NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RINGING THE BELL; SOUNDING THE ALARM: A PROPOSAL FOR THE SIMULTANEOUS ADVANCEMENT OF SECURITY AND PRIVACY

by

Kneilan K. Novak

March 2006

Thesis Advisor:	Robert Bach
Second Reader:	Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Ringing the Bell; Sounding the Alarm: A Proposal for the Simultaneous Advancement of Security and Privacy			**5. FUNDING NUMBERS**
6. AUTHOR(S) Capt Kneilan K. Novak, USAF			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited)			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The need for domestic intelligence and information sharing to detect indications and warnings of terrorist acts and prevent them has raised privacy and civil liberties concerns. The relationship between national security and privacy and civil liberties is often modeled as a scale with security on one end and privacy and civil liberties on the other. Success is said to be achieved when security and privacy are balanced. This model forces these values to be traded in a zero-sum game.

A new model that decreases the "cost" to privacy and increases the "value" to security is needed. Technological, policy and organizational innovation hold promise in designing new intelligence and information-sharing architectures capable of detecting indications and warnings of terrorism *and* protecting the privacy and civil liberties of Americans.

Using government documents that articulate attributes for a terrorism early warning system and widely accepted privacy principles as design requirements, the thesis examines technologies that could meet the challenges of both security and privacy. Designing and building a system that supports both security and privacy will benefit both. The thesis argues, this system will enable the Nation to fight terrorism while upholding the liberties that form the core values of the American people.

14. SUBJECT TERMS Intelligence, Information Sharing, Terrorism, Counterterrorism, Homeland Security, Homeland Defense, Privacy, Civil Liberties			**15. NUMBER OF PAGES** 103
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RINGING THE BELL; SOUNDING THE ALARM: A PROPOSAL FOR THE SIMULTANEOUS ADVANCEMENT OF SECURITY AND PRIVACY

Kneilan K. Novak
Captain, United States Air Force
B.S., Colorado State University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2006**

Author: Kneilan K. Novak

Approved by: Dr. Robert Bach
Thesis Advisor

Robert L. Simeral, CAPT, USN (Ret)
Second Reader

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The need for improved domestic intelligence and information sharing to detect indications and warnings of terrorist acts and prevent them has raised concerns over privacy and civil liberties. The relationship between national security and privacy and civil liberties is often modeled as a scale with security on one end and privacy and civil liberties on the other. Success is said to be achieved when security and privacy are balanced. This model forces one value to be traded for the other in a zero-sum game.

A new model is needed, one that decreases the "cost" to Americans' privacy and increases the "value" to national security. Technological, policy and organizational innovation hold great promise in designing a new intelligence and information-sharing architecture capable of detecting indications and warnings of terrorism and, at the same time protecting the privacy and civil liberties of Americans. The system must be designed with both ends of the continuum in mind.

Using government documents that articulate desirable attributes for a terrorism early warning system and widely accepted privacy principles as requirements to design to, the thesis examines current or near-term technologies that could meet the challenges of both security and privacy. Designing and building a system that supports both security and privacy will benefit both. Ultimately, the thesis argues, this system will enable the Nation to fight terrorism effectively while upholding the liberties that form the core values of the American people.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am grateful to a number of organizations and individuals for their role in my ability to participate in this program and complete this thesis. I stated in my application to the program that one of my primary motivations in applying was to form relationships and a network to respond to the challenges posed by terrorism. I count my classmates as more than a network, I count them as friends. Your communities are blessed to have you as their leaders and I am blessed to have you as part of my life.

I would like to extend deepest thanks to the men and women of the NORAD Policy and Plans directorate whose encouragement during the last eighteen months has helped sustain me. I would particularly like to thank Colonel Dave Blehm and Lieutenant Colonel Dan Fox for their support and for allowing me fourteen weeks in Monterey to "swim with the dolphins."

I am extremely grateful to the Center for Homeland Defense and Security staff and professors. My experience in this program has been first rate despite the fact I was forced to do "real work" to earn this degree. Special thanks should go to my thesis advisor Dr. Bob Bach and CAPT Simeral for their guidance and assistance in completing this project. You have proven yourselves not only as excellent thinkers, but also as great servants to our Nation.

Lastly, I want to express my deepest love and appreciation to my wife, Jodi, who deserves numerous medals for skipped date nights, below average number of ski days for two consecutive ski seasons and for not hurting me for typing when I should have been listening. Your faith, hope and strength in battling brain cancer inspire me to bring those qualities to battling terrorism. I treasure you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: SOUNDING THE ALARM; RINGING THE BELL

On April 18, 1775, at about 11 O'clock in the evening, Paul Revere crossed the Charles River to begin his famous ride toward Lexington and Concord.[1] In Boston 650 to 900 British troops were preparing to cross the Charles River themselves to carry out General Thomas Gage's order to destroy the American militia's stores of weapons at Concord. Revere's "sounding the alarm" enabled the American militia to be prepared for the British attack. When the British arrived at Concord North Bridge, the Americans were waiting for them and the "Shot Heard Round the World" touched off the American Revolution and eventually led America to liberty.[2]

Revere and his fellow riders, William Dawes and Samuel Prescott, could be considered America's first "early warning system." Early warning systems have changed throughout the years ranging from the low tech system of Revere and his fellow riders to a network of radars and satellites designed to warn us of a Soviet missile launch during the Cold War. Yet, their importance has remained a constant. National security demands that the United States not be surprised by an undetected attack. Pearl Harbor and the September 11, 2001 attacks (9/11) reveal the necessity for an effective early warning system to "sound the alarm."

The day after Revere's famous ride, a bell rang out in Philadelphia in honor of the battles being waged at Lexington and Concord. This bell, since its installation in 1753, had been rung on numerous significant occasions. It was rung when Benjamin Franklin traveled to England to discuss the America's grievances against the British. It was rung for the assembling of the first Continental Congress. It was rung to call people together to discuss the Sugar Act and the Stamp Act. Now the bell was rung at the beginning of

---

1 The Paul Revere House, "The Real Story of Paul Revere's Ride," http://www.paulreverehouse.org/ride/real.shtml (accessed December 15, 2005)

2 Worcester Polytechnic Institute Department of Military Science, http://www.wpi.edu/Academics/Depts/MilSci/BTSI/Lexcon (accessed December 15, 2005)

what would become America's war for independence. This cracked bell would later be dubbed the Liberty Bell.[3] The ringing of bells came to mean both impending danger and celebration of freedom.

The dual meaning of bell ringing is especially relevant today. America suffered a surprise attack on 9/11. The warning bells were silent. A system capable of perceiving indications and warnings of terrorism was non-existent. Four years later the government is still struggling to put together an early warning system that can detect indications of an impending terrorist attack and enable a response to prevent it. In these efforts, the Government has also not been able to proclaim a celebration or protection of freedom and liberty. Early initiatives to construct an early warning system have touched off deep concerns over potential infringement on privacy and civil liberties.

Concerns over privacy and impacts to liberty have blocked several attempts to develop systems designed to provide indications and warning of terrorism. A few examples include the Terrorism Information Awareness (TIA) program, Computer Assisted Passenger Prescreening (CAPPS II) and Terrorism Information and Preventive Systems (TIPS). Privacy advocates such as the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) celebrate the de-funding and blockage of these programs as victories for privacy and critical to upholding liberty. The only problem is that the victory has come at the expense of "early warning." As a result, government continues to declare its need for better surveillance and information sharing, and for the capability to engage in data mining.

This thesis examines ways in which obtaining security and safety from terrorism may be achieved while maintaining essential liberty. It was a critical question for our founding fathers, and remains so today. Benjamin Franklin once challenged the Nation: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[4] Must our counterterrorism activities today be overly intrusive to Americans' privacy and way of life? Must security come at the price of liberty? Is it

---

[3] Independence Hall Association, "The Liberty Bell," http://www.ushistory.org/libertybell/ (accessed December 15, 2005).

[4] Benjamin Franklin, *Historical Review of Pennsylvania, 1759*, as quoted in Robert Bach, "Special Topics in Homeland Security" (lecture, Naval Postgraduate School, Monterey, CA, July 14, 2005).

even possible today to develop a strategy to "sound the alarm" to avoid being surprised by terrorism again while continuing to ring the bell of freedom?

A. MORE THAN CONNECTING DOTS

The 9/11 Commission Report showed that much of the information necessary to avert the terrorist attacks on the World Trade Center and Pentagon was available, but the intelligence community (IC) and law enforcement failed to "connect the dots." Additionally, certain "dots" were not available to the IC because of a prohibition on using certain collection methods within the borders of the United States. Clearly, excellent intelligence is necessary to prevent another terrorist attack in the United States. What is less clear is the policy that should govern domestic intelligence collection and the new imperative for vastly improved "information sharing" within the IC and agencies with responsibilities in homeland defense and security.

An improved domestic intelligence capability and greater information sharing have many people legitimately concerned about the impact to privacy and civil liberties. The 9/11 Commission recognized the impact improved domestic intelligence and information sharing would likely have on privacy and civil liberties and pointed out government's responsibility toward both security and civil liberty. "Therefore, while protecting our homeland, Americans should be mindful of threats to vital personal and civil liberties. This balancing act is no easy task, but we must constantly strive to keep it right."[5]

While the commission should be lauded for recognizing the importance of both values, the language they chose is problematic. The problem with framing the debate with the metaphor of a scale with security on one end and privacy and civil liberties on the other is that it promotes the idea that one must come at the cost of the other. Rather than view the problem as a balancing act between security and liberty, an effective policy should simultaneously advance both. As the Gilmore Commission put it, "Rather than

5 National Commission on Terrorist Attacks Upon the United States, Thomas H. Kean and Lee H. Hamilton eds, *The 9/11 Commission Report* (Washington, D.C.: WW Norton & Co., 2004), 394.

the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, these values should be recognized as mutually reinforcing."[6]

This difference in language, while subtle, is more than just semantics. Embracing the idea that security and privacy are complementary values rather than competitive can significantly reorient the thinking of the architects of a terrorism early warning system. Americans, their policymakers and innovators must recognize that both virtues are equally noble and vital to America's continued freedom and prosperity. They should demand that their terrorism early warning system cause both national security and privacy and civil liberties protection to increase, not be traded one for the other.

The *Gilmore Commission* correctly observed, "The exercise of civil liberties and our way of life contributes to our strength and security."[7] Operating from this frame of mind, the United States can develop the innovations in policy, technology and organizational structures necessary to simultaneously advance the ability to collect and share information vital to prevent a terrorist attack and protect the constitutional and privacy rights of Americans.

B. TECHNOLOGY AND THE ZERO-SUM FALLACY

The balance metaphor is dangerous in the current national security context because it assumes that security and privacy are pitted against each other in a zero-sum game, assuming that an advance of one comes at the expense of the other. The zero-sum equation fueled, in large part, the construct which came out of the Church Commission. In an attempt to curb abuse and tip the scales back toward privacy and civil liberties, domestic intelligence powers were severely limited.

During the Cold War, since the enemy was largely overseas, this limitation did not significantly impact national security. However, the threat of transnational terrorism, including terrorist cells inside the homeland, drives the need for improved domestic intelligence.

---

[6] The Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, "Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty," December 15, 2003, E-1.

[7] Ibid, E-2.

In a zero-sum construct, an improvement in homeland security comes at the cost of privacy and liberty. There must be a better metaphor and better way to achieve homeland security.

An underlying assumption in the zero-sum fallacy is that the only tools available to protect the people from domestic intelligence abuse are laws and policy. This view may have been true in the 1970s when most intelligence existed on paper and was stored in manila file folders in someone's desk, but it is unnecessarily narrow in the information age. There are many more tools that can be used to curb government abuse of information. The use of policy and law is one means, technology is another. The combination of technology and policy, or a policy enforced through technological means has the potential to change the calculus from a zero-sum game to an equation that allows gains to both security and privacy.

It is significant to note that in its efforts to improve information sharing and develop a terrorism early warning system, the government is primarily pursuing electronic means. Connecting counterterrorism agencies, analysts and operators and the information they hold electronically, in an online environment, carries implications that would not be present if they were connected via other means. One important implication is that it allows software to be used as a means to regulate behavior.

It has been said that in an online environment, "code is law."[8] Implementing software as a means to regulate and constrain the interaction and behavior of domestic and foreign intelligence analysts and operators could effectively turn "the wall" between the law enforcement and foreign intelligence domains into a "gate" which permits certain information to be shared while limiting that which is inappropriate. An example of controlling behavior through software from the commercial world might clarify this point.

Apple's I-tunes software enables people on a network to share music files (digital information). One simply has to check boxes that say "look for shared music" or "share

[8] This phrase was popularized by Stanford Professor Lawrence Lessig's book, *Code and Other Laws of Cyberspace*, which is currently being updated using a wiki to account for the numerous technological innovations that have occurred since its writing in 1999. For information regarding the updated version see: http://codebook.jot.com/WikiHome (accessed December 15, 2005)

my music" and he can either listen to a co-worker's music or enable his co-workers to listen to his over a network connection. Sharing music over a network is not contrary to anti-piracy laws. What is contrary to anti-piracy laws is the "unauthorized copying" of music. Rather than rely on law and a person's moral character to prevent the "unauthorized copying" of shared music, I-tunes wrote the software to make it impossible to copy a music file that is being shared on a network.

This "policy plus technology" construct for preventing the unauthorized copying of shared music has some interesting parallels that are relevant to sharing information for national security.

First, the I-tunes construct enables "knowledge discovery" but at the same time limits the "discoverer's" ability to abuse (by making an illegal copy) his access to the information. For example, Jim may be a fan of country music and accustomed to only buying country music. On his own accord he would likely not be interested in alternative music, let alone a band called "The Dead Milkmen." Suppose one day he is listening to his co-worker, Sue's, shared music and "discovers" that he really likes a song called "Punk Rock Girl." In a moment of weakness he may attempt to disregard the law and illegally copy "Punk Rock Girl." To his dismay, I-tunes software thwarts any attempt to copy the song. Finally, Jim decides that having "Punk Rock Girl" for himself is critical to his continued happiness, so he goes to the I-tunes store and pays the ninety-nine cents to purchase the song legally. Apple declares victory because it has figured out a way to expand Jim's musical interest, has thwarted illegal copying and has benefited from the revenue produced by Jim purchasing the newly discovered music.

This example, while seemingly trivial in comparison to national security and Constitutional freedoms, shows how sharing information over a network can lead to increased knowledge discovery and at the same time limit the person making the discovery to a course of action consistent with policy. The fictitious Jim could just as easily be a DoD intelligence analyst searching for information within a Terrorism Information Sharing Environment. Technology could force the information to be shared in a way that preserves a USPERSON's privacy (i.e. comply with Executive Order 12333 and DoD 5240.1-R) and yet enable collaboration between foreign and domestic

intelligence analysts. Their collaboration may enable the establishment of a terrorism nexus and open the door to legally investigate the USPERSON with increased scrutiny. This collaboration may not be possible in an information sharing environment that, in order to protect privacy, severely restricts the flow of information between domestic and foreign analysts.

C. THE NEED TO INNOVATE

The apparent clash between security and privacy is clearly a difficult problem requiring new and creative solutions. Yet, that dilemma is an old, familiar one. Plato said "necessity is the mother of invention."[9] Abraham Lincoln said, "The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew."[10] Both men understood that when an existing paradigm is inadequate to deal with a new problem, new paradigms must be invented.

"Innovation" has become a buzzword in today's business world out of necessity. Business leaders in the information age understand that they must continuously "think anew and act anew" in order to maintain their market share in an increasingly competitive and global business environment. Innovation is critical to the survival of many businesses. Innovation is also critically important to national security. Connecting dots or moving from a "need to know" to a "need to share" culture is a challenging problem. Doing it in a way that protects personal privacy and individual liberties is an even greater challenge—one that invites solutions from leading thinkers in technology, policy and organizational theory.

The national security climate the United States currently faces demands a full-scale assault on paradigms that continue to treat security and privacy as a zero-sum game.

---

9 Plato, *Republic*, as quoted in *The New Dictionary of Cultural Literacy*, 3rd ed., ed. E.D. Hirsch, Jr., Joseph F. Kett, and James Trefil (New York: Houghton Mifflin, 2002). Accessed at http://www.bartleby.com/59/3/necessityist.html (accessed December 15, 2005).

10 *Brainy Quote*, http://www.brainyquote.com/quotes/quotes/a/abrahamlin121071.html (accessed December 15, 2005).

Innovators from numerous disciplines must engage to change the calculus of both security and privacy. Such innovation will require novel forms of cooperation between those tasked with defending and securing America from terrorism and ardent privacy advocates.

The international best-selling business book *Blue Ocean Strategy*, suggests that the key to business growth lies not in competing for market share (in bloody "red oceans"), but by creating uncontested market space or "blue oceans." The authors of *Blue Ocean Strategy* found that what often separates winning companies apart is not a focus on beating the competition, but rather on creating a "leap in value" for the company and its customers. This is what the authors call "value innovation."

Conventional logic suggests that a company can either offer increased value to the customer at a higher cost or offer a product of reasonable value at a lower cost. Value innovation breaks this logic by offering a product that an industry has never offered before at a cost the customer believes to be reasonable. Value innovation is "the region where a company's actions favorably affect both its cost structure and its value proposition to buyers."[11] Value innovation does not focus on achieving an optimal balancing point between cost and value to undercut the competition, it focuses on creating a "never-offered-before," more desirable product at an appealing price. In doing so, it breaks away from the zero-sum constraint between cost and value imposed by industry competition.

