliance and to developing privacy impact assessments. This interview will help to develop a better understanding of the relevance that the privacy impact assessment process plays as a method of compliance with U.S. privacy laws.

This research is being conducted to satisfy the requirements for completing my Ph.D. in Public Administration & Policy at Virginia Polytechnic Institute and State University (Virginia Tech). The scope of this research is intended to better understand the privacy impact assessment as both a policy tool and as a measure of privacy compliance.

Confidentiality Option
Your participation in this interview is important for gathering information to develop a better understanding of the privacy impact assessment process at the VA and other relevant privacy compliance practices. We will talk about the how the VA is structured to address privacy compliance and more specifically, discuss how and why privacy impact assessments are developed and implemented. You can choose whether or not your participation in this interview is confidential. If you choose to participate confidentially, the final report produced will not reflect your name or any personal identifying characteristics such as your name, position or title. Your personal identity will not be identifiable to anyone except the research team; as such, the researchers promise not to divulge that information. However, the VA, location, and details related to privacy compliance practices will be identified in the report.

Transcripts
Upon completion of the interview, I will transcribe the interview using a transcription service. Once the transcript has been prepared, it will be reviewed against the initial recording to ensure accuracy. The data from this study will be used to complete a dissertation study to fulfill the requirements for a Doctor of Philosophy in Public Administration & Policy at Virginia Polytechnic Institute & State University. The recording from this interview will be erased or destroyed in 2013.

Interview Length. Approximately 60-90 minutes. The interview may be conducted by phone or in person.

Voluntary Participation. You may choose not to participate at all, or you may refuse to answer certain questions or discontinue your participation at any time without penalty. There is no compensation for your participation in this study.

Questions or Comments? I have included below contact information for the office responsible for ensuring that this research is done fairly, respectfully and honestly. I encourage you to contact me directly if you have any questions or concerns about this project. Virginia Tech can also respond to any concerns about how information is being gathered, how it is being recorded and how it will be used.

I look forward to your participation.

Best regards,
Susan M. Pandy Ph.D Candidate Center for Public Administration and Policy Virginia Polytechnic Institute and State University 703-561-3953
spandy@nacha.org

Principal Investigator Virginia Tech Institutional Review Board Anne Meredith Khademian, Ph.D. Dr. David Moore, IRB Chair Center for Public Administration & Policy Virginia Polytechnic Institute and State University Virginia Polytechnic Institute and State University Research Compliance Office Alexandria, Virginia 1880 Pratt Dr., Ste. 2006 (0497) akhademi@vt.edu Blacksburg VA 24061
(703) 706-8119 Telephone: 540-231-4991

APPENDIX A: Agency Interview Recruitment Emails

USPS Recruitment Email
Subject: Virginia Tech PhD Dissertation regarding Privacy Impact Assessments

I am writing to request an interview with you to better understand the U.S. Postal Service's approach to managing privacy compliance and to developing privacy impact assessments. This interview will help to develop a better understanding of the relevance that the privacy impact assessment process plays as a method of compliance with U.S. privacy laws.

This research is being conducted to satisfy the requirements for completing my Ph.D. in Public Administration & Policy at Virginia Polytechnic Institute and State University (Virginia Tech). The scope of this research is intended to better understand the privacy impact assessment as both a policy tool and as a measure of privacy compliance.

Confidentiality Option
Your participation in this interview is important for gathering information to develop a better understanding of the privacy impact assessment process at the VA and other relevant privacy compliance practices. We will talk about the how the VA is structured to address privacy compliance and more specifically, discuss how and why privacy impact assessments are developed and implemented. You can choose whether or not your participation in this interview is confidential. If you choose to participate confidentially, the final report produced will not reflect your name or any personal identifying characteristics such as your name, position or title. Your personal identity will not be identifiable to anyone except the research team; as such, the researchers promise not to divulge that information. However, the VA, location, and details related to privacy compliance practices will be identified in the report.

Transcripts
Upon completion of the interview, I will transcribe the interview using a transcription service. Once the transcript has been prepared, it will be reviewed against the initial recording to ensure accuracy. The data from this study will be used to complete a dissertation study to fulfill the requirements for a Doctor of Philosophy in Public Administration & Policy at Virginia Polytechnic Institute & State University. The recording from this interview will be erased or destroyed in 2013.

Interview Length. Approximately 60-90 minutes. The interview may be conducted by phone or in person.

Voluntary Participation. You may choose not to participate at all, or you may refuse to answer certain questions or discontinue your participation at any time without penalty. There is no compensation for your participation in this study.

Questions or Comments? I have included below contact information for the office responsible for ensuring that this research is done fairly, respectfully and honestly. I encourage you to contact me directly if you have any questions or concerns about this project. Virginia Tech can also respond to any concerns about how information is being gathered, how it is being recorded and how it will be used.

I look forward to your participation.

Best regards,
Susan M. Pandy Ph.D Candidate Center for Public Administration and Policy Virginia Polytechnic Institute and State University 703-561-3953
spandy@nacha.org

Principal Investigator Virginia Tech Institutional Review Board Anne Meredith Khademian, Ph.D. Dr. David Moore, IRB Chair Center for Public Administration & Policy Virginia Polytechnic Institute and State University Virginia Polytechnic Institute and State University Research Compliance Office Alexandria, Virginia 1880 Pratt Dr., Ste. 2006 (0497) akhademi@vt.edu Blacksburg VA 24061
(703) 706-8119 Telephone: 540-231-4991

APPENDIX B: List of Interviewees

U.S. Department of Veterans Affairs

Privacy Officer, Office of Information & Technology (Request to remain anonymous)

John Buck, Acting ADAS, Office of Privacy and Records Management

Hal Corbin, Acting Deputy Director of Information Technology, U.S. Department of Veterans Affairs

Stephania Griffin, Privacy Officer, Director Information Access and Privacy, U.S. Veterans Health Administration

Dennis Stewart, Director, Privacy Service, U.S. Department of Veterans Affairs

Sally Wallace, ADAS Privacy and Records Management (Retired). U.S. Department of Veterans Affairs

U.S. Postal Service

Deborah Kendall (Retired). Former Manager, Strategy and Processes, Consumer Affairs, U.S. Postal Service

Supplemental Interviews

Zoe Strickland (Retired). Former Chief Privacy Officer, U.S. Postal Service