2009-09

Privacy protection standards for the information sharing environment

Holmstrup, Mark A.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PRIVACY PROTECTION STANDARDS FOR THE INFORMATION SHARING ENVIRONMENT

by

Mark A. Holmstrup

September 2009

Thesis Co-Advisors: Richard D. Bergin
Robert A. Josefek

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Privacy Protection Standards for the Information Sharing Environment	5. FUNDING NUMBERS
6. AUTHOR(S) Mark A. Holmstrup	
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)

Created in response to findings of the 9/11 Commission concerning the lack of information sharing as a primary factor in the failure to stop the September 11, 2001, attacks, the Information Sharing Environment (ISE) was mandated by the *Intelligence Reform and Terrorist Prevention Act of 2004* (IRTPA). The ISE was intended to build on existing information sharing systems and promote increased information sharing through the creation of a collaborative culture among a diverse group of participants. Another goal of the ISE is to protect information privacy. ISE efforts to meet the goal of information privacy protection are stymied by a lack of uniform privacy standards that are equally applicable to all ISE participants. The thesis compares two policy options—voluntarily adopted mandatory standards and federally imposed mandatory standards—to the status quo system of voluntary guidelines. These policy options are evaluated in terms of their effect on collaboration and information sharing, their constitutionality, their consistency and enforceability in application, and political acceptability. Based on projected relative outcomes, this thesis recommends that the ISE adopt a privacy protection system consisting of voluntary standards that, once adopted, become mandatory in application.

14. SUBJECT TERMS Information Sharing Environment, privacy, collaboration, constitutionality, Transportation Security Administration, Program Manager Information Sharing Environment, information sharing	15. NUMBER OF PAGES 115
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PRIVACY PROTECTION STANDARDS FOR THE INFORMATION SHARING ENVIRONMENT

Mark A. Holmstrup
Supervisory Attorney-Advisor, Department of Homeland Security, Transportation Security Administration, Coppell, TX
B.S., George Mason University, 1986
J.D., George Mason University School of Law, 1990

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
September 2009

Author: Mark A. Holmstrup

Approved by: Richard D. Bergin
Thesis Co-Advisor

Robert A. Josefek
Thesis Co-Advisor

Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Created in response to findings of the 9/11 Commission concerning the lack of information sharing as a primary factor in the failure to stop the September 11, 2001, attacks, the Information Sharing Environment (ISE) was mandated by the *Intelligence Reform and Terrorist Prevention Act of 2004* (IRTPA). The ISE was intended to build on existing information sharing systems and promote increased information sharing through the creation of a collaborative culture among a diverse group of participants. Another goal of the ISE is to protect information privacy.

ISE efforts to meet the goal of information privacy protection are stymied by a lack of uniform privacy standards that are equally applicable to all ISE participants. The thesis compares two policy options—voluntarily adopted mandatory standards and federally imposed mandatory standards—to the status quo system of voluntary guidelines. These policy options are evaluated in terms of their effect on collaboration and information sharing, their constitutionality, their consistency and enforceability in application, and political acceptability. Based on projected relative outcomes, this thesis recommends that the ISE adopt a privacy protection system consisting of voluntary standards that, once adopted, become mandatory in application.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to my wife and children, in recognition of their limitless support and endless patience.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> With proper planning we can have both enhanced privacy protections and increased information sharing—and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people.
>
> National Strategy for Information Sharing (2007), p. 27.

A. PROBLEM STATEMENT

Created in response to findings of the 9/11 Commission concerning the lack of information sharing as a primary factor in the failure to stop the September 11, 2001, attacks, the Information Sharing Environment (ISE) was mandated by the *Intelligence Reform and Terrorist Prevention Act of 2004* (IRTPA). The ISE was intended to build on existing information sharing systems and promote increased information sharing through the creation of a collaborative culture among a diverse group of "federal departments and agencies and state, local, and tribal governments, the private sector, and foreign partners" (Program Manager-Information Sharing Environment [PM-ISE], n.d.). One of the five stated goals of the ISE is to "***ensure*** sharing procedures and policies and protect information privacy and civil liberties" (PM-ISE, n.d.).

ISE efforts to meet the goal of information privacy protection are stymied, in part, by a lack of settled law in this area (exacerbated by a paucity of Supreme Court cases that fail to address immense changes in information technology in the three decades since they were decided), and a hodgepodge of federal and state laws that do not provide uniform privacy protection.

Furthermore, other than supplying very general guidelines to the ISE, there has been little action taken by the ISE program manager to remedy this gap in privacy protection. The PM-ISE guidelines identify privacy issues and provide assistance with preparing privacy protection policies but, in practice, do not mandate any particular privacy protections; in fact, "privacy" is not even defined in the guidelines (PM-ISE, n.d.). Participation in the ISE is not

conditioned upon compliance with the PM-ISE guidelines. Instead, privacy protection standards are promulgated by each ISE participant, leading to inconsistencies in protection. Moreover, despite a pronouncement that the private sector and foreign partners are an important part of the ISE, those sectors are rarely mentioned in the PM-ISE guidelines, much less the subject of any regulation or control.