This idea from business can be borrowed and applied to creating a terrorism early warning system. Rather than designing a system based solely on the design constraints intended to improve security and trying to use the system in a way that does not offend freedom, government should design a system that looks for opportunities where security and privacy attributes are complimentary rather than competitive. "Value innovation" in this context would seek the development of a system which simultaneously increases the ability for networked agencies to share information and solve intelligence problems (thereby improving the "value" of intelligence to the American people) and reducing the cost to privacy and civil liberties to a pre-determined, acceptable price. Just as a "value

[11] W. Chan Kim and Renee Mauborgne, *Blue Ocean Strategy* (Boston: Harvard Business School Press, 2005), 12-16.

innovation" in business attracts new customers and makes competition irrelevant, building a system that considers both security and privacy attributes in its design has the potential to win broad support from both those concerned about security and those concerned about privacy.

Figure 1 graphically represents the intent to design a system which drives down the "cost" to privacy while increasing the "value" to national security. This is not a balancing or competitive relationship. It is a symbiotic, mutually reinforcing relationship. The "value innovation" region is intended to depict the region where the impact to both privacy and security is favorable.

In business, successfully defining this region likely means that both seller and buyer walk away pleased, each feeling as if they have gotten a good deal. In the context of our problem, those tasked with protecting America from terrorists attacks and privacy advocates should both feel as if they are "getting a good deal." Ultimately, of course, this system is for the American people and its existence should make the American people more secure and free, not ask them to choose between values.

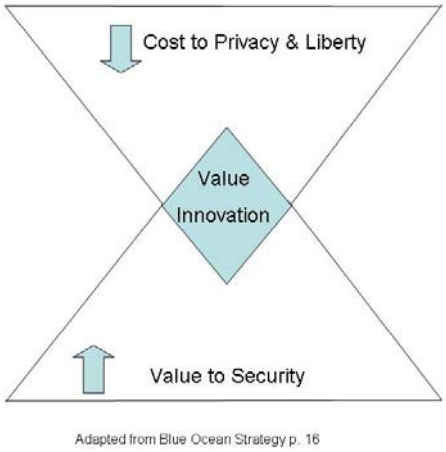

Figure 1. The goal to simultaneously pursue increased Security *and* Privacy should guide the development of a terrorism early warning system.
(From: Kim and Mauborgne, *Blue Ocean Strategy*, 16.)

The authors of *Blue Ocean Strategy* developed several analytical tools to help make the pursuit of blue oceans as actionable as competing within red oceans. One of these analytical tools, the "four actions framework" lends itself particularly well to a discussion on the relationship between security and privacy.

The four actions framework is intended to break the trade-off between market differentiation and low cost. It can be readily adapted to our effort to break the trade-off between security and privacy. In working to establish a blue ocean in business, the four actions framework asks four key questions:

- Which factors the industry takes for granted should be eliminated?
- Which factors should be reduced well below the industry's standard?
- Which factors should be raised well above the industry's standard?
- Which factors should be created that the industry has never offered?[12]

Applying these questions to our problem involves looking at the current situation in which privacy and improved domestic intelligence and information sharing are viewed as competitors then asking which factors need to be eliminated, reduced, raised or created. Figure 2 attempts to provide an answer to these questions and show how these answers might lead to the view that privacy and security can be mutually reinforcing rather than competitive.

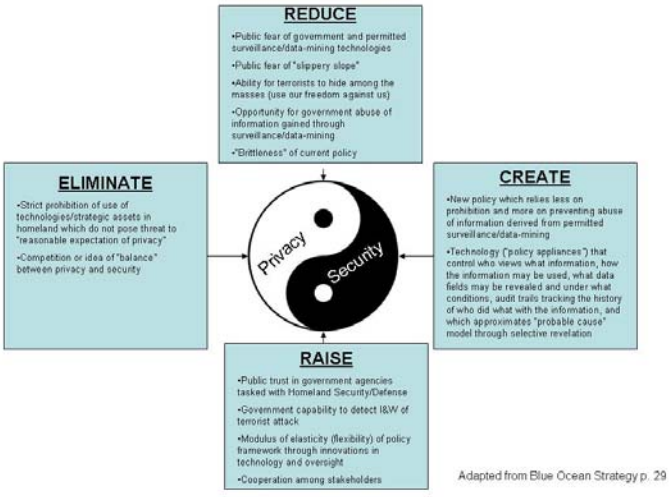

Figure 2. Factors that must be reduced, eliminated, raised or created in pursuing a system which simultaneously pursues both values of privacy and security. (From: Kim and Mauborgne, *Blue Ocean Strategy*, 29.)

12 Kim and Mauborgne, *Blue Ocean Strategy*, 29.

D. METHODOLOGY: DEVELOPING A PRIVACY AND SECURITY MATRIX

With the goal to develop a system which simultaneously increases the government's ability to perceive indications and warnings of a terrorist attack and protect Americans' privacy and civil liberties, it is important to discern and develop the attributes necessary to succeed at both. These privacy and security attributes can then collectively form the requirements which can be used to design a system. The effectiveness of the system can be measured against how well it meets both the privacy and security requirements.

Using the best available literature for both privacy and security, a matrix can be developed to guide the design and development of the system. Innovations can then be compared to the matrix to identify which attributes a particular innovation fulfills.

Figure 3 shows attributes which have been pulled from the literature and serve as a roadmap for the remainder of the thesis. The left hand side of the matrix is concerned with those attributes, as identified in various government documents, necessary to significantly improve information sharing and to perceive indications and warnings of terrorism. The right hand side of the matrix is concerned with those attributes necessary to protect privacy.

	SECURITY / INFORMATION SHARING					PRIVACY	
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356	FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies	Notice/Awareness	Data Quality
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC	Choice/Consent	Purpose Specification
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination	Access/Participation	Use Limitation
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards	Security/Data Integrity	Collection Limitation
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information	Enforcement	Security Safeguards
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods		Openness
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security	Match data access to roles and responsibilities of oranizations engaged in countering terrorism	Produce multiple versions (security classifications) of information		Individual Participation
			Facilitate oversight through use of audit trails, user authentication and access controls				Accountability

Figure 3. A Privacy and Security Reference Matrix

This matrix forms the foundation from which the rest of the thesis will flow. The next two chapters show the origins of these attributes and elucidate on their meaning. With these chapters as a backdrop, attention can then be turned to some current or near-term technological innovations that can fulfill attributes on both sides of the matrix.

II. MEETING THE NEEDS OF HOMELAND OPERATORS AND ANALYSTS

"In this war, we don't have radar, we have intelligence." Department of Homeland Security Secretary, Michael Chertoff made this statement while defending the use of National Security Agency (NSA) assets to listen in on the telephone conversations of suspected terrorists. "The total set of tools we have, whether it is the NSA monitoring programs, whether it is the Patriot Act, these tools are critical tools in defending this country against terror."[13]

Times used to be simpler. During the Cold War, when the nation was worried about the Soviets flying "Bear" Bombers into our airspace or launching nuclear missiles, we had a system of radars and infrared satellites to alert us. Imagery satellites captured large troop movements or the movement of military equipment. There was little chance of a surprise strategic attack. This early warning system, as it would have enabled a retaliatory strike that would devastate the Soviet Union, made the strategy of "mutually assured destruction" feasible. This strategy, though grim, guided us through the Cold War.

Unfortunately, terrorist actions and planning are not as easily observed and discerned as the movement of missiles, submarines, tanks and military aircraft. Terrorists use commercial communications, improvised explosive devices, the internet and commercial air travel. The transactions which enable their heinous acts blend into a backdrop of the normal, everyday actions of an increasingly global society.

Looking at the Cold War in the rear view mirror, defending against the symmetric threat posed by the Soviet Empire seems like an "easy" task compared to defending against the asymmetric threat posed by terrorists, but it would be a mistake to think that winning the Cold War was "easy." When the Cold War began, the missile warning satellite constellation, Defense Support Program (DSP), did not exist. The first DSP

[13] Greg Simmons, "Debate Rages Over Legality of NSA Wiretap Program," Greg Simmons, *Fox News*, www.foxnews.com, (accessed December 21, 2005).

satellite was not launched until the early 1970s.[14] When the Cold War began there were no imagery satellites. The first photo reconnaissance satellite, Corona, was not launched until 1958.[15] The early warning system we relied on to win the Cold War was not developed overnight. It took a serious national effort, vast amounts of money and decades to develop. To put it simply, America rose to meet the threat posed by the Soviet Union and the Cold War. Meeting the threat required a guiding strategy, new technologies, new organizations and new policies working in concert. While the Cold War strategy remained fairly constant, technology, policy, and organizations, evolved with the changing landscape and in response to the enemy's actions.

This fact should serve as an encouragement in our present struggle. The United States does not yet have all the tools it needs to effectively meet the threat posed by transnational terrorists, but the nation is making progress. The process of identifying the capabilities needed to build a terrorism early warning system and thereby prevent terrorism is well underway. Many of these capabilities have been documented in numerous strategies, executive orders, laws and reports.

This chapter will capture those needs as articulated in the National Homeland Security Strategy, the National Strategy for Homeland Defense and Civil Support, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the National Intelligence Strategy and Executive Orders relevant to building a terrorism early warning system and improving information sharing. Figure 4 shows the security attributes derived from each of the documents. The descriptions of each document that follows serve to provide context and expound on the attributes culled from each document.

---

[14] United States Air Force, "Defense Support Program Fact Sheet," http://www.af.mil/factsheets/factsheet.asp?id=96 (accessed December 22, 2005).

[15] National Reconnaissance Office, "Corona Fact Sheet," http://www.nro.gov/corona/facts.html (accessed December 22, 2005).

	SECURITY / INFORMATION SHARING				
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security	Match data access to roles and responsibilities of oranizations engaged in countering terrorism	Produce multiple versions (security classifications) of information
			Facilitate oversight through use of audit trails, user authentication and access controls		

Figure 4. Desirable Security and Information Sharing attributes as articulated in various government documents.

A. NATIONAL HOMELAND SECURITY STRATEGY

The National Homeland Security Strategy, published in July 2002 prior to the establishment of the Department of Homeland Security, identifies six critical mission areas for Homeland Security. The first three mission areas focus on the prevention of terrorist attacks: Intelligence and Warning, Border and Transportation Security and Domestic Counterterrorism. In addition to the critical mission areas, the strategy identifies four "Foundations of Homeland Security" which "cut across all of the mission areas, across all levels of government, and across all sectors of our society."[16] These four foundations are: law, science and technology, information sharing and systems and international cooperation. The mission areas of intelligence and warning and domestic counterterrorism and the four foundations taken together formulate a high level outline of what is needed to develop a terrorist early warning system.

16 Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C., 2002).

1. Intelligence and Warning

The mission area of intelligence and warning is focused on eliminating the terrorists' ability to launch a surprise attack. The strategy acknowledges the difficulty in determining the identity, location, capabilities and intent of terrorists since they often move freely within democratic societies. The Intelligence and Warning section of the strategy specifically mentions the need to improve human source intelligence overseas (HUMINT), improve information sharing among agencies at all levels of government, to better utilize foreign-language documents and to identify, collect and analyze "new observables."

The linchpin in improving intelligence and warning is analysis. The strategy breaks analysis down even further into tactical threat analysis, strategic analysis of the enemy, vulnerability assessment and threat-vulnerability integration or "mapping." The four types of analysis are intended to result in policy changes and capability development, preventive action and warning and protective action. Figure 5 shows how the different types of analysis are intended to interact.

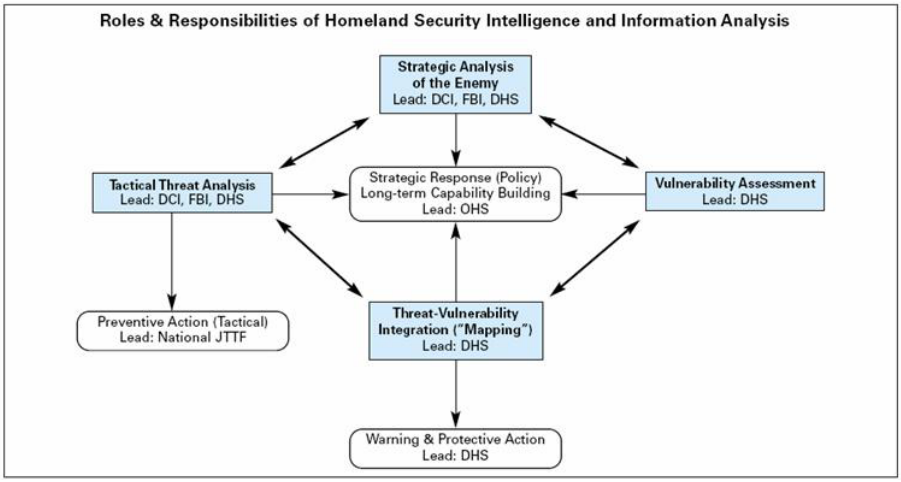

Figure 5. Roles and Responsibilities of Homeland Intelligence and Information Analysis (From: National Strategy for Homeland Security, 16.)

Since analysis is identified as the linchpin, the major initiatives the strategy recommends the nation undertake are all related to analysis. The first, enhancing the

analytical capabilities of the FBI, speaks to increasing the total number of analysts, improving those analysts skills and improving the information systems the analysts use. Additionally, it speaks of improving the relationship between the FBI and CIA. The strategy speaks only of improving the analytic capability of the FBI, but it has become clear since its writing that the analytic capability of the entire intelligence community must be improved for counterterrorism.

The second initiative, building capabilities through the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) division gave IAIP the burden of developing vulnerability assessments. It also gave them the responsibility of mapping terrorist threats to infrastructure vulnerabilities. Success in this area is dependent on IAIP being able to gather information from the entirety of the intelligence community as well as from state and local agencies and the private sector.

A DHS reorganization in 2005 broke IAIP into an intelligence function, now called the Office of Intelligence and Analysis (IA) and a critical infrastructure protection function, now residing in the Directorate for Preparedness. The fact remains that threat must be linked to vulnerability in an effective early warning system.

The third initiative, implementing the Homeland Security Advisory System, is envisioned simply as a way to communicate indications and warnings of terrorism to the American people. It is intended to be the output of the intelligence and warning system to the American people. As with any security system, a properly functioning system should be in place prior to activating the alert mechanism, otherwise the alert mechanism is prone to go off without due cause. This is akin to a car alarm going off for no particular reason—after numerous unspecified alerts, the alarm begins to be ignored.

The fourth initiative, utilizing dual-use analysis, speaks to the ability for analysts to identify the equipment and material that might be linked to carrying out an attack and to be able to evaluate whether or not the purchase of such materials might be linked to a potential terrorist act.

The final initiative, employing "red team" techniques, is simply another way to analyze the steps a terrorist would need to take prior to carrying out an attack and identifying vulnerabilities that might be subject to attack. Use of these red teams could

be particularly useful in identifying the transactions which precede (buying certain goods or services, etc) carrying out an attack. The knowledge gathered during red team exercises could aid pattern recognition to identify when these transactions are taking place.

2. Domestic Counterterrorism

The domestic counterterrorism chapter continues to emphasize the need for better information sharing among all levels of government. It states, "The U.S. government has not yet developed a satisfactory system to analyze information in order to predict and assess the threat of a terrorist attack."[17] The need for the federal government to be able to use information owned by state and local governments and for state and local governments to be able to access federal databases is clearly identified.

Major initiatives listed in the domestic counterterrorism chapter include: improving intergovernmental law enforcement coordination, facilitating the apprehension of potential terrorists, continuing ongoing investigations and prosecutions, restructuring the FBI to emphasize the prevention of terrorist attacks, targeting and attacking terrorist financing and tracking foreign terrorists and bringing them to justice.

A common thread running through each of these initiatives is the necessity to access information wherever it resides. Specific sources of information mentioned in this section of the strategy include the FBI's National Crime Information Center (NCIC) database, the Department of State's TIPOFF System which provides information on known and suspected terrorists and the use of commercially available databases (when used consistent with Constitutional standards). The strategy also mentions the FBI's creation of a consolidated watch list, fully accessible to the law enforcement and intelligence communities which would include information derived from the intelligence community, Department of Defense, foreign governments and the FBI. Again, the need to link law enforcement and foreign intelligence information is clearly identified.

B. NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT

The National Strategy for Homeland Security addresses what is needed for law enforcement and DHS agencies, but it does not deal specifically with the capabilities that

[17] *National Strategy for Homeland Security*, 25.

must be developed for the Department of Defense (DoD). The June, 2005 National Strategy for Homeland Defense and Civil Support identifies the capabilities DoD must possess if it is to be effective in the fight against terrorism. This strategy makes no false division between a "home game" and the "away game." It more accurately describes a war that knows no boundaries and states that the highest priority for DoD is "protecting the United States homeland from attack."[18]

1. Active, Layered Defense

The cornerstone of the strategy is what the authors call an "active, layered defense:"

> This active, layered defense is global, seamlessly integrating US capabilities in the forward region of the world, the global commons of space and cyberspace, in the geographic approaches to US territory, and within the United States. It is a defense in depth. To be effective, it requires superior intelligence collection, fusion, and analysis, calculated deterrence of enemies, a layered system of mutually supporting defensive measures that are neither passive nor ad hoc, and the capability to mass and focus sufficient warfighting assets to defeat any attack.[19]

2. Lead, Support, and Enable

The strategy sets up a framework that acknowledges that there are things that DoD must take leadership in, things they must support civil authorities in doing, and things DoD can do to enable other domestic and international partners to improve their contribution to homeland defense and security. In speaking of leading, the strategy focuses on carrying out military operations to "dissuade, deter, and defeat attacks upon the United States" including its people and critical infrastructure. In speaking of supporting, the strategy focuses on those tasks in which DoD personnel or equipment is needed to help another government agency be more effective in preventing, protecting or recovering from an attack. In speaking of enabling, the strategy focuses on ways technology and expertise can be shared across military and civilian boundaries.

Whether DoD is leading, supporting or enabling, it is important to note that in defending the homeland, DoD never acts alone. The strategy makes it clear that DoD

---

[18] U.S. Department of Defense, *Strategy for Homeland Defense and Civil Support* (Washington D.C., June 2005), 1.

[19] Ibid., 1-2.

needs other agencies (federal, state, local, private, international) and that it believes the other agencies need DoD to effectively combat terrorism.

3. Key Objectives

Operating within the lead, support, enable framework, the strategy lists five key objectives in priority order:

1. Achieve maximum awareness of potential threats.
2. Deter, intercept and defeat threats at a safe distance.
3. Achieve mission assurance.
4. Support civil authorities in minimizing the damage and recovering from domestic chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) mass casualty attacks.
5. Improve national and international capabilities for homeland defense and homeland security.

The primary objective in homeland defense lies in "achieving maximum awareness" of an enemy that knows no borders or boundaries. If terrorists can plan and launch an attack from anywhere in the world, including within the United States, it is reasonable to assume that any system designed to perceive indications and warnings of that attack must be able to operate anywhere in the world, including within the United States, in order to be effective. A system and military only capable of achieving awareness of threats originating outside of its borders is insufficient. It must have the capability to look within the borders if that is where the threat originates.

4. Capabilities for Achieving Maximum Awareness of Threats

The strategy advocates for the development of numerous core capabilities in support of the objectives listed above. The capabilities most relevant to "achieving maximum awareness" or developing a terrorism early warning system revolve around improving the nation's intelligence, surveillance, and reconnaissance (ISR) capability and improving information-sharing. The core capabilities listed in this strategy are the capabilities DoD views as necessary to implement the National Security Strategy, the National Strategy for Homeland Security and the National Defense Strategy. For a strategy document, the core capabilities listed are fairly specific.

a. Core Capability: Capable and Agile Defense Intelligence Architecture.

Protecting the United States from asymmetric threats require the intelligence community to adjust its focus. The intelligence community had grown quite

adept at targeting and understanding the nature of Cold War threats. The intelligence community must bring that same skill and professionalism to focus on the threat of terrorism.

This adjustment is well underway as evidenced by the establishment of the National Counterterrorism Center (NCTC), the establishment of DoD's Joint Task Force for Combating Terrorism (JITF-CT), the establishment of DHS's Information Analysis and Infrastructure Protection (IAIP) directorate, the passage of the IRTPA and the issuance of numerous executive orders regarding intelligence reform and information sharing. For its part in reorienting intelligence priorities, DoD will:

- Focus on integrated collection management of foreign and military information and its application to homeland defense and homeland security;
- Better utilize national intelligence capabilities to increase early warning and support prevention, interception, and disruption of potential threats overseas or in the approaches to the United States;
- Collect homeland defense threat information from relevant private and public sector sources, consistent with US constitutional authorities and privacy law;
- Identify capability needs for CBRNE sensors to meet homeland defense requirements; and
- Develop automated tools to improve data fusion, analysis, and management, to track systematically large amounts of data, and to detect, fuse, and analyze aberrant patterns of activity, consistent with US privacy protections.[20]

b. Core Capability: Collect, Analyze, and Understand Potential Threats.

With regards to improving collections, the strategy focuses mostly on improving its overseas human intelligence capability. It also states that the NSA and the National Geospatial-Intelligence Agency (NGA) "will continue to provide their unique capabilities in support of the national homeland security mission in accordance with applicable laws and regulations."[21] While not much more is said about use of signals intelligence (SIGINT) and imagery intelligence (IMINT) it should be pointed out that using these assets inside the homeland "in accordance with applicable laws and

[20] *Strategy for Homeland Defense and Civil Support*, 20-21.

[21] Ibid., 21.

regulations" is not a trivial matter. However, Hurricane Katrina proved how technical intelligence assets can play a critical role inside the homeland and that it can be accomplished without major privacy implications. For example, the NGA began providing imagery from both classified and commercial satellite systems in the aftermath of the hurricane to aid in the response and recovery effort. In addition to satellite imagery, on September 1, the Air Force provided a U-2 reconnaissance aircraft to take pictures of the Katrina-ravaged gulf coast.[22] The use of these assets inside the homeland during the disaster serves as powerful evidence that intelligence platforms typically reserved for overseas use will be demanded for use in the homeland when overwhelming political pressure is present as it was during Katrina.

Figure 6 serves as a visual testimony to the utility of overhead reconnaissance. In this case, the use of commercial satellite imagery of New Orleans before and after Katrina allowed a wide audience to grasp the devastation.

Figure 6. Commercial Satellite Imagery of New Orleans before and after Katrina. Image Courtesy DigitalGlobe
(From: David Leonard, "Military, Civilian Satellites Aid Katrina Relief.")

In addition to improved collection capabilities, the Strategy for Homeland Defense and Civil Support places emphasis on developing "a cadre of specialized terrorism intelligence analysts within the Defense intelligence community." An improved analysis capability is absolutely vital to achieving awareness of threats since

[22] David Leonard, "Military, Civilian Satellites Aid Katrina Relief," *MSNBC*, September 6, 2005, http://www.msnbc.msn.com/id/9229100/ (accessed September 7, 2005).

unanalyzed collections are practically worthless. DoD envisions their analysts imbedded at interagency centers, but states that their analytical capability is specifically intended to "support military activities overseas and in the approaches to the United States."[23] Given this exclusion inside our borders, it is essential that the information sharing processes be in place to allow rapid cooperation between DoD and interagency analysts covering domestic intelligence should a DoD response become necessary inside the homeland.

c. Core Capability: Detection, Identification, and Tracking of Emerging Threats in All Operational Domains

Air and maritime domain awareness are a particularly challenging problem for homeland defense due to the high volume of traffic within these domains. The unimpeded flow of commercial shipping and air travel are critical to maintaining the economy. As a result, the air and maritime domains represent an excellent opportunity for terrorists to hide among the masses, or blend in with normal, everyday air and sea traffic. In addition, there are grave consequences associated with military action against a civilian target (for example the shootdown of a commercial airliner). Simply put, the military cannot afford to make a mistake by misidentifying a friendly vessel or aircraft as hostile.

As a result, it is not sufficient merely to detect, identify and track vessels and aircraft. An effective surveillance capability would additionally allow military analysts and operators to discern the intent of a vessel or aircraft of interest. This is a particularly challenging situation since a domestic persistent, wide-area surveillance capability with enough fidelity to determine intent is likely to raise privacy concerns. Without these capabilities, however, the military may be forced to take action with incomplete information perhaps resulting in the loss of innocent lives.

Much work has been done since 9/11 to improve NORAD's air surveillance capabilities by integrating Federal Aviation Administration (FAA) radar feeds, but the coverage is not sufficient against all potential threats at all altitudes.[24] A similar problem exists in the maritime domain. Developing a persistent, wide-area

---

23 *Strategy for Homeland Defense and Civil Support*, 21.

24 Author's operational experience

surveillance capability within the borders and in the approaches to the United States "could require the development of advanced technology sensors to detect and track" aircraft and vessels of interest.[25]

d. Core Capability: Shared Situational Awareness within DoD and with Domestic and Foreign Partners

"Shared situational awareness is defined as a common perception of the environment and its implications."[26] Based on the fact that the indicators preceding acts of terrorism quite often look like crime rather than building up for war, this strategy advocates for an "unprecedented degree of shared situational awareness among Federal agencies, with state, local, tribal, and private entities, and between the United States and its key foreign partners."[27] It goes on to lay out some specific capabilities necessary to achieve the goal of shared situational awareness:

- Seamless connectivity and timely, accurate, and trusted information available to all DoD components
- The ability to process information and move it to warfighters, policymakers, and support personnel on demand
- Ability to establish a real-time link among sensors, decision makers, and warfighters to facilitate the rapid engagement of enemy targets

These capabilities are dependent upon a worldwide, integrated information infrastructure with connectivity to wherever the pertinent information may reside. DoD acknowledges the power inherent in such a vast, well-networked information system and identifies that its development "requires appropriate safeguards to ensure that DoD intelligence components rigorously apply laws that protect Americans' civil liberties and privacy."[28]

C. INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) lays out succinct requirements for attributes that should be included in what it calls the "Information Sharing Environment" (ISE) in Title I Section 1016 of the law. Prior to

---

25 *Strategy for Homeland Defense and Civil Support*, 23

26 Ibid.

27 *Strategy for Homeland Defense and Civil Support*, 23

28 *Strategy for Homeland Defense and Civil Support*, 24

listing those attributes, the law clarifies that the ISE is specifically intended for the use of sharing "terrorism information." The law provides a narrow definition for terrorism information.

> The term "terrorism information" means all information, whether collected, produced, or distributed by intelligence, military, law enforcement, military, homeland security or other activities relating to:
>
> a. the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
>
> b. threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
>
> c. communications of or by such groups or individuals or
>
> d. groups or individuals reasonably believed to be assisting or associated with such groups or individuals.[29]

The law tasks the President with the burden of creating the ISE "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." The law additionally tasks the President with designating "the organizational and management structures that will be used to operate and manage the ISE" and with the task to "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE."[30]

Having narrowed the ISE's use to sharing terrorism information and established the President's authority and obligation to establish it, the law moves on to specify certain attributes the ISE must contain. Generally the law specifies that the ISE should ensure the ability to share "terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and

[29] U.S. Congress, House, *Intelligence Reform and Terrorism Prevention Act of 2004* (December 7, 2004, 108th Cong, 2d sess,. House report No. 108-796).

[30] *Intelligence Reform and Terrorism Prevention Act of 2004*, 29.

technologies" and that it should be a "decentralized, distributed, and coordinated environment."[31] More specifically the law directs that the President should build an ISE that:

> a. connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
>
> b. ensures direct and continuous online electronic access to information;
>
> c. facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;
>
> d. builds upon existing systems capabilities currently in use across the Government;
>
> e. employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
>
> f. facilitates the sharing of information at and across all levels of security;
>
> g. provides directory services, or the functional equivalent, for locating people and information;
>
> h. incorporates protections for individuals' privacy and civil liberties; and
>
> i. incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

Working from this guidance, the Director of National Intelligence, whose position was created by IRTPA and the ISE Program Manager have made substantial progress. One of the first fruits of their labor was the writing of the National Intelligence Strategy.

D. NATIONAL INTELLIGENCE STRATEGY

The subtitle of the National Intelligence Strategy is telling—transformation through integration and innovation. Transformation speaks of the need for change—not incremental change, but of a new way of doing things for a new era. Integration speaks of the acknowledgement that intelligence organizations should not view themselves as

[31] *Intelligence Reform and Terrorism Prevention Act of 2004,* 29.

independent but interdependent. It also speaks of the vision to merge foreign intelligence with domestic intelligence to thwart transnational terrorism. Innovation speaks to the need for creativity in transforming and integrating the intelligence community.

One thing that is clear from the beginning of the Intelligence Strategy to the end is that it intends to remove any barriers or "walls" to sharing information between foreign and domestic intelligence agencies or analysts. It states very clearly, "the time has come for our domestic and foreign intelligence cultures to grow stronger by growing together."[32] The intentional destruction of the "wall" is noteworthy because it forces a hard look at why the wall between foreign and domestic intelligence was constructed in the first place. The wall, conceived as a necessary protection of American's privacy and liberty, must be replaced by something as effective (if not more so) as domestic and foreign intelligence grow together.

Equally as noteworthy as the removal of the wall is the strategy's stated commitment to preserving privacy and civil liberties. As it states, "the emphasis placed on national intelligence reflects a change in the threats we face as a nation, not a change in our commitment to civil liberties and freedom."[33]

The overarching goal of the strategy is to integrate, through policy, doctrine and technology, the various elements of the intelligence community. To accomplish this goal, the document offers fifteen strategic objectives in all, breaking them between mission objectives and enterprise objectives. Some of these objectives, and their subsequent elucidation, give further insight into the type of tools required for a terrorism early warning system.

1. Mission Objectives

Three of the five mission objectives contain guidance that are highly relevant to building an early warning system for terrorism. The first mission objective, "defeat terrorists at home and abroad by disarming their operational capabilities and seizing the initiative from them by promoting the growth of freedom and democracy," identifies the need to:

---

[32] Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America* (Washington D.C., October 2005), 1.

[33] *National Intelligence Strategy*, 2.

- Integrate and invigorate all US intelligence efforts to identify and disrupt terrorist organizations abroad and within US borders
- Uncover terrorist plans and intentions, especially those that may involve obtaining or using weapons of mass destruction
- Enable those outside the Intelligence Community with valuable counterterrorism information (such as police, corrections officers, and border patrol officers) to contribute to the national counterterrorism effort.
- Create an information sharing environment in which access to terrorism information is matched to the roles, responsibilities, and missions of all organizations engaged in countering terrorism, and is timely, accessible, and relevant to their needs.[34]

The task of creating the ISE is laid upon the Program Manager, ISE, John Russack. Additionally, this office is responsible for identifying the needs of federal, state, local, and tribal governments and the private sector and ensuring their needs are satisfied by the ISE.

The fourth mission objective is focused on developing innovative ways to gain insight into the most difficult intelligence targets. It offers two particularly relevant capabilities to this discussion. The intelligence community needs the capability to break into the thinking of terrorist leaders by:

- Making the best use of all-source intelligence, including from open sources, on the most difficult targets
- Improving human intelligence and corresponding technical intelligence capabilities.[35]

2. Enterprise Objectives

There are ten enterprise objectives listed in the strategy, all of which contain important ideals for transforming the intelligence community. There are two objectives which are particularly relevant within the scope of this thesis. The first enterprise objective, "build an integrated intelligence capability to address threats to the homeland, consistent with US laws and the protection of privacy and civil liberties," stresses the importance of uniting all of the players with the intelligence community. It insists that all intelligence elements, in accordance with applicable laws and consistent with the protection of civil liberties and privacy, focus their capabilities to ensure that:

---

[34] *National Intelligence Strategy*, 6.

[35] *National Intelligence Strategy*, 9.

- All Intelligence Community components assist in facilitating the integration of collection and analysis against terrorists, weapons of mass destruction, and other threats to the homeland.
- State, local, and tribal entities and the private sector are connected to our homeland security and intelligence efforts.[36]

The fifth enterprise objective also contains guidance that identifies capabilities that homeland operators and analysts need in order to sufficiently protect the nation from terrorism. This objective, "ensure that Intelligence Community members and customers can access the intelligence they need when they need it" is a reiteration of IRTPA's direction to "ensure maximum availability of and access to intelligence information."[37] To meet this objective, the intelligence community must:

- Remove impediments to information sharing within the Community, and establish policies that reflect need-to-share (versus need-to-know) for all data, removing "ownership" by agency of intelligence information
- Build a user-friendly system that allows customers to find needed intelligence and access it immediately
- Develop flexible and secure networks adaptable to a rapidly changing environment and capable of getting intelligence in an unclassified form to non-traditional customers such as state, local, and tribal governments and the private sector
- Create an intelligence "cyber community" where analysts, collectors, and customers can interact swiftly and easily in considering classified information.

Taken together, the National Intelligence Strategy and IRTPA give the sense that the intelligence community is intent on transforming, integrating and innovating to meet the challenges of the twenty first century. The pursuit of the above objectives shows that the DNI is intent on developing a comprehensive network of analysts and operators whether they wear suits, military uniforms, badges, or some type of protective gear. This is significant because "it takes networks to fight networks."[38]

E. EXECUTIVE ORDERS

President Bush signed three executive orders on August 27, 2004, each of them addressing some aspect of intelligence reform and information sharing.

36 *National Intelligence Strategy*, 11.

37 *National Intelligence Strategy*, 14.

38 John Arquilla, David Ronfeldt and Michele Zanini, "Networks, Netwar and Information-Age Terrorism," *Countering the New Terrorism* (Santa Monica, CA: RAND, 1999), 42.

1. Executive Order 13354 – The Establishment of the National Counterterrorism Center (NCTC)

EO 13354, sets policy for information sharing, establishes the NCTC as the primary "place" where the integration of counterterrorism information should happen, and defines the responsibilities of various players within the intelligence community in relation to the NCTC. The policy, consistent with the documents above, states that:

> a. To the maximum extent consistent with applicable law, agencies shall give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of transnational terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information.
>
> b. Agencies shall protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing section 1(a) of this order.[39]

The order establishes that the NCTC as the primary organization within the government for analyzing and integrating terrorism and counterterrorism information. The center is intended to support all other agencies tasked with counterterrorism missions. The center was not established to execute operations, but rather to support, with the best available intelligence and planning, those organizations with operational responsibilities. The center does have the authority to task agencies with specific counterterrorism operations though an agency who objects to their tasking may appeal to the National or Homeland Security Council.

The order appointed the Director of Central Intelligence to supervise the center[40], but the role has since passed to the DNI as a result of IRTPA.[41] The order also directs heads of military, intelligence, homeland security, diplomatic and law enforcement agencies with terrorism information and responsibilities to make their information readily available to the center.

---

39 U.S. President, *Executive Order*, National Counterterrorism Center, Executive Order 13354, *Federal Register 69*, no. 169 (1 September 2004).