Besides the apparent deleterious effects on privacy itself, the lack of uniform standards may actually work against the creation of a collaborative information sharing environment. For example, some participants in the ISE may be less likely to share information if they cannot ensure that the recipient of that information has adequate privacy protections in place (Stimson, 2008). Violations of privacy rights through improper dissemination of personal information can also lead to decreased support for counterterrorism efforts (National Research Council, 2008).

Although information concerning specific instances of privacy issues in the ISE is not readily available, the existence of the issue was recognized in a recent report by the Markle Foundation Task Force on National Security in the Information Age (2009). The Markle report detailed the steps the group believes the Obama administration should take to improve information sharing that, in its view, remains inadequate (Markle Foundation, 2009). Included in the report is a discussion of the need for an effective framework for information sharing, including "government-wide policy guidelines and oversight to provide robust protections for privacy and civil liberties" (Markle Foundation, 2009, p. 7). The report goes on to discuss the problems that could arise in the absence of those protections:

> Without those privacy protections in place, the American people won't have confidence in their government, while the analysts and operatives using the information sharing framework won't have confidence that they know what they are expected and allowed to do, and that their work is lawful and appropriate.(Markle Foundation, 2009, p. 2)

The need to address privacy concerns is becoming more acute. The National Research Council (2008) found that over time "the public is growing less certain of the need to sacrifice civil liberties for terrorism prevention, less willing to make such sacrifices, and more concerned that government counterterrorism efforts will erode privacy" (p. 283). Furthermore, "trust in government is negatively associated with affirmation of civil rights: those with greater trust in government are more willing to sacrifice freedoms, compared with those with less trust" (National Research Council, 2008, p. 321). However, the National Resource Council (2008) found that threat perception, among other considerations, also impacts the public's balancing of civil liberty protections and counterterrorism efforts.

B. RESEARCH QUESTION

Is there a need for a new conception of information privacy law for application in the Information Sharing Environment, and, if so, which policy options to apply this new concept would most effectively protect privacy rights while promoting increased information sharing and creating a collaborative environment among the wide variety of ISE participants?

C. SIGNIFICANCE OF RESEARCH

This research is intended to be of interest to the homeland security academic and legal communities by proposing a new conceptual framework for information privacy law. The immediate consumers of this research, however, are the Program Manager of the Information Sharing Environment all ISE members from the federal, state, local, and tribal governments. In addition, this research identifies new privacy protection policy options for consideration by policymakers and homeland security practitioners and, given the paucity of literature in this policy area, ideally would form the basis for future debate and research. In summary, by ensuring the uniform and mandatory application privacy protection standards for all members of the ISE, homeland security can be improved and individual rights and liberties can be protected.

D. LITERATURE REVIEW

This literature review concerns (1) the jurisprudential basis for the concept of information privacy; (2) existing federal privacy statutes; and (3) selected general approaches to protecting information privacy rights.

1. Jurisprudential Basis for the Concept of Information Privacy

Closely related to the Fourth Amendment's prohibition of unreasonable searches and seizures, the right of privacy is judicially recognized as a fundamental right protected by the Constitution (Richards, 2006). Although the two protections are related, the right of privacy and the Fourth Amendment are not coterminous.

In addition to its relationship to the Fourth Amendment, the right of privacy arises from several other constitutional provisions—namely, the First Amendment (freedom of speech), the Third Amendment (peacetime quartering of soldiers), the Fifth Amendment (privilege against self-incrimination), the Ninth Amendment (preservation of rights not specifically enumerated) and the Fourteenth Amendment (Due Process Clause) (Kramer, 2007).

Commonly divided into distinctive constituent parts, the general law of privacy encompasses (1) "informational privacy," which concerns the "dissemination or misuse of sensitive and confidential information," and (2) "autonomy privacy," which deals with "making intimate personal decisions or conducting personal activities without observation, intrusion, or interference" (Kramer, 2007, §§ 603, 604). In essence, then, the right of privacy can be thought of as the right to be left alone (autonomy privacy) and the right to keep personal information personal (information privacy).

Information privacy—the part of privacy implicated by the ISE—is further subdivided into areas concerning the collection and storage of personal information by the government, on one hand, and the public release of that information on the other hand (Kramer, 2007). In contrast to other rights, including the right of autonomy privacy, information privacy has not often been

considered by the courts. Two of the primary Supreme Court cases dealing with information privacy focused on the role of the Fourth Amendment—to the exclusion of other bases for the right of privacy—in concluding that there is no reasonable expectation of privacy in bank records (U.S. v. Miller, 425 U.S. 435 (1976)) or dialed phone numbers (Smith v. Maryland, 442 U.S. 779 (1979)) because in both cases the information at issue was voluntarily given to third parties. In a third case from the 1970s, Whalen v. Roe, 429 U.S. 589 (1977), the court expressly distinguished information privacy from autonomy privacy.