40 Ibid.

41 *Intelligence Reform and Terrorism Prevention Act of 2004.*

2. Executive Order 13355 – Strengthened Management of the Intelligence Community

This executive order gives greater authority to the DCI, expands the role of national intelligence by amending EO 12333, gives the DCI greater control and oversight of the overall intelligence budget, gives the DCI greater authority in approving the heads of intelligence organizations and gives the DCI greater oversight in the development of minimum standards for the intelligence community.[42] Most of the power and authority given to the DCI under this executive order were transferred to the DNI through the signing of IRTPA.[43]

Some of the key amendments to EO 12333 related to the sharing of terrorism information include:

> …ensure that United States intelligence collection activities are integrated in: (i) collecting against enduring and emerging national security intelligence issues; (ii) maximizing the value to the national security; and (iii) ensuring that all collected data is available to the maximum extent practicable for integration, analysis, and dissemination to those who can act on, add value to, or otherwise apply it to mission needs.
>
> Establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:
>
> > the fullest and most prompt sharing of information practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats against our homeland, our people, our allies, and our interests; and
> >
> > the establishment of interface standards for an interoperable information sharing enterprise that facilitates the automated sharing of intelligence information among agencies within the Intelligence Community.[44]

---

[42] U.S. President. *Executive Order*. "Strengthened Management of the Intelligence Community, Executive Order 13355." August 27, 2004. Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html (accessed January 4, 2006).

[43] *Intelligence Reform and Terrorism Prevention Act of 2004.*

[44] U.S. President, Executive Order, "Strengthened Management of the Intelligence Community," 1.

3. Executive Order 13356 – Strengthening the Sharing of Terrorism Information to Protect Americans

The third order President Bush signed on August 27, 2004, as the title suggests, deals directly with sharing information within the structure set up by the preceding two orders. There is some repetition and overlap among the three orders, EO 13356 reiterates the policy put forth in EO 13354 and quoted above. The order then specifically identifies the duties of the heads of agencies who collect terrorism information in ensuring the information is shared as widely as possible. In addition, a requirement is given for the establishment of common information standards to improve the sharing of information across agencies such as:

> requiring, at the outset of the intelligence collection and analysis process, the creation of records and reporting, for both raw and processed information including, for example, metadata and content, in such a manner that sources and methods are protected so that the information can be distributed at lower classification levels, and by creating unclassified versions for distribution whenever possible;
>
> requiring records and reports related to terrorism information to be produced with multiple versions at an unclassified level and at varying levels of classification, for example on an electronic tearline basis, allowing varying degrees of access by other agencies and personnel commensurate with their particular security clearance levels and special access approvals;
>
> requiring terrorism information to be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any other agency to which it has been made available, to the maximum extent permitted by applicable law, Executive Orders, or Presidential guidance;
>
> minimizing the applicability of information compartmentalization systems to terrorism information, to the maximum extent permitted by applicable law, Executive Orders, and Presidential guidance; and
>
> ensuring the establishment of appropriate arrangements providing incentives for, and holding personnel accountable for, increased sharing of terrorism information, consistent with requirements of the Nation's security.[45]

[45] U.S. President, *Executive Order,* "Strengthening the Sharing of Terrorism Information to Protect Americans," August 27, 2004. Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html (accessed January 4, 2006).

Finally, Section five of the order establishes an Information Systems Council (ISC) tasked with planning and overseeing the establishment of an information sharing environment to facilitate the automated sharing of terrorism information. Contained within their task is the need to examine existing systems for gaps and overlap, recommend near-term solutions and to develop and environment that is scalable so that it can incorporate future sources of information. In summary, EO 13356 establishes the need for the creation of common standards for information sharing, a recommendation for the establishment of clear procedures and guidelines regarding information sharing, and for the development of a plan to establish the ISE. These tasks were given to the ISC. At the present, the ISC has published their initial plan (20 December 2004) and is working in conjunction with the ISE Program Manager's office.

F. SUMMARY

At the core of building an early warning system to deal with today's threat of transnational terrorism is the ability to share information with any person or agency involved in the fight. Today's enemy is diffuse and networked. As a result, the indicators of their intended attacks are diffuse and networked. Perceiving these indicators requires a diffuse and networked system of people, information and technology centered on common objectives, policy and guidelines.

The above documents give a roadmap of what the government envisions is necessary to make this network a reality. These documents can be reduced to the following attributes forming the "left hand side" or security side of the matrix. These attributes are summarized in Figure 7.

	SECURITY / INFORMATION SHARING				
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security	Match data access to roles and responsibilities of oranizations engaged in countering terrorism	Produce multiple versions (security classifications) of information
			Facilitate oversight through use of audit trails, user authentication and access controls		

Figure 7. The Left Hand or Security Side of the Privacy and Security Reference Matrix

Very simply, the vision must be to create an environment where the right people can quickly and easily get the information they need, wherever it may reside, to carry out their mission to preempt acts of terrorism. In doing so, as all of the guidance above affirms, the privacy and civil liberties of Americans must always be a key consideration.

III. MEETING THE PRIVACY NEEDS OF AMERICANS

If the government is to generate an ISE or early warning system capable of putting "actionable intelligence" into the hands of those who need it to preempt a terrorist act, it must do more than just say it has the desire to protect the privacy and civil liberties of Americans while doing so. It must articulate what is meant by privacy, convince the American public (or at least its representatives) that this definition is sound and show that the policy and technical control mechanisms governing the system can sufficiently guarantee this privacy can be maintained.

This chapter identifies some of the privacy advocates' key arguments and offers widely accepted privacy principles that should be considered in the development of an ISE architecture. These principles formulate the right-hand side of the matrix and are captured in Figure 8.

PRIVACY	
FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
Notice/Awareness	Data Quality
Choice/Consent	Purpose Specification
Access/Participation	Use Limitation
Security/Data Integrity	Collection Limitation
Enforcement	Security Safeguards
	Openness
	Individual Participation
	Accountability

Figure 8. Desirable privacy attributes that are widely accepted by privacy advocates form the Right Hand or Privacy side of the Privacy and Security Reference Matrix

A. VARIABLE DEFINITIONS OF PRIVACY

Not all Americans share a common or even similar definition of privacy. Similarly, not all Americans value privacy equally. At one end of the spectrum is Scott McNeely, CEO of Sun Microsystems, who infamously commented on privacy in the information age. "You have no privacy, get over it."[46] At the other end of the spectrum are those who equate secrecy with privacy.

The first notion of privacy (or lack thereof) in the context of government surveillance and increased information sharing is disconcerting and politically untenable. The latter notion likely faded with the advent of the computer, databases, the internet and e-commerce.

Many Americans are apathetic toward the notion of the government being able to collect their personal information, making statements such as, "If I don't do anything wrong, why should I care if the government reads my e-mail?"[47] To others, the mere notion of improving the government's ability to search across even its own databases or improve surveillance generates the fear that the government is developing Big Brother.[48]

While it is outside the scope of this paper to develop an exact definition of privacy, it is assumed that most Americans concept of privacy lies somewhere between these two extremes. Most Americans do not expect to live in absolute secrecy, nor do they expect nor desire their government to be able to intrude on the intimate details of their lives.[49]

B. THE FOURTH AMENDMENT IN THE INFORMATION AGE

Early efforts to increase the government's ability to mine and more effectively share data after 9/11, TIA and CAPPS II, were mired in controversy. The controversy led to their ultimate demise via the loss of congressional support and funding. A major

---

46 Polly Sprenger, "Sun On Privacy: 'Get Over It,'" *Wired News*, January 26, 1999, http://www.wired.com/news/politics/0,1283,17538,00.html, (accessed January 6, 2006).

47 Personal conversations with the author in discussing this thesis topic often resulted in a similar sentiment.

48 See, for example, Jay Stanley and Barry Steinhardt, American Civil Liberties Union, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," January 2003, 1.

49 See, for example, Daniel J. Solove, "A Taxonomy of Privacy" for more on the definition of privacy. Available online: http://ssrn.com/abstract=667622

contributor to these programs' demise is the absence of clear legal standards relating the use of new technology to the fourth amendment.[50]

The *United States v. Miller* decision offers little help in this dilemma since it ruled that the fourth amendment does not apply to government acquisition of data in the hands of a third party since there is no "reasonable expectation of privacy" for information already released by the individual.[51] The Miller case, decided in 1976, held that the government's subpoena and subsequent use of Miller's bank records to convict him of conspiracy did not constitute unlawful search and seizure. In their ruling, the court commented that copies of the checks in question were "business records of the bank" not the "respondent's private papers." Furthermore, the court stated that Miller could not expect those records to remain private since they contained information he "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[52]

This precedent continues to hold despite the fact that personal information is much more readily available via the internet and through information brokers such as ChoicePoint or Lexis/Nexis than it was at the time of the *United States v. Miller* decision.

The ubiquitous nature of personal and transactional information in 2006 combined with this Supreme Court ruling means government has access to large volumes of information unfettered by Constitutional law. If a third party has a piece of information, there is virtually no Fourth Amendment limitation to keep the government from obtaining it. Effectively, this makes it easier for a government agency to buy transactional information from information brokers than to gather it on its own.

Normally, in the absence of Constitutional limits, Congress passes statutory limits. To date, however, there is no clear statutory guidance for data mining and

---

50 Fred H. Cate, "Legal Standards for Data Mining," in forthcoming *Emergent Information Technologies and Enabling Policies for Counter Terrorism*, ed. Robert Popp and John Yens (Hoboken, N.J.: Wiley-IEEE Press, 2006), 1.

51 United States v. Miller, 425 U.S. 435 (1976), as quoted in Cate, "Legal Standards for Data Mining," 2.

52 United States v. Miller, 425 U.S. 435 (1976)., http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?navby=volpage&court=us&vol=425&page=442, (accessed February 21, 2006).

information sharing activities. This is especially problematic if the information available for purchase from information brokers is less accurate than information the government might be able to obtain on its own.

The lack of clear legal guidelines intersecting modern information sharing and data mining capabilities impacts both privacy and security. This lack of guidance undermines public confidence in the government's ability to share and mine information in a way that does not threaten liberty. Additionally, it leads to uncertainty among those analysts and operators tasked with counterterrorism responsibilities.[53] An analyst or operator uncertain as to whether or not he could "get in trouble" or jeopardize his credibility or career for a particular action is likely to avoid the risk.

Thus, the letter of the law, as interpreted by court decisions, is of little use in lighting the way ahead. However, the spirit of the fourth amendment, particularly the ideals of "reasonableness" and "probable cause," is useful in the ongoing security and privacy debate. Relying on these principles applied in a modern environment, Congress must rigorously engage in the debate and provide a statutory law to enable the government to make progress in preventing terrorism while addressing privacy concerns. Such a statutory law could further clarify the "rules of engagement" for the sharing of information and the design of a terrorism early warning system. In the absence of such guidance, it is useful to examine the chief concerns of privacy advocates.

C. THE PRIMARY CONCERNS OF PRIVACY ADVOCATES

1. The Chilling Effect

The chilling effect stems from the concern that people, if they feel they are being watched, will act differently or not engage in constitutionally protected activities out of a fear of being monitored. This is not a new fear. Vice President Hubert Humphrey articulated the impact of the chilling effect over forty years ago: "we act differently if we feel we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change."[54] The chilling effect could be a positive or negative depending on who changes their behavior

[53] Cate, "Legal Standards for Data Mining," 3.

[54] Hubert H. Humphrey, Foreword to Edward V. Long, *The Intruders* at viii (1967). As quoted in "Safeguarding Privacy in the Fight Against Terrorism," Report of the Technology and Privacy Advisory Committee (TAPAC) (Washington DC: March 2004), 35.

as a result of feeling like they are being watched. A terrorist, for example, might be deterred from a certain activity out of fear of detection. However, an American may feel he cannot attend a religious service, associate with a certain person, or engage in political dissent out of a fear of observation or retribution as a result of that observation. Since this has the potential to limit civil liberties, it is clearly a negative aspect of the chilling effect.[55]

The chilling effect has not been particularly well supported by the courts. For example, Laird v. Tatum, showed that, in order to be considered in conflict with liberty, actual harm and significant effect on constitutionally protected activities must be shown. In summary the court found that chill was not simply the result of the knowledge of being observed or "from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual."[56] Furthermore, the decision in Younger v. Harris showed that the mere presence of a chilling effect is not sufficient to deem a state action unconstitutional, especially if the state lacks an alternative means for controlling a particular conduct.[57]

The chilling effect argument may carry less weight as society becomes more and more accustomed to being observed. For example, some individuals appear to have grown quite comfortable with having private conversations in public places, sending e-mails on computer systems emblazoned with "use of this system constitutes consent to monitoring" stickers and talking to spouses in the virtual "panopticon" of life inside cubicle farms.[58] This is not to imply that the chilling effect should be dismissed, rather it is intended to place the argument in a modern context.

---

55 *TAPAC Report*, 35.

56 408 U.S. 1 (1972) at 11, as quoted in K. A. Taipale, "Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd," *Yale Journal of Law and Technology* 7, no. 123, December 2004. Available at SSRN: http://ssrn.com/abstract=601421

57 Younger v. Harris, 401 U.S. 37, 51 (1971), as quoted in "Technology, Security and Privacy," 143.

58 Author's personal observation from eight years of experience in living inside of cubicles with various coworkers who use phones and computers "subject to monitoring."

The TAPAC report suggests that "to diminish these risks [of the chilling effect], it is critical that government data mining activities be as transparent as possible and subject to both clearly defined limits and effective oversight."

2. The Slippery Slope (Expansive Use)

The slippery slope derives from the fear that if new and greater power is given to the government to fight terrorism, it will eventually be used to address lesser crime. The context of recent NSA wiretapping headlines is an illustrative example. If wiretapping suspected overseas al Qaeda members' phone calls to parties within the United States proves particularly effective, a fear is that it may spiral to tapping purely domestic telephone conversations. Wiretapping may then be implemented to fight narcotics trade, then perhaps white collar crime and eventually petty crime. Before long, wiretapping becomes the norm leading to what William Safire called the "supersnoop's dream"[59] and Michael Froomkin dubbed "perfect law enforcement."[60]

The slippery slope is a real danger when one considers the noble zeal most law enforcement, homeland defense and homeland security professionals bring to their jobs. These professionals are almost always driven to "do better" and the leaders of such organizations are normally more than willing to expand their power or reach as widely as possible in an effort to protect the populations they are responsible for.

Unfortunately, history has shown a correlation between expanding power and the potential for corruption. This presents the opportunity for what starts as a pure motive to serve the public the potential to turn into a threat to privacy and civil liberties. To address the slippery slope, power must somehow be balanced and oversight mechanisms put in place to curb the slide from noble intentions to corruption.

To guard against expansive use and the slippery slope, it is imperative that government clearly define the types of information that may be shared and not allow this definition to creep. Fortunately, the authors of IRTPA provided a narrow definition of

59 William Safire, "You are a Suspect," *New York Times*, November 14, 2002.

60 Michael Froomkin, "The Death of Privacy?" *Stanford Law Review* (2000): 1461-1471.

"terrorism information." This definition is helpful as it defines that the use of the ISE is to be constrained to tackling the problem of transnational terrorism, not applied more broadly.

3. Abuse and Misuse

Many of the prohibitive policies that currently govern domestic surveillance, intelligence and information sharing practices trace their origins to recommendations made by the Church Committee Report which addressed the problem of intelligence abuse and misuse during the sixties and seventies. These abuses are not make-believe stories that the privacy lobby invented. An excerpt from the report succinctly summarized the problem.

> (The Church Committee) found control and accountability failures in oversight and supervision. Those responsible for overseeing and supervising domestic intelligence activity delegated broad authority without establishing guidelines and procedural checks, failed to monitor activities, were at times willfully ignorant of improper or illegal activity, and even requested questionable practices. Internal agency oversight was inadequate. Investigations were overbroad, operated without standards, and dragged out long after any national security objective had expired. Information was often collected and disseminated to serve the political interests of a particular intelligence agency or administration or to influence social policy and political decisions, and information on individuals was disseminated too freely and retained past any point of relevance for national security purposes.[61]

Given this relatively recent history of government abuse, the public's fear of abuse and misuse of personal information is one that must be confronted head on. The policy and technologies put in place to enable oversight and guard against abuse must not only be effective they must be explainable to the public is such a way that results in increased trust. As a goal, these mechanisms should strive to satisfy even the most aggressive privacy advocates. In fact, they should likely be developed with the policy advocate's input. Quite simply, the protections against misuse and abuse must be overwhelmingly convincing or they will become mired in the political process and the system is likely to never see the light of day.

---

[61] Mary De Rosa, "Privacy in the Age of Terror," *Washington Quarterly* (Summer 2003), 29-30.

4. Mistaken Identity or Misidentification

Mistaken identity or misidentification rises out of the fear that a negative action, might be taken against an innocent individual. In a system designed to preempt or prevent terrorism (as opposed to waiting for the criminal act to occur) it is possible that innocents could be arrested, harmed or even killed. Misidentification could manifest itself in myriad ways such as data errors, through the process of data integration, as the result of matching names only and through false positives.[62]

Databases often contain incorrect or inaccurate information. Pam Dixon of the World Privacy Forum conducted a study of the accuracy of one of the country's leading information brokers, ChoicePoint. In her sample, 90% of the records she obtained had errors. Some of the errors were glaring such as the wrong sex. Numerous anecdotes reflect individuals obtaining their ChoicePoint report and noting errors such as being identified as owners of businesses they did not own or having post office boxes they did not have.[63]

Data errors can occur by transposing letters or numbers, by transposing first and last names, by mixing data fields (e.g. associating one person's address with the wrong name) and many other ways. Given that data can often be inaccurate, information should be corroborated through multiple sources when possible and negative action should be greatly constrained when there is uncertainty in the accuracy of the data. As an example, the government should not detain a person based solely on data obtained from a third party data broker such as ChoicePoint or Lexis/Nexis.

Integrating vast volumes of data carries with it the difficulty of ensuring that data is attributed to the correct individual and only that individual. The TAPAC report highlights many of these challenges.

One challenge is that names are often spelled and stored in various ways. For example the author may be referred to as Kneilan Novak, Kneil Novak, Kneilan K.

---

62 *TAPAC Report*, 37-38.

63 Electronic Privacy Information Center, "ChoicePoint," www.epic.org/privacy/choicepoint (accessed February 22, 2006).

Novak, K. Novak, or perhaps by a misspelling such as Neil Novak or Neil Knovak. Ensuring that personal information is matched to each potential rendering of a name is a challenge.

Another challenge is name changes. There are 2.3 million marriages and 1.1 million divorces annually, most of which result in name changes.[64] Databases must keep up with these name changes and ensure that all pertinent data fields are transferred from one name to the next.

An additional challenge is that many people share names. There are tens of thousands of John Smiths in the United States. Keeping straight which information goes with which John Smith is a difficulty.[65] Many individuals have multiple addresses and/or post office boxes. Additionally, according to the US Postal Service, seventeen percent of Americans (43 million people) change addresses every year. Keeping up with which address goes with which person poses a great challenge.

Finally, organizations record personal information in numerous different ways, in numerous different formats and on numerous different computer systems. The problem of information integration is difficult in the English language. The problem is exacerbated by the inclusion of foreign names and multiple aliases. This poses a great challenge to keeping accurate and up-to-date watchlists.

Cases of mistaken identity using watch lists based on name only matching has been documented in the press. A 2003 *USA Today* article highlights the travel difficulties encountered by individuals such as Greg Yasinitski and David Nelson who have the misfortune of having the same names as suspected terrorists.[66] Fortunately, these cases only involve traveling hassles, not something more serious like false imprisonment or loss of life. Nevertheless, an effective terrorism early warning system must minimize cases of mistaken identity.

---

64 National Center for Health Statistics, *NationalVital Statistics Reports* 51, no. 8 (May 19, 2003): 1, table a. As quoted in *TAPAC Report*, 37.

65 *TAPAC Report*, 37.

66 Editorial, "Glitches Repeatedly Delay Innocent Air Travelers," *USA Today*, June 25, 2003.

False positives, or identifying innocent people as potential terrorists when they are not, as a result of pattern matching in data algorithms is certain to occur.[67] In fact, the more sensitive an algorithm or process is, the more likely it is to generate false positives. Highly sensitive tests in medicine such as PSA tests for prostate cancer and pap smears for cervical cancer have high false positive rates. This has the benefit of low false negative rates (missing the cancer that is in fact present).[68] An early warning system reliant on pattern recognition or data-mining must compensate for false positives and establish clear guidelines for correcting the data or process that led to the erroneous alert.

To address the concerns highlighted above and establish privacy attributes that could be incorporated into a terrorism early warning system, it may be useful to consider two existing frameworks. The concepts underlying the Privacy Act have come to be known as "The Fair Information Practices" and are helpful in outlining a framework for privacy.

Another existing framework is the Organization for Economic Cooperation and Development's (OECD) Privacy Guidelines. These two frameworks can be used to guide the development of privacy features necessary in future information sharing, data-mining and surveillance technologies.

D. FAIR INFORMATION PRACTICES

A proposal to establish a government centralized repository of information on US citizens in 1965 invigorated debate that led to the passage of the Privacy Act of 1974. The principles known as "fair information practices" were first presented in a 1973 Department of Health, Education and Welfare report.[69] The Privacy Act emerged out of this report. Today these principles still enjoy wide consensus as an effective means to

---

67 Paul Rosenzweig, "Proposals for Implementing the Terrorism Information Awareness System," Heritage Foundation Legal Memorandum #8 (2003).

68 Jim Breckenridge, lecture, Naval Postgraduate School, Monterey, CA, October 4, 2005.

69 Daniel J. Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection v. 2.0", GWU Law School Public Law Research Paper No. 132, (April 25, 2005), available at http://ssrn.com/abstract=699701.

protect privacy. In fact, in recent times the Federal Trade Commission has sought to apply the fair information practices to internet commerce as a way to protect the privacy of consumers.[70]

1. Notice/Awareness

Notice or awareness refers to the necessity for data collectors to make users aware of the fact that they are collecting information and make them aware of their information practices. This includes what information they collect, how they collect it, how they use the information, whether or not they provide it to other parties, and how they provide for the other fair information practice principles in the handling of personal information. A modern representation of the notice principle is the ubiquitous use of a "privacy policy" link on web sites. Clicking on this link gives notice to the web site user of the site's policies regarding use of personal information.

Notice may be a difficult principle to apply in a national security context since it is generally disadvantageous to let an enemy know that you are collecting intelligence on them. However, in a domestic context it is important for the government and the governed to understand what information needs to be collected, the purpose for which it is being collected, why it is effective in fighting terrorism and any potential risk the collection poses to society. The principle of notice need not be applied to the collection of foreign intelligence, but domestic collections should be rigorously debated with full disclosure of how the information is used. Temptations to develop secret domestic intelligence gathering mechanisms should be avoided since their eventual disclosure (through a leak to the press of some other means) would likely cause a setback for both security and privacy.

2. Choice/Consent

Choice refers to the ability of the person whose information is being gathered to have a say in how their personal information is used. On the internet this is often seen in the form of check boxes at the bottom of a form requiring personal information. The check boxes may ask whether or not a person wants to be added to a mailing list, receive

70 "Privacy Online: Fair Information Practices in the Electronic Marketplace," Report to Congress, FTC May 2000.

e-mails regarding certain products or services or have their information released to a third party. These opt-in or opt-out constructs are common ways to provide for choice.

The idea of consent is not constrained to the internet. Consent operates in the law enforcement domain every day. A law enforcement official may legally search personal property (such as the trunk of a car) if consent is given. However, in the absence of consent an officer must establish probable cause to pursue a warrant to conduct the search. Miranda rights offer suspects certain choices such as "the right to remain silent." Sometimes suspects choose to waive this right and incriminate themselves, but it is important that they be given the choice.

Choice may, at first, seem to limit the government's ability to extract terrorist information. It may seem improbable that information concerning a terrorist act would be willfully surrendered, but it is certainly not unheard of for criminals to choose to confess to a crime or turn themselves in. The legal system allows for confession, but provides the avenue for the suspect to remain silent and force the burden of proof onto the government's evidence. A terrorism early warning system, since terrorism often presents itself as crime, should provide for a similar mechanism.

3. Access/Participation

Access from a consumer perspective means that a person should be able to view his own personal information held in a database and contest its accuracy. An example is the ability to request one's own credit report and address inaccuracies contained in the report with credit reporting agencies such as EquiFax, Experian or TransUnion. The Fair Credit and Reporting Act requires that adverse action (denial of credit or refusal to hire based on information in a credit report) be reported to the individual.[71]

4. Security/Integrity

Data collectors must take steps to ensure that the personal information they collect remains secure from unauthorized use. In the context of an ISE this should not only include security from outside threats such as hackers and identity thieves trying to gain access to personal information contained in the ISE, but also from insiders who have access to the system. In the national security environment, data security is also known as "Information Assurance."

[71] Solove and Hoofnagle, "A Model Regime of Privacy Protection (Version 1.1)."

5. Enforcement

Enforcement refers to the capability for government or self-regulating bodies to impose penalties or sanctions on those who fail to abide by fair information practices. In the information sharing and terrorist early warning context it is critical that privacy policy be enforceable. This enforcement should be a primary motive in developing the architecture and technologies that are part of the ISE. Technologies that could enable enforcement will be discussed later.

E. OECD PRIVACY GUIDELINES

OECD member countries recognized early on the need to protect the privacy of personal information in transborder trade. They understood that a country that failed to adequately protect information privacy could face trade sanctions. The member nations developed privacy guidelines to protect privacy, but they also developed them to avoid potentially more restrictive definitions of privacy that might restrict the flow of information required for trade. These principles are generally well accepted amongst privacy advocates worldwide.

1. Data Quality

Data quality simply refers to the need for data to be up-to-date and accurate. Additionally, the data should be relevant to the purpose for which it is to be used.

2. Purpose Specification

Purpose specification dictates that the purpose for which the data is collected should be articulated no later than the time of collection. Subsequent uses of the data should be compatible with the original specified purpose. If the data is to be used for another purpose, the additional purpose should be specified.

3. Use Limitation

The use limitation principle states that personal data should not be disclosed or made available for purposes other than those specified unless authorized by the data subject or by the authority of law.

4. Collection Limitation

The collection limitation principle states that personal information should be obtained via lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

5. Security Safeguards

The security safeguards principle requires that personal data should be reasonable protected against loss, unauthorized access, destruction, use, modification or disclosure of the data.

6. Openness

The openness principle states that "there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[72]

7. Individual Participation

This principle espouses the belief that individuals should have the right to know what information a data holder possesses related to him. The individual should be able to gain access to what information a data holder has within a reasonable time, at a charge that is not excessive, in a reasonable manner and in a form that is intelligible to him. Additionally, the person should be given a reason if a request for information is denied and should have opportunity to challenge the denial. If the individual discovers that the data holder has inaccurate data, he should be able to challenge and have the information erased, rectified, completed or amended as necessary.

8. Accountability

Accountability is similar to the fair information practice of enforcement. Data holders should be held accountable to abide by the principles and implement measures or technology to ensure the ability to comply.

F. PRIVACY MATRIX

Using the fair information practices and the OECD guidelines as guiding principles for privacy, it is possible to represent them in a matrix. This "right hand side" of the matrix articulates the privacy requirements that should be considered when developing the architecture and technologies necessary in a terrorism early warning

---

72 Organisation for Economic Co-Operation and Development (OECD), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed February 6, 2006).

system. These principles, since they are widely accepted by privacy advocates in the United States and international community, provide an aiming point that would likely gain bipartisan consensus in Congress.

Adding the "right hand side" of the matrix to the "left hand side" results in a matrix than can be used to guide the development of an architecture which considers both information sharing and privacy requirements. Figure 9 displays this resultant matrix.

	SECURITY / INFORMATION SHARING					PRIVACY	
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356	FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies	Notice/Awareness	Data Quality
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC	Choice/Consent	Purpose Specification
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination	Access/Participation	Use Limitation
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards	Security/Data Integrity	Collection Limitation
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information	Enforcement	Security Safeguards
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods		Openness
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security	Match data access to roles and responsibilities of oranizations engaged in countering terrorism	Produce multiple versions (security classifications) of information		Individual Participation
			Facilitate oversight through use of audit trails, user authentication and access controls				Accountability

Figure 9. A Privacy and Security Reference Matrix

Having described the attributes the government says it must have to detect indications and warnings of terrorism and discussed principles which could help ensure Americans' privacy is maintained within the system, attention can be turned to technologies which might further the advancement of both security and privacy.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TECHNOLOGIES THAT COULD ADDRESS BOTH SECURITY AND PRIVACY

With the matrix developed, it is possible to investigate some existing or near-term technologies that might be able to meet some of the requirements from one or both sides of the matrix. This chapter, while not an exhaustive listing of technologies that could be used, shows how technological innovation could facilitate an architecture designed to meet security needs, provide for Americans' privacy and protect against a too-powerful government.

A. AN INFORMATION MANAGEMENT PROBLEM

In many cases, counterterrorism analysts and operators do not want more information as it could lead to information overload. Rather, they want the right information with enough accuracy and fidelity to do something with it. Stated another way, having unfettered access to all Americans' information is not desired. Having access to relevant, actionable terrorism information is the desire.

A primary concern for privacy advocates is innocent people being judged falsely or out of context or having constitutionally protected activities scrutinized. Essentially they are concerned about government having the right information too, as articulated in the previous chapter. In this regard, security and privacy share a common goal: get the right information (indications and warnings of terrorism) and filter out all irrelevant or unnecessary information. This requires an unprecedented capability to carefully manage information.

B. AN INFORMATION MANAGEMENT SOLUTION

Fortunately, the ability to manage information has exploded over the last several decades. Even in the last year, innovations such as Really Simple Syndication (RSS) and Podcasting have proliferated on the internet. RSS has even been introduced on classified intranets such as Intelink.

Yet, the policy which governs the way intelligence and information sharing are conducted in the United States has largely failed to take advantage of the information revolution. The policies have not taken advantage of technology's vast capabilities to better manage information and, as a result, curb the abuse of information.

It seems government has made ample use of technology as a means to collect more information, but has chosen to rely solely on policy as a means to control information regarding US citizens. Perhaps this is due to the fact that during the Cold War the only threats perceived to be capable of destroying the nation were outside of our borders, therefore the need to collect information inside the borders was so infrequent that law and policy alone could sufficiently handle the problem. Now that it has been shown that a strategic attack against the country can originate from inside our borders, a greater need to be able to conduct domestic intelligence activities may force an information management solution—one that is guided by clear policy and enforced through code or technical means.

It is ironic that the initial investment and development work that resulted in the Internet was a government initiative at Defense Advanced Research Projects Agency (DARPA). The irony lies in the fact that the internet has revolutionized the way information is shared and managed and yet one of the significant government failures to prevent 9/11 was an inability to share information across the government or "connect the dots."[73]

This failure led to reform in the Intelligence Community,[74] the work of the Markle Foundation and significant investigation of what would constitute a Trusted Information Network,[75] the delivery of several Executive Orders dealing with information sharing[76] and new legislation governing how the law enforcement and intelligence communities should interact. Despite these efforts, there is still not a great deal of national consensus on how to go about responding to terrorism while maintaining privacy and fundamental liberties. There is still great division among government agencies trying to combat terrorism and privacy advocates who wield great power in

73 *The 9/11 Commission Report*.

74 *Intelligence Reform and Terrorism Prevention Act of 2004.*

75 Zoe Baird and James L. Barksdale, co-chairmen, "Creating a Trusted Network for Homeland Security." *Second Report of the Markle Foundation Task Force on National Security in the Information Age* (New York: The Markle Foundation, 2003).

76 U.S. President, *Executive Order,* "Strengthening the Sharing of Terrorism Information to Protect Americans."

influencing congressional support of tools intended to aid the "war on terrorism."[77] For this reason, the technology government develops to further improve information sharing must dually serve security and enhance privacy protections in a real way.

The remainder of this chapter focuses on near-term technologies that can impact security and privacy. Each technology discussed will reference the Privacy and Security Reference Matrix developed in the previous chapters, highlighting the attributes from either side of the matrix the particular technology may be able to accommodate.

C. TECHNOLOGIES THAT SERVE BOTH PRIVACY AND SECURITY

1. General Attributes of Privacy and Security Enhancing Technologies

There are several general attributes a network must possess in order to accomplish the goal of simultaneously enhancing information sharing and protecting the privacy and Constitutionally-protected rights of Americans.

a. Access Control

The network must ensure that only people with counterterrorism, homeland defense and homeland security responsibilities can access the information contained within the network. The network must be secure and require some form of authentication to access it.

b. User Type Identification

The network must further be able to differentiate between different types of users in order to determine what users are allowed to see what data. For example, under current guidance established in EO 12333 and DoD 5240.1-R it would be inappropriate for an intelligence analyst at NORTHCOM to have access to the name, social security number, address and phone number of a USPERSON unless a terrorism nexus has already been established.[78] A military analyst may, however, benefit from being able to see anonymized transactions the USPERSON is engaged in and be able to add a puzzle piece from foreign intelligence that may disrupt a terrorist plot before it reaches the execution phase. User type identification would recognize the user as a military analyst and provide only de-identified data (data that does not allow the analyst

[77] For example the Privacy Lobbyists efforts led directly to the Congress's cancellation of programs such as TIPS, TIA and CAPPS II.

[78] Christopher Thornlow, "Fusing Intelligence With Law Enforcement Information: An Analytic Imperative" (master's thesis, Naval Postgraduate School, 2005).

to determine the identity of the subject yet provide all information regarding the person's suspicious activity allowing the military analyst to look for terrorism ties). The point of user type identification is to control what information a particular user may access and what he may do with the information once he has accessed it (save a copy, print, share with another agency, etc.) This provides users access at the data level rather than the system level—an attribute called for in IRTPA and reflected in the matrix.

c. Audit Trails

Another attribute of an information sharing network should be the capability to produce immutable and non-repudiable audit trails. In other words, the network should keep track of the information that users access and what they do with the information. These audit trails would be key to effective oversight and accountability. Policy must clearly dictate who reviews the audit trails and what action should be taken if they reveal impropriety.

d. Decentralized Information

The information available within the network should not be stored in a central database nor controlled by a central information broker. The network should pull from existing (legacy) databases that various organizations already possess and enable individual analysts to search for the information they need across the multiple data repositories (assuming they have the right credentials to access the information). If information is power, decentralizing the information effectively decentralizes power. This may serve to alleviate some of the fear associated with one organization gaining too much power.

e. Near Real-Time Operations

The network must have sufficient capacity and data rates to support dissemination, collaboration and communication among users in near real-time.[79] Some information may be deemed only suitable to be shared during an ongoing terrorism operation (e.g. information that could be used to mount a military response to an attack in progress). This could serve privacy by allowing certain sensitive data only to be sent to certain agencies as needed. Additionally, access to certain information could be unavailable in an archived format or be set with accesses that expire after a certain period

[79] *Second Report of the Markle Foundation Task Force on National Security in the Information Age.*

of time. This would preclude certain users' ability to archive or analyze this data, yet provide a means for the government to respond if necessary.

2. A Model of Technologies Acting with Synergy

Many of these attributes are captured in a model known as the "Policy Appliance Reference Model developed by Mr. K. A. Taipale from the Center for Advanced Studies in Science and Technology Policy. Mr. Taipale's model offers a nice skeleton to narrow an investigation of the types of technologies that might prove useful in an information sharing network which protects the privacy and civil liberties of Americans. The two figures below describe the model.[80]

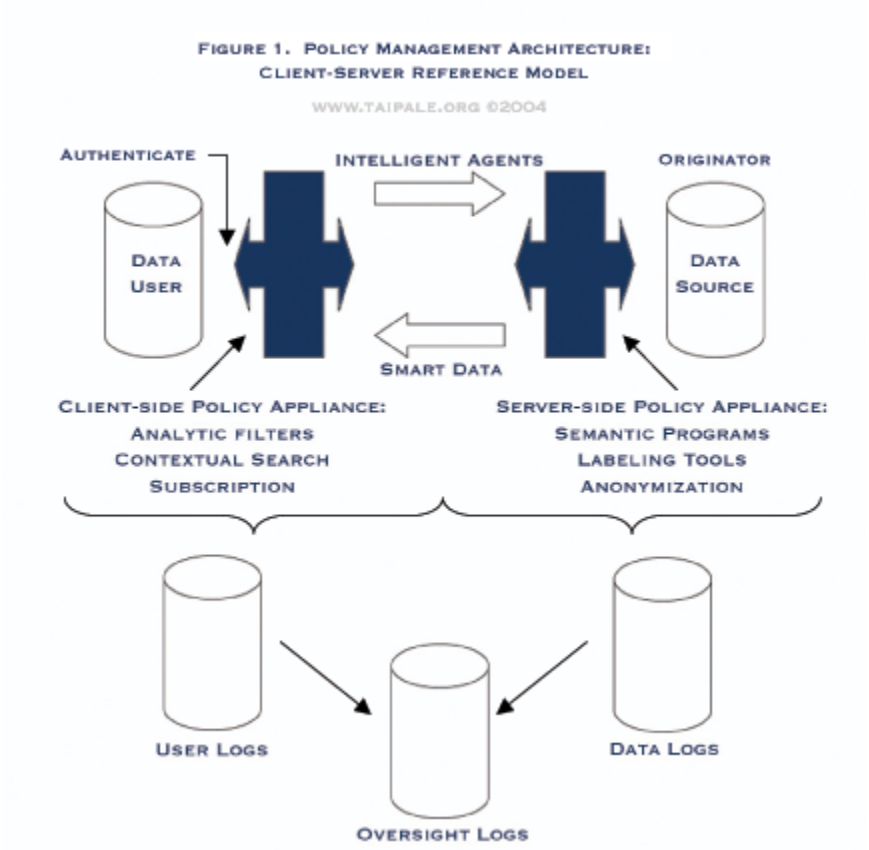

Figure 10. POLICY MANAGEMENT ARCHITECTURE: Client-Server Reference Model. An *enterprise architecture* reference model for *knowledge management* (an information product approach) that includes *policy appliances* (technical control mechanisms to enforce policy rules and ensure accountability) interacting with *smart data* (data that carries with it contextual relevant terms for its own use) and *intelligent agents* (queries that are self-credentialed, authenticating, or contextually adaptive).

80 K. A. Taipale, "Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties," Chapter 9.4 in *Emergent Information Technologies and Enabling Policies for Counter Terrorism*, ed. Robert Popp and John Yens (Hoboken, N.J.: Wiley-IEEE Press, forthcoming 2006), 1.

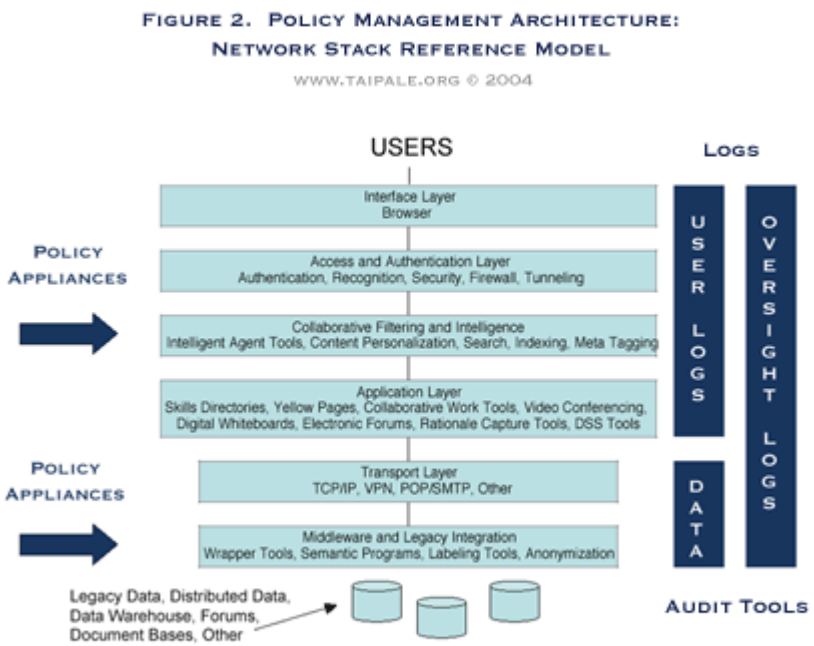

Figure 11. POLICY MANAGEMENT ARCHITECTURE: Network Reference Model. An *enterprise architecture* reference model showing *policy appliances* (technical control mechanisms to enforce policy rules) and *logging functions* (to record and audit for accountability) in network stack relationship.

With these attributes and models as a frame of reference, it is possible to propose some specific existing or emerging technologies that could be used and how they might serve both the privacy of citizens and the needs of those tasked with keeping the nation secure.

3. Specific Technologies

a. Access Control and Authentication

The Defense Department's (DoD) Common Access Card (CAC) serves as the new identification card as well as a means for physical (to buildings) and logical access (to DoD computer systems). The CAC card combines smart card and Public Key

Infrastructure (PKI) technologies and will eventually replace username and password as the means to access computer systems. Some form of this could be used to control access to an information sharing network.

(1) Smart Card. The DoD CAC card is a form of smart card which contains information within a gold token embedded on the card and a magnetic stripe on the back of the card. A biometric (left and right index fingerprint) is collected at the time the cards are issued, but the biometric is not stored within the card. Currently, the biometric is only used when a card needs to be reissued to verify the identity of the person receiving the new card. When a user inserts the card into a card reader at his computer he is prompted for a six to eight digit pin number. Upon successfully entering the pin number, the user is able to access the computer network. The requirement to both have the smart card and know the pin number provides good access control.

(2) PKI. The gold chip embedded in the card contains a digital certificate which establishes the card user's identity and contains PKI encryption and authentication keys. DoD uses the PKI to enable CAC card holders to digitally sign e-mail and access encrypted web sites. The most common use of the PKI is the emergent Defense Travel System (DTS).

DTS, now in use at select military installations is the latest means for military members to create travel orders, make travel arrangements and file travel vouchers. PKI encryption allows the user to securely exchange personal information (including government credit card and personal bank account numbers) with the DTS site. The digital signatures included with PKI also provide non-repudiation. Once a member makes a reservation or signs a travel voucher, he cannot deny doing so.

Within DTS there are different levels of users. A "traveler" only has access to his own information. An "approval authority" can see all of the "travelers" she is responsible for within the organization. This person usually has responsibility for the travel budget and needs to be able to see certain information and take certain actions that a "traveler" does not. Further, the "CTO" or travel agent who is responsible for the actual booking of flights and rental cars needs to be able to see a different set of data and use different functions. The accessible data and available functions are all controlled by the person's identity which is authenticated through the "gold chip."

(3) Disadvantages of Applying to an Information Sharing Network. One of the major disadvantages of using a technology similar to CAC to control access would be the logistics of issuing a card to every user. DoD currently issues approximately 10,000 cards per day at approximately 1300 sites. At the present time, more than five million cards have been issued. These are impressive numbers, but it has taken years to reach these levels. The CAC card distribution was made simpler for DoD by virtue of the fact that they leveraged existing personnel databases such as the Defense Eligibility Enrollment Reporting System (DEERS) and the Real-Time Automated Personnel Identification System (RAPIDS). Though all of the necessary personnel information existed in the databases, the databases needed to be redesigned to allow the CAC cards to be issued through the RAPIDS software. The database redesign included PKI certificate management, Java Card applications and SSL client/server software. Additionally, hardware such as smart card encoders and readers, card printers, fingerprint pads, and personal identification number pads were introduced to be able to produce and issue the cards.[81]

Proliferating this technology to non-DoD federal workers plus state and local agencies (any person or agency with a need to share terrorism information) may prove challenging if they do not have existing personnel databases that can readily be modified to issue the cards. Additionally, it may not be cost effective to supply every agency with the equipment and training necessary to accommodate decentralized distribution of the cards.

(4) Security Benefits of Applying to an Information Sharing Network. Despite challenges which may arise in distributing the cards, a CAC card or equivalent technology could work well for controlling access to the information sharing network. Without a card and pin number (and potentially biometric identifier) a person attempting to access the network would not be able to.

In addition to controlling access at the system level, the card would satisfy the need to be able to establish the person's identity and organization for the purposes of controlling what information and functionality is available to that specific

[81] Global Platform, DoD Case Study, "Common Access Cards—Expanding the Functionality of ID Cards for the US Department of Defense," http://www.globalplatform.org/fcs/DOD_Case_Study.pdf (accessed July 10, 2005).

user. This function would enable meeting IRTPA's requirement to control access to data, not just systems and allow information to be displayed for DoD users in accordance with EO 12333 and DoD 5240.1-R. The users card could also indicate his level of security clearance, making it possible for the system to control access across multiple security levels.

An additional advantage of each user of the network using PKI is that e-mail or chat traffic between counterterrorism analysts at separate agencies could be encrypted and digitally signed giving a level of confidence that the person on the other end in fact is who he claims to be and works for the agency he claims to work for. In essence, any information sharing network must first have the trust of its users. Use of smart cards and PKI could provide this trust, enabling the establishment of an intelligence "cyber community," extending access to anyone with a card including state, local and tribal agencies and formatting the information for the particular user in accordance with guiding policy and directives.

(5) Privacy Benefits of Applying to an Information Sharing Network. The requirement for data security is one of the fair information practices. Privacy expert, and law professor Daniel Solove articulates this principle well. "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data."[82] The principle of security is also specifically mentioned in numerous statutory laws intended to guard privacy. Some examples include the Privacy Act, the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act which deals with the privacy of financial transaction, the Health Insurance Portability and Accountability Act of 1996, and the Computer Fraud and Abuse Act which is intended to prevent computer hacking.

Data security is also one of the OECD guidelines. Security of data is important to privacy because of the risk to unauthorized disclosure either within the government to an individual or agency who may use the information for an unauthorized purpose or to someone outside the government, for example an identity thief or hacker.

---

[82] Solove, "A Taxonomy of Privacy," 28.

Smart card and PKI technology are accepted as a means to protect computer networks, and would likely be an acceptable means to fulfill the data security principles. Additionally, smart card and PKI technologies would serve as enabling technologies to building audit trails and oversight mechanisms, providing accountability for how information is used and, by extension, ensuring it is used for the purpose specified Together, smart card and PKI technologies have the potential to meet or enable the matrix attributes highlighted in Figure 12.

	SECURITY / INFORMATION SHARING					PRIVACY	
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356	FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies	Notice/Awareness	Data Quality
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC	Choice/Consent	Purpose Specification
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination	Access/Participation	Use Limitation
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards	Security/Data Integrity	Collection Limitation
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information	Enforcement	Security Safeguards
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods		Openness
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security		Produce multiple versions (security classifications) of information		Individual Participation
			Facilitate oversight through use of audit trails, user authentication and access controls				Accountability

Figure 12. Attributes that could be met or enabled by PKI and Smart Card technologies as a means for authentication and access control

b. Semantic Web Technologies

While the semantic web as a whole is not a reality today, many of its foundational technologies do exist and could be used to exchange information in a way that serves security, privacy and civil liberties. Tim Berners-Lee describes the Semantic Web as "an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation."[83]

The power of semantic web to an information sharing network is best described by the World Wide Web Consortium's (W3C) web site: "The Semantic Web

83 Tim Berners-Lee, James Handler, Ora Lassila, "The Semantic Web," *Scientific American*, May 17, 2001. http://www.scientificamerican.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21&catID=2 (accessed July 2, 2005).

provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries."[84] Given that an information sharing system would link numerous agencies running different software applications on different networks, the power to share and reuse data across applications, enterprise and community boundaries is exactly what is needed.

The goal of Semantic Web is to have data defined and linked on the web in a way that it can be automated, integrated and reused on many applications—not just displayed. The net effect of these technologies operating across a terrorism early warning system would be reducing the amount of time analysts spend searching for information related to the particular intelligence problem they are trying to solve, offering an improved analysis capability. Much of the searching would be turned over to the computer or intelligent agents working on the analysts behalf. "The Semantic Web will bring structure to the meaningful content of web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users."[85] An effect of this is that human analysts would spend less time combing and sifting through irrelevant information thereby lowering the probability of that analyst's exposure to information forbidden by law or policy.

(1) eXtensible Markup Language (XML). XML provides the syntax, or rules, for how data should be labeled. The basic function of the XML language is to provide tags to data that describe what the data mean. For example a number might have a tag which tells whether the number is a zip code, phone number, date or price.[86] XML standardizes the way data is described, making it possible for multiple parties (or multiple software programs) to understand what the data is. XML data tags can then be used by scripts or programs in sophisticated ways.

(2) Resource Data Framework (RDF). RDF goes beyond describing what data mean and describe the relationships between the data. RDF revolves around the idea that things being described have properties which, in turn have

---

84 Frank Manola and Eric Miller, "RDF Primer 2004," http://www.w3.org/TR/rdf-primer/ (accessed June 26, 2005).

85 Berners-Lee, "The Semantic Web."

86 Kenneth C. Laudon and Jane P. Laudon, *Essentials of Management Information Systems* (Upper Saddle River, NJ: Prentice Hall Publishers, 2005), 212.

values. Resources can then be described by making statements identifying the properties and values. A simple example might help clarify. Consider the following statement:

This thesis has an **author** whose name (value) is **Kneil Novak**

This statement has a subject (This thesis), a predicate (author) and an object (Kneil Novak). The subject is the thing the statement is about, the predicate is the property or characteristic the statement is about and the object specifies the value of that property or characteristic.

Of course a computer could not read and understand the english statement above. In order to make statements machine-readable, RDF uses Uniform Resource Identifiers (URIs) to specifically identify a subject, predicate or object. This is particularly useful because it enables machines to distinguish between things that have the same name. For example, if a person named Muhammad Atta were on a terrorism watch list he might have a specific URI assigned to him. The "bad" Muhammad Atta could be distinguished from other Muhammad Attas who would have different URIs assigned to them. One can see how this would enable better data search mechanisms using technology such as intelligent agents.

An analyst working on Muhammad Atta would be able to have an intelligent agent roaming other agencies databases for information on the Muhammad Atta of interest and not waste time combing through mounds of information concerning every Muhammad Atta in the world.

One can also see how RDF could potentially protect innocent people from being confused with terror suspects or prevent any inclination to round up all the Muhammad Attas "just in case."

(3) Web Ontology Language (OWL). In order to have effective information sharing, searches that cross multiple, decentralized databases must be able to recognize when two different databases identify the same concept in a slightly different way. Stated another way, computers must be able to recognize similar concepts across multiple databases. Ontologies are the way to accomplish this.

Internet and artificial intelligence researchers and developers use the term ontology to describe a document or file that formally defines relationships among terms.[87] Two important concepts related to ontologies are taxonomies and inference rules.

Taxonomies provide a way to describe classes of objects and subclasses within them. A simple example is the taxonomy most people learned in high school biology. Humans, or the species homo-sapiens, are part of the larger class of mammals.

Inference rules describe associations. For example, we also know from high school biology that animals that have hair and nurse their young are mammals. Since humans have hair and nurse their young, they must be mammals.

Ontologies have the potential to enable information sharing in multiple ways. First, they have the ability to enable more accurate search mechanisms by searching for precise information and eliminating ambiguity. For example analysts could search for the Muhammad Atta who holds a German passport, enrolled at a flight school somewhere in Florida versus performing a general search on the name Muhammad Atta. These searches need not be constrained to single web pages or single databases rather they can cross multiple databases. For example the search might touch an Immigration and Customs database when searching for the passport information, a Federal Aviation Administration database when looking for flight school records and a Florida Department of Motor Vehicles database to establish the presence in Florida.

The capability to search across databases adds a level of complexity since databases may not refer to data fields in exactly the same way. For example one database might use slightly different terminology in referring to the same concept. In order for machines to "talk" more effectively, there needs to be a common standard. OWL provides this standard.

OWL is a specific language, recommended by W3C used to describe ontologies. Since W3C recommendations generally have the weight of international policies or standards when it comes to web development, it is likely that OWL will become as widespread as html or XML in the future.

---

[87] Berners-Lee, "The Semantic Web."

(4) Disadvantages of Using Semantic Web technologies. The primary disadvantage of using semantic web technologies is that they are still relatively new. Although the use of XML is quickly growing on the internet, most legacy government databases are not likely tagged with XML. This means that there would need to be a significant amount of effort to attach the XML tags or build the meta data to make information sharing and privacy protection a reality.

Another difficulty is found in the ability to market the effectiveness of these technologies as a means to protect t privacy. These technologies are relatively complex and sometimes difficult for people without a technical background to understand.

If information sharing is ever going to happen, the public is going to have to be reassured that the privacy and civil liberty protection built into the architecture is for real and not just a farce. Explaining semantic web technologies before they are widely proliferated could be a challenge. People might not be willing to trust a system based on technology they do not understand. As a result, government may not be able to rally the support they need to make such a system successful.

(5) Security Advantages of Using Semantic Web Technologies. A key advantage to using these technologies is the ability to cross application, enterprise and community boundaries. This is important because it does not rely on one proprietary system or method to search for and/or display information. The DoD, FBI, CIA, and state and local agencies can keep their own databases and use displays that their people are trained on and familiar with—they just need to be able to "pull in" and "push out" the appropriate data. These tools have the potential to open the door for meaningful analysis to be conducted by machines. This will transform the way agencies work together to gain knowledge and solve difficult problems. Finally, semantic web technologies, in conjunction with smart cards and PKI will make it possible for information to be put into the right hands at the right time, in the right format and for legitimate purposes.

(6) Privacy Advantages of Using Semantic Web Technologies. An advantage of using Semantic Web technologies to privacy is that much of the searching and sifting of information will be automated and carried out by intelligent agents rather than humans putting eyes on private information. This alone should

alleviate some concerns that the government is collecting and storing information regarding groups and activities that are protected under the constitution.

Semantic Web technologies enable searches to be conducted across decentralized databases alleviating the need for a centralized government database. This decentralization not only increases the analytical power necessary to identify indications and warnings of terrorism, it effectively "federates" the power of the government.

The use of semantic web technologies can significantly improve data quality using XML. XML tags attach meta data (data about data), lending more specificity to the information. URIs could help drastically improve watchlists by enabling the capability to tell the difference between the Ted Kennedy who is a terrorist and the one who is a Senator.

A great benefit to the use of semantic web technologies is the ability to customize the display of information for various users. Used in conjunction with smart card and PKI technologies (identifying the user and his agency) semantic web technologies can enable the display of select fields of data from a database. This has the potential to enable foreign intelligence analysts to access domestic databases, but view it in a way that is devoid of personal information (i.e. analyze transactions or behavior without knowing who the person is carrying out the transaction or behavior).

Finally, semantic web technologies are another key enabler to generating detailed audit logs. These audit logs, in the hands of a responsible oversight body, give credibility to the capability to enforce privacy standards and provide accountability.

In summary, semantic web technologies could likely meet or enable the attributes highlighted in Figure 13.

	SECURITY / INFORMATION SHARING					PRIVACY	
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356	FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies	Notice/Awareness	Data Quality
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC	Choice/Consent	Purpose Specification
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination	Access/Participation	Use Limitation
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards	Security/Data Integrity	Collection Limitation
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information	Enforcement	Security Safeguards
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods		Openness
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security		Produce multiple versions (security classifications) of information		Individual Participation
			Facilitate oversight through use of audit trails, user authentication and access controls				Accountability

Figure 13. Attributes that could be met or enabled by the use of semantic web technologies

c. Anonymization and Pseudonymization

Anonymization refers to the capability to strip personal identifiers from other important information. The medical field seems to be leading the way in the development of anonymization techniques.

Doctors and medical researchers have a need to be able to share information to prevent and find cures to disease. Epidemiologists and public health professionals need ways to detect the outbreak of a communicable disease and curb its spread. To respect the privacy of their patients, the medical community is working on ways to share this information without identifying individual patients. To achieve the ends they seek, the patient's identity is not needed or even desirable to conduct research and respond to disease.

One medical study showed that a technique known as cell suppression was successful at removing personal data, yet allowed the information to be useful in predictive analysis.[88]

Another anonymization method used in the medical field is a technique known as one way hashing. One way hashing exchanges actual data for a cryptic code.

88 Lucila Ohno-Machado, M.D., Ph.D; Staal Vinterbo, Ph.D; Stephan Dreiseitl, Ph.D; "Effects of Data Anonymization by Cell Suppression on Descriptive Statistics and Predictive Modeling Performance," *Journal of the American Medical Informatics Association*, November/December 2002 http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=419433&blobtype=pdf (accessed June 29, 2005).

In our context one way hashing could be applied to names on a no-fly list to generate a list of codes. The same hashing technique could then be applied to airline manifest. This would result in the cryptic codes being compared rather than actual names. If the two codes matched, the actual name could be released to an appropriate authority. Without a match no personally identifying information would be viewed.[89]

Another anonymization technique is known as k-anonymity. k-anonymity provides a means to release a dataset in which the included information is incapable of being traced or matched to a specific individual about whom the data concerns. This provides de-identified data, but maintains the utility of the data.[90] In our context k-anonymity would allow domestic intelligence analysts the ability to push de-identified information to foreign intelligence analysts without having to reveal personal information. This could be particularly powerful in linking domestic transactions or behavior to known terrorists overseas. The benefit is that in the event no terrorism nexus were revealed, foreign intelligence analysts would not have been exposed to USPERSON data.

Pseudonymization refers to representing personally identifying information by pseudonym. A simple example of pseudomymization is the use of screen names in chat rooms, blog sites, at online auction sites such as E-Bay, or when writing a book review at Amazon.com. The use of pseudonyms is a commonplace practice in trying to preserve privacy on the internet.

Anonymization and pseudonymization techniques are gaining acceptance as a means to protect privacy. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule sets forth rules governing the sharing of healthcare information. The summary of the Privacy Rule spans twenty-five pages. However, the rule specifically states, "there are no restrictions on the use or disclosure of de-identified health information." This speaks volumes to the privacy protection that the healthcare community believes anonymization techniques provide.

---

[89] James X. Dempsey and Paul Rosenzweig, Heritage Foundation, "Technologies That Can Protect Privacy as Information is Shared to Combat Terrorism," May 2004, 1-2 http://www.heritage.org/Research/HomelandDefense/lm11.cfm (accessed February 22, 2006).

[90] Latanya Sweeney, "k-anonymity: A Model for Protecting Privacy," International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10 (5) 2002: 557-570.

(1) Security Advantages of Using Anonymization/ Pseudonymization. Many of the analysis functions required to improve security can be accomplished with using anonymized data including pattern matching and data mining.[91] This may enable state, local and tribal law enforcement agencies to share information with the intelligence community in unprecedented ways enabling greater analysis of "new observables" and the ability to link overseas and domestic transactions that may be precursors to a terrorist strike.

The removal of personally identifying information in general meets the need to share information with the DoD community in a way that is consistent with EO 12333 and DoD 5240.1-R while enabling DoD analysts access to transactional data. This would allow DoD analysts to participate in the search for aberrant patterns without having the capability to know who is participating in the activity. This fact essentially makes the "wall" between domestic and foreign intelligence analysts largely irrelevant. Finally, the use of anonymized data would allow information to be integrated, analyzed and disseminated much more widely.

(2) Privacy Advantages of Using Anonymization/ Pseudonymization. The removal of personal information from data sets or the release of data sets that make it impossible to re-identify the person the data regards offers a great benefit in the protection of privacy. Since the privacy principles are intended to govern the use of personal information, the use of anonymous data may offer a "work around" to adhering to privacy principles. This has the potential to make the principles of notice/awareness and choice/consent irrelevant. More research is needed to support this assertion.

In summary, anonymization and pseudonymization techniques may be able to support, enable or provide a work around to the attributes highlighted in Figure 14.

---

[91] K.A. Taipale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd," *Yale Journal of Law and Technology* 7, no. 123 (December 2004), 182. *available at* http://ssrn.com/abstract=601421 (accessed December 15, 2005).

	SECURITY / INFORMATION SHARING					PRIVACY	
DESIRED ATTRIBUTES	NATIONAL HOMELAND SECURITY STRATEGY	NATIONAL STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT	IRTPA OF 2004	NATIONAL INTELLIGENCE STRATEGY	EXECUTIVE ORDERS 13354 - 13356	FAIR INFORMATION PRACTICES	OECD PRIVACY GUIDELINES
	Improve analysis capability	Establish capable and agile intelligence architecture	Share terrorism information among federal, state, local, tribal governments and private sector	Remove the "wall" between law enforcement and foreign intelligence	Share information among federal, state and local agencies	Notice/Awareness	Data Quality
	Access information wherever it resides	Enable data fusion	Connect existing information systems	Enable those outside the intelligence community to access information	Make information available to NCTC	Choice/Consent	Purpose Specification
	Improve HUMINT	Analyze aberrant patterns or activity	Ensure direct and continuous online electronic access to information	Incorporate open source intelligence	Make data available for integration, analysis and dissemination	Access/Participation	Use Limitation
	Collect and analyze "new observables"	Improve analysis capability	Facilitate analysis of information	Connect all intelligence community components as well as state, local, tribal governments and the private sector	Establish common security and access standards	Security/Data Integrity	Collection Limitation
	Map indications and warning of terrorist attack to critical infrastructure vulnerabilities	Extract/display sensor data in a format in accordance with EO 12333 and DoD 5240.1-R	Build upon existing government information systems	Ensure the intelligence community and its customers can access information when they need it	Establish standards that facilitate automated sharing of information	Enforcement	Security Safeguards
	Identify transactions which precede attack	Share situational awareness with federal, state, local and tribal governments and private sector	Control access to data, not just systems	Create an intelligence "cyber community"	Protect sources and methods		Openness
	Link law enforcement and foreign intelligence		Facilitate information sharing across multiple levels of security		Produce multiple versions (security classifications) of information		Individual Participation
			Facilitate oversight through use of audit trails, user authentication and access controls				Accountability

Figure 14. Attributes that could be met, enabled or deemed irrelevant by using anonymization/ pseudonymization technologies

While not all attributes in the matrix are addressed by the technologies discussed in this chapter, it should be apparent that the use of technology has the potential to meet attributes on both the security and privacy sides of the matrix. Hopefully, it is also apparent that privacy and security need not be considered rivals within the context of a terrorism early warning system. Additional research and technological advancements are likely to yield even more opportunities to expand both security and privacy improving analysts' and operators' ability to keep the nation safe from terrorism and protecting American's rights to engage in protected activities.

THIS PAGE INTENTIONALLY LEFT BLANK

V. POLICY AND ORGANIZATIONAL INNOVATIONS

While technological innovations have the potential to radically change the calculus of the relationship between security and privacy, the entirety of the problem cannot be solved by technology alone. Policy and technology must be married in a symbiotic relationship with the overarching goal of establishing a terrorism early warning system that values security and privacy. In this relationship, one should give energy to the other. For example, a particular technological innovation may enable a policy to be more enforceable or the advent of a particularly innovative policy option may spawn research into the technology to make the policy more feasible. The point is that policy and technology should always be considered jointly, not irrespective of each other. This requires collaboration between technologists, privacy advocates, analysts, operators and policy and lawmakers. One way to encourage this collaboration is through the establishment of privacy and civil liberties officers within agencies with counterterrorism responsibilities.

A. INSTITUTING PRIVACY AND CIVIL LIBERTY OFFICERS

Numerous efforts are underway that could provide a solid foundation to build an early warning system or ISE cognizant of privacy and civil liberty concerns. One effort, signed into law in section 1061 of IRTPA, establishes the Privacy and Civil Liberties Oversight Board. This board, appointed by the President, is to serve as the principal watchdog in ensuring citizens' rights and privacy are not violated by domestic intelligence gathering. Furthermore, Section 1062 of the law states, "It is the sense of Congress that each executive department or agency with law enforcement or antiterrorism functions should designate a privacy and civil liberties officer."[92] This "sense of Congress" is worth building upon.

Appointing talented leaders within agencies responsible for homeland defense and security as Privacy and Civil Liberties Officers (PCLOs) would pave the way to establish a system capable of protecting privacy. It is not enough, however, to simply appoint PCLOs for the sake of having them. An effective strategy must establish what PCLOs should do once they are appointed. An effective strategy must also provide a structure or

92 *Intelligence Reform and Terrorism Prevention Act of 2004*, 47-48.

framework in which they can operate and define their role and level of influence. The goal of the strategy should be to provide opportunities for PCLOs to learn about the importance of civil liberties then insert them into the corporate processes which acquire, develop, and transition new surveillance and information sharing systems to operations. Furthermore, PCLOs should be given the opportunity to network with other agencies' PCLOs and the Privacy and the President's Civil Liberties Oversight Board.

Finding the right people to be PCLOs is critically important. PCLOs should be selected from talented mid-level engineers, acquirers, system operators, investigators, action officers, or intelligence analysts. They should be respected as stars or rising stars in their fields and possess the capability to articulate complex thoughts in a pressure environment. They should not be easily intimidated by rank or authority, but should have the utmost respect for those in positions of authority. PCLOs should not be lawyers themselves, though they should strive to develop a relationship with their agency's lawyers (or office of general counsel) and feel comfortable seeking their advice. PCLOs should not be senior decision makers within their organization, but they should be able to command their attention and feel comfortable working with them.

The person best suited to be a PCLO is not the person who would sit in the back of a meeting and say, "you can't do that," and offer no suggestion to a workable solution. PCLOs should be the type of people who can sit in a relatively technical meeting and say, "if we design the architecture or system in this way, we might be able to minimize the likelihood that the information could be abused." They should not be required to come up with technical solutions on their own, but they must be able to identify opportunities to build safeguards or accountability into the system being designed, acquired or used. Finally, PCLOs should be selected from willing candidates. The duty of PCLO should be recognized as being significant and not dumped on some unwilling person as another additional duty. In order to encourage people within an agency to take on this duty, the position should be rewarding and attractive. It can be made attractive through the opportunity to travel and engage in exciting training and unique responsibilities.

1. PCLO Training and Responsibilities

PCLOs should receive training on a quarterly or perhaps semiannual basis. Since the PCLOs would be selected from experts in their respective fields, the initial training sessions should focus on the role of civil liberties in the United States.

The first topic PCLOs should be educated (or perhaps re-educated) on is our founding documents and the founding fathers' views on liberty. Studying documents such as the Declaration of Independence, the Constitution and the Federalist Papers would remind PCLOs of the significance liberty plays in America. A noteworthy instructor could teach this at an inspiring location such as Philadelphia or Williamsburg, Virginia. Studying America's past would undoubtedly stir the PCLOs to make wise decisions regarding liberty in its future. Understanding what American activities are legitimate and protected would enable the PCLOs to influence the design of a system that would not store or abuse data concerning those activities.

Having studied the founding documents, it would then be useful to receive training on judicial processes and specific jurisprudence related to civil liberties, privacy, Posse Comitatus, implications of Executive Order 12333 and DoD 5240.1-R, the USA PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA). Such a course could include a trip to the Supreme Court and be taught by a professor from a leading law school in the Washington D.C. area. In addition, leading civil liberties or privacy scholars from the area could be invited to lecture. Understanding legal frameworks would clarify which government agencies could legally view, store, or handle which types of information.

This understanding would facilitate the design of a system that automatically knows what information it may stream to whom. It may also enable data sets to be rapidly sent to an agency that may not normally receive them. To use a 9/11scenario as a hypothetical example, the Federal Aviation Administration (FAA) may always receive information regarding the airline, pilot, location, passenger list and speed of an aircraft while NORAD may not. NORAD would not need the information if everything were

"business as usual." In the event that military assistance is needed, the FAA may enable the surveillance information, or specific pieces of it, to be viewed at NORAD to deal with an imminent threat.

After the PCLOs are established and trained on these topics, consideration should be given to conducting a course on systems engineering. In this course, PCLOs could explore how to design architectures with privacy and civil liberties as a key design factor. A list of these design factors could be adapted from documents mentioned in this thesis and from the Markle Foundation Task Force's report "Protecting America's Freedom in the Information Age," specifically illustration number three: guidelines for database access and use.[93]

Consideration should be given to awarding PCLOs with a degree or certificate for accomplishing this training. Such formal recognition for the training would be a motivator for the PCLOs to complete it and would appropriately recognize the people with this specific knowledge.

The content of all of this training would be extremely important, but the relationships formed by going through the training with counterparts from different agencies around the country would be just as significant. The relationships formed during these sessions would lead to the establishment of a PCLO network.

2. Networked Leaders Creating an Information Sharing Network

The network established as a result of social bonds and common training would strengthen the resolve of individual PCLOs to continue to pursue the advancement of both liberty and security in their individual organizations. The collaboration and information sharing between PCLOs would likely spread beyond themselves and result in greater collaboration and information sharing between the agencies as a whole. For example, as PCLOs from several agencies interact they may find that each agency is engaged in developing their own surveillance system with strikingly similar requirements and capabilities. This discovery may prompt the agencies to develop one shared system

93 Baird and Barksdale, "Protecting America's Freedom," 32-34.

rather than many stovepiped systems. This avoidance of a duplication of effort could result in savings to the taxpayer, not to mention the obvious advantage of shared information.

The connection of PCLOs to each other is vitally important, but they should also be connected to the "Privacy and Civil Liberties Board" established by the President. This connection would foster a cohesive national effort to pursue the advancement of both liberty and security and give more clout to agency PCLOs. The senior decision makers in each agency may be more apt to give credence to their PCLO's recommendations if they know he has direct access to this board (and the board direct access to the President). As PCLOs generate numerous ideas at their agencies, the Privacy and Civil Liberties Board could identify best practices and recommend changes to the President. Working in reverse, the Privacy and Civil Liberties Board could provide guidance to the agency PCLOs while allowing them autonomy within their agencies.

PCLOs would benefit from having access to a set of collaborative tools to keep in touch and share ideas with each other. Information technology tools such as on-line forums and secure chat rooms would make this possible. It is likely that many of the organizations with PCLOs would already have the necessary information technology infrastructure to make this relatively simple and cheap to provide.

A network of people from every agency would play a great role in developing a terrorism early warning network that could potentially connect every agency. The network of sensors and computers would enable the right information to be put into the right hands at the right time. The network of people would ensure the information is not used by the wrong agency, for the wrong purpose, anytime. They can ensure this by designing the system with that end in mind. Furthermore, this networking could enable an unprecedented level of oversight.

B. INSTITUTING "ACTIVE, LAYERED OVERSIGHT"

Oversight is paramount to the development of a terrorism early warning system dedicated to preserving liberty. The system must enable the capability to "watch the watchers" to ensure no one agency or branch of government assumes an inordinate amount of power. The framers of the Constitution were gravely concerned about

establishing proper checks and balances within government and spreading power amongst the three branches of the federal government and the states.

The concept of "active, layered oversight" attempts to build checks and balances into the oversight of the system. At the same time, it attempts to recognize and deal with abuses at the lowest possible level with the capability to deal with them at higher levels if necessary. Active, layered oversight relies on each agency overseeing its own use of information (intra-agency), a mechanism for interagency oversight (one agency overseeing another), executive branch oversight and Congressional oversight. Each layer of oversight would be empowered by audit trails and logs showing how information was used by a particular agency. The hope is that very view issues would need to be solved at the executive branch or Congressional levels.

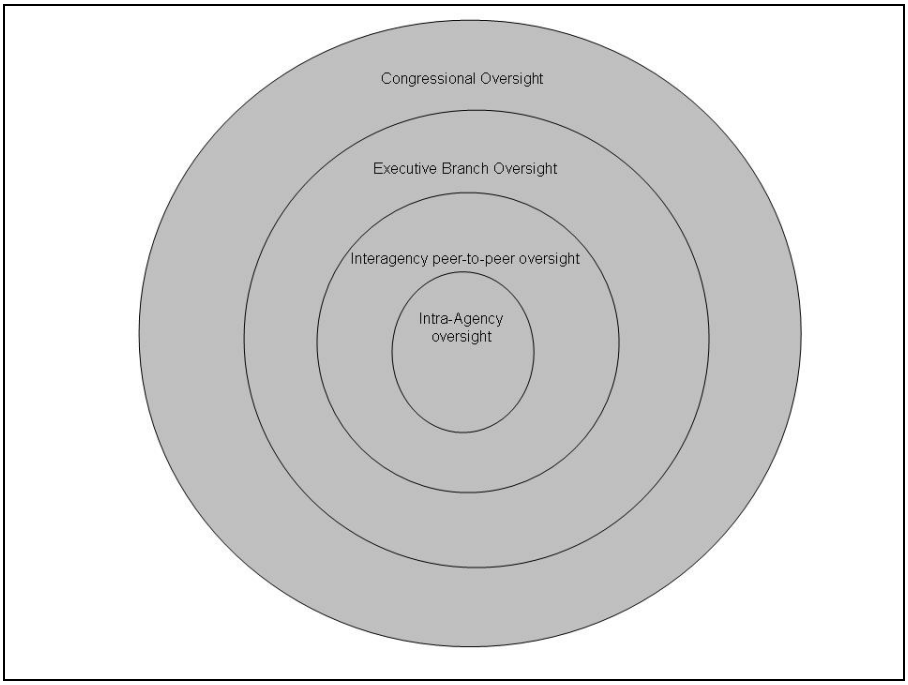

Figure 15. An Active, Layered Oversight Model

1. Internal (Intra-Agency) Oversight

The first layer of oversight requires each agency with access to the terrorism early warning system to develop the capability and mechanisms to monitor its own use of information. Most organizations with counterterrorism responsibilities already possess

an inspector general or internal affairs office. This office could be responsible for reviewing audit trails and information use logs to ensure its analysts and operators are appropriately using the data they have access to. Additionally, each agency should develop training programs to train its operators and analysts on what uses are considered proper. The space operations career field has a process in place whereby commands sent to satellites can be "played back" and operators held accountable or given additional training for mistakes.[94] A similar method could be adopted in a system that is capable of auditing how information is used. Internal oversight would likely curb a large percentage of potential abuse or misuse of information.

2. Interagency Peer-to-Peer Oversight

Most elementary school children who have taken spelling tests understand that integrity increases manifold simply by exchanging papers when the time comes for grading. Interagency, peer-to-peer oversight is based on the concept of accountability and could leverage existing technology to exchange audit logs with peers in other agencies. These "peers" could be randomized to prevent any collusion between agents at different agencies to abuse information.

A similar concept already exists on the internet for friends or "accountability partners" to share internet activity reports in an effort to avoid pornography on the web. One company, Covenant Eyes, has developed a scoring algorithm which rates the "offensiveness" of internet material and automatically generates and e-mails a report to one's accountability partner in the event it suspects the person is viewing pornographic material.[95] The algorithm is not perfect. Sometimes false reports are generated, but these false positives can normally be resolved through discussion.

The Covenant Eyes model could be adapted for use in a terrorism early warning system. Building on access and semantic web technologies discussed earlier, an algorithm could be developed to score audit logs and warn of potential misuse of personal information. For example, logs might be traded between NSA and CIA agents and

---

[94] Author's experience as a satellite operator and evaluator.

[95] See www.covenanteyes.com for more information on how the scoring algorithms and the system in general operate.

indications of abuse may simply warrant a phone call to ask, "What are you doing?" The ensuing conversation may clear up confusion or it may prevent a disingenuous use of personal information.

In the event one peer became belligerent or insists in engaging in suspect behavior, the other peer could then forward a complaint to the next layer of oversight.

3. Executive Branch Oversight

Hopefully, very few instances of abuse would reach this layer of oversight. Its existence, however, is necessary to provide a forum to consolidate reports of abuse from lower levels and to arbitrate any disputes over allegations of abuse between agencies. The most likely candidates to take on this function would be the DNI's Privacy Office and/or the Privacy and Civil Liberties Board—both established by IRTPA. These offices might oversee the development and deployment of a Covenant Eyes-like technology and conduct periodic inspections of its own to ensure compliance with policy and law.

Additionally, this layer of oversight could establish a web form or hotline as a collection point for complaints of information abuse. This would provide whistleblowers an outlet (other than the media) to resolve their concerns. In the event a whistleblower felt uncomfortable lodging a complaint within the executive branch, he could take it to the next level—Congressional oversight.

4. Congressional Oversight

Given that Congress has the power to pass laws and controls the nations "purse," the final layer of oversight needs to be conducted by Congress, more specifically by a select congressional committee or subcommittee. The 9/11 Commission Report offers some practical suggestions on how Congress could engage in its oversight function.

The 9/11 Commission recommended Congress pursue establishing a Joint Committee for intelligence oversight based on the model of the Joint Committee on Atomic Energy or a committee in each house of Congress combining authorizing and appropriating authorities. Either framework would likely work. What is essential is that Congress recognize its role in developing the laws and policies that guide the development and use of a terrorism early warning system and that they demand its development tend to the values of privacy and security—not attempt to achieve a balance.

Where existing policy is irrelevant either by the current national security environment or the advent of new technology, Congress needs to lead by formulating policies that provide for the nation's protection from external and internal threats.

Finally, whatever structure Congress chooses in organizing itself to conduct oversight, they must maintain a close relationship with the Privacy and Civil Liberties Board and the Privacy Officers within the DNI and DHS. This is essential as these executive offices have the capability to reach into the next layer of oversight.

Technology has a significant role to play in enabling the concept of "active, layered oversight," but leadership has an even more significant role. Without Congressional leadership, oversight mechanisms are likely to remain status quo, relying on policy developed during the Cold War to guide us in a much more complex environment. Leadership is essential, and if Congress fails to lead the executive will likely attempt to fill the void. This will likely threaten the balance of power that is crucial to our form of government.

C. SUMMARY AND CONCLUSION

The following bullet points are offered as a summary to the main points developed in the thesis.

- There is a mandate to vastly improve the ability to share terrorism information as a means to respond to terrorism. Since terrorism does not respect borders, this mandate includes improved sharing of domestic intelligence and the "growing together" of foreign and domestic intelligence
- In the sharing of this information, as all of the government documents relevant to this subject affirm, the privacy and civil liberties of Americans must be protected
- Responding to terrorism while protecting privacy and civil liberties is often articulated as "finding the right balance." This model is dangerous, as it implies security and privacy are values that must compete or be traded in a zero-sum game
- A better model represents these values as mutually reinforcing and equally beneficial to the continued success of American society in the age of terrorism
- Armed with this mindset, it is possible to identify privacy and security principles that could be used as requirements in the design and

development of a terrorism early warning system. The requirements can be represented in a Security and Privacy Reference Matrix

- Current and near-term technologies show great promise in being able to address requirements on both the privacy and security sides of the matrix. Additional research and development is needed to further
- Strong cooperation among stakeholder agencies and privacy advocates is needed to develop a system which vigorously considers the principles articulated on both sides of the matrix. This cooperation could be facilitated by instituting PCLOs within stakeholder agencies, enabling the formation of a network of PCLOs across the country.
- Strong leadership from all branches of government is necessary to ensure the terrorism early warning system or ISE is designed and built with these principles in mind and to establish the laws, policy and oversight mechanisms that will govern its use.

Transnational terrorists, particularly terrorists determined to obtain and use weapons of mass destruction, pose a significant national security threat. Responding to this threat requires the development of an early warning system with the capability to warn of indications of attack wherever on the globe they may surface, including within our own borders.

The capability to look for indications of terrorism within our own borders carries weighty implications. The development of an effective terrorism early warning system must not threaten the privacy and civil liberties of Americans, otherwise we run the risk of the nation crumbling from the inside out. This risk is just as real as that posed by an external attack.

Achieving the proper relationship between liberty and security is not unique to the twenty-first century or to the struggle in dealing with terrorism. The Founding Fathers struggled with this concept at length. In Federalist Paper Eight Alexander Hamilton expressed concern over an America focused on security at the expense of freedom.

> Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war—the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty, to resort for repose and

> security to institutions, which have a tendency to destroy their civil and political rights. To be more safe they, at length, become willing to run the risk of being less free.[96]

In what is likely to be a long war against terrorism, America must guard against the tendency to be less free. Security and liberty are not values to be traded, they are values that must be defended. In the case of liberty, it should not be defended solely by privacy advocates, but also by those who have taken oaths to "support and defend the Constitution" and by the people at large.

It is possible to build an effective terrorism early warning system that protects against unnecessary intrusions on privacy. Building such a system will take the cooperation of technology, policies, laws and effective oversight mechanisms. More importantly it will take the collective national will to research, design and build the system—not a fight between two camps continually trying to add weight to one side of a security-privacy scale.

The days of Revere, Franklin, Hamilton were uncertain. The future of America was, at times, in doubt. The courage, leadership and ingenuity of such men, however, set a course that has served the country well. Similar courage, leadership and ingenuity are needed today so that we can hear the warning bells predicting attack and at the same time continue listen to the sweet sound of freedom ringing.

---

96 Alexander Hamilton, "Federalist Paper Number 8," *The Federalist Papers*, ed. Gary Wills (New York: Bantam Publishers, 1982).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Arquilla, John, David Ronfeldt, and Michele Zanini. "Networks, Netwar and Information-Age Terrorism," *Countering the New Terrorism.* Santa Monica, CA: RAND Corporation, 1999.

Berners-Lee, Tim, James Handler, and Ora Lassila. "The Semantic Web," *Scientific American*, May 17, 2001 http://www.scientificamerican.com/article.cfm?articleID=00048144-10D2-1C70-84A9809EC588EF21&catID=2 (accessed July 2, 2005).

Cate, Fred H. "Legal Standards for Data Mining," in forthcoming *Emergent Information Technologies and Enabling Policies for Counter Terrorism*, ed. Robert Popp and John Yens. Hoboken, NJ: Wiley-IEEE Press, 2006.

Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force on National Security in the Information Age. New York: The Markle Foundation, 2003.

Dempsey, James X. and Paul Rosenzweig. Heritage Foundation. "Technologies That Can Protect Privacy as Information is Shared to Combat Terrorism," May 2004, 1-2. http://www.heritage.org/Research/HomelandDefense/lm11.cfm (accessed July 2, 2005).

De Rosa, Mary. "Privacy in the Age of Terror." *Washington Quarterly* (Summer 2003), 29-30.

Electronic Privacy Information Center. "ChoicePoint." www.epic.org/privacy/choicepoint (accessed February 22, 2006).

Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*. Washington, D.C., 2000.

Franklin, Benjamin. *Historical Review of Pennsylvania, 1759* in Robert Bach, "Special Topics in Homeland Security." Lecture, Naval Postgraduate School, Monterey, CA, July 14, 2005.

Froomkin, Michael. "The Death of Privacy?" *Stanford Law Review* (2000): 1461-1471.

Gilmore Commission. *The Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, "Forging America's New Normalcy: Securing Our Homeland, Preserving Our Liberty*. Washington, D.C.: GPO, December, 2003.

Global Platform, DoD Case Study. "Common Access Cards—Expanding the Functionality of ID Cards for the US Department of Defense." http://www.globalplatform.org/fcs/DOD_Case_Study.pdf (accessed July 10, 2005).

Hamilton, Alexander. "Federalist Paper Number 8." *The Federalist Papers*, ed. Gary Wills. New York: Bantam Publishers, 1982.

Independence Hall Association. "The Liberty Bell." http://www.ushistory.org/libertybell/ (accessed December 15, 2005)

Kim, W. Chan and Renee Mauborgne. *Blue Ocean Strategy*. Boston: Harvard Business School Press, 2005.

Laudon, Kenneth C. and Jane P. Laudon. *Essentials of Management Information Systems.* Upper Saddle River, NJ: Prentice Hall Publishers, 2005.

Manola, Frank and Eric Miller. "RDF Primer 2004." http://www.w3.org/TR/rdf-primer/ (accessed June 26, 2005).

National Commission on Terrorist Attacks upon the United States. *The 9/11Commission Report; Final Report of the National Commission of Terrorist Attacks Upon the United States.* New York: W.W. Norton & Company, 2004.

National Reconnaissance Office. "Corona Fact Sheet." http://www.nro.gov/corona/facts.html (accessed December 22, 2005).

Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C.: U.S. Government Printing Office, 2002.

Office of the Director of National Intelligence. *National Intelligence Strategy of the United States of America.* Washington D.C., 2005.

Ohno-Machado, Lucila M.D., Ph.D; Staal Vinterbo, Ph.D; Stephan Dreiseitl, Ph.D. "Effects of Data Anonymization by Cell Suppression on Descriptive Statistics and Predictive Modeling Performance." *Journal of the American Medical Informatics Association*, November/December 2002. http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=419433&blobtype=pdf (accessed June 29, 2005).

Organisation for Economic Co-Operation and Development (OECD). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed February 6, 2006).

Plato. *The Republic*. In *The New Dictionary of Cultural Literacy*, 3rd ed., ed. E.D. Hirsch, Jr., Joseph F. Kett, and James Trefil. New York: Houghton Mifflin, 2002. Accessed at http://www.bartleby.com/59/3/necessityist.html. (accessed December 15, 2005).

Protecting America's Freedom in the Information Age: Report of the Markle Foundation Task Force on National Security in the Information Age. New York : The Markle Foundation, October 2002.

Rosenzweig, Paul. "Proposals for Implementing the Terrorism Information Awareness System." *Heritage Foundation Legal Memorandum #8* (2003).

Safire, William. "You are a Suspect." *New York Times*, November 14, 2002.

Simmons, Greg. "Debate Rages Over Legality of NSA Wiretap Program." Greg Simmons, *Fox News*, www.foxnews.com. (accessed February 6, 2006).

Solove, Daniel J., "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (Fall 2005): 477-564. Available at SSRN: http://ssrn.com/abstract=667622. (accessed December 22, 2005).

Solove, Daniel J. and Chris Jay Hoofnagle. "A Model Regime of Privacy Protection (Version 1.1)." GWU Law School Public Law Research Paper No. 132, March 8 2005. Available at SSRN: http://ssrn.com/abstract=681902 or DOI: 10.2139/ssrn.681902 (accessed December 15, 2005).

Stanley, Jay and Barry Steinhardt. American Civil Liberties Union. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." January 2003.

Sweeney, Latanya. "*k*-anonymity: A Model for Protecting Privacy." *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 10: 5 (2002): 557-570.

The Paul Revere House. "The Real Story of Paul Revere's Ride." http://www.paulreverehouse.org/ride/real.shtml (accessed December 15, 2005).

Technology and Privacy Advisory Committee. "Safeguarding Privacy in the Fight Against Terrorism." Washington, D.C.: n.p., 2004.

Taipale, K.A. "Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties." Chapter 9.4 in *Emergent Information Technologies and Enabling Policies for Counter Terrorism*, ed. Robert Popp and John Yens. Hoboken, NJ: Wiley-IEEE Press, forthcoming 2006.

Taipale, K.A. "Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd." *Yale Journal of Law and Technology* 7, no. 123, December 2004. Available at SSRN: http://ssrn.com/abstract=601421. (accessed February 6, 2006).

Thornlow, Christopher. "Fusing Intelligence With Law Enforcement Information: An Analytic Imperative." Master's thesis, Naval Postgraduate School, 2005.

United States Air Force. "Defense Support Program Fact Sheet." http://www.af.mil/factsheets/factsheet.asp?id=96 (accessed December 15, 2005).

United States v. Miller, 425 U.S. 435 (1976).

U.S. Congress. House. *Intelligence Reform and Terrorism Prevention Act of 2004.* 108th Cong., 2d sess., 2004 House report No. 108-796.

U.S. Department of Defense. *Strategy for Homeland Defense and Civil Support*. Washington, D.C., 2005.

U.S. President. *Executive Order*. "National Counterterrorism Center, Executive Order 13354" *Federal Register 69*, no. 169 (1 September 2004).

U.S. President. *Executive Order*. "Strengthened Management of the Intelligence Community, Execuritve Order 13355." (27 August 2004).Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html.

U.S. President. *Executive Order*. "Strengthening the Sharing of Terrorism Information to Protect Americans, Executive Order 13356" (27 August 2004). Available [Online]: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html.

Worcester Polytechnic Institute Department of Military Science. http://www.wpi.edu/Academics/Depts/MilSci/BTSI/Lexcon (accessed December 15, 2005).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Paul Stockton, Director
Center for Homeland Defense and Security
Naval Postgraduate School
Monterey, California

4. David Blehm, Colonel, USAF
Chief, Future Concepts and Capabilities Division
NORAD
Colorado Springs, Colorado

5. Daniel Fox, Lieutenant Colonel, USA
NORAD
Colorado Springs, Colorado