These Supreme Court precedents, in effect, treat information privacy as an on-off switch. Information is either entirely private or entirely public—with either full protection or virtually no protection, respectively. With limited exceptions for privileged communications, such as the attorney-client privilege, once information is communicated to a third party there ceases to be a reasonable expectation of privacy.

The constitutionality of a New York state statute requiring the identification of patients who obtained certain controlled prescription drugs was the subject of Whalen. In upholding the state statute, the Supreme Court expressly stated its view that privacy, as a concept, actually involves two different kinds of interests. The first involves *decisional privacy*, the "interest in making certain kinds of important decisions," and second pertains to *informational privacy*, defined as "the individual interest in avoiding disclosure of personal matters" (429 U.S. at 599).

In *dicta*—a non-dispositive opinion of a court—the court discussed "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files" (429 U.S. at 605). However, the court recognized that certain government functions, such as law enforcement, "require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing

if disclosed" but that the "right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures" (429 U.S. at 605).

In Miller, the federal government appealed a Court of Appeals ruling that Miller's Fourth Amendment right against unreasonable search and seizure were violated when the government required a third-party bank to copy all of the Miller's personal checks. The U.S. Supreme Court reversed the Court of Appeals and held that Miller did not have a protected Fourth Amendment interest in copies of his personal checks.

Distinguishing the current case from Boyd v. United States, 116 U.S. 616 (1886), the Supreme Court held that, unlike Boyd, where "private papers" were found to be protected against compulsory production, the papers in the Miller case were not private, even though Miller claimed that he had a reasonable expectation of privacy in the check copies. In so holding, the court stated that it had

> held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will only be used for a limited purpose and the confidence placed in the third party will not be betrayed. (Miller, 425 U.S. at 443)

Smith involved a criminal case in which a pen register, used to record phone numbers dialed, was installed on Smith's telephone line by a phone company at the request of the police. Smith claimed that the use of the pen register, installed without a warrant. improperly infringed on his reasonable expectation of privacy. The "reasonable expectation of privacy," as the Supreme Court explained by reference to Katz v. United States, 389 U.S. 347 (1967), depends "on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action" (Smith, 442 U.S. at 740) [internal cites omitted]. Thus, as the court continued, a reasonable expectation of privacy analysis requires an

examination of two questions. First, has an actual, subjective expectation of privacy, as evidenced by conduct, been exhibited? Second, is society willing to recognize that subjective expectation of privacy as reasonable? Both questions must be answered in the affirmative for there to be a finding of a reasonable expectation of privacy.

In applying these questions to the case at hand, the Court held that Smith, and telephone users as a whole, do not "harbor any general expectation that the numbers they dial will remain secret" Smith, (442 U.S. at 743). Although the analysis could have ended there, the Court went on to hold that even if Smith had had a subjective expectation of privacy, such an expectation would not be one that society would find to be reasonable, stating that the Court "consistently has held that a person has no legitimate expectation of privacy he voluntarily turns over to third parties" (Smith, 442 U.S. at 743-744) [internal cites omitted].

Subsequently, Congress passed legislation to statutorily supersede these two cases. In response to Miller, the Right to Financial Privacy Act (12 U.S.C. § 3401 *et seq.* (1978)), was enacted to allow individuals to challenge administrative subpoenas of financial records in court. Smith, in turn, was superseded by 18 U.S.C. § 3121(a) (1989), which prohibited use of pen registers without a warrant.

Nonetheless, the underlying holding in both Miller and Smith—that there is no reasonable expectation in information voluntarily given to third parties—still stands notwithstanding the subsequent legislation. In Securities and Exchange Commission v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984), third-party subpoenas issued under the Securities Act of 1933 and the Securities Exchange Act of 1934 were upheld as constitutional. The court, citing Miller, reiterated the principle that it is "established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities" (467 U.S. at 743).

Despite these Supreme Court cases, information privacy law remains unsettled many years later. Legal scholars continue to debate the nature of the right itself (Richards, 2006). Should exposure of information to others retain its private character? Does it matter whether the exposure was accidental or intentional? Does intentional release of information in a limited fashion eliminate the right as to further release to others? Does the right protect the confidentiality of relationships? These are but a sampling of the issues currently being debated in this body of law (Richards, 2006). Although it is recognized as a fundamental right, the right of privacy "remains a piecemeal, poorly understood, and only partially successful body of jurisprudence" (Richards, 2006).

Solove (2008) provides a succinct overview of the myriad conceptions of privacy that have been considered since the idea of privacy was first considered in the nineteenth century. In Solove's (2008) view, existing theories of privacy are either too broad, in that they fail to exclude matters which are not commonly deemed private, or too narrow because they fail to include matters commonly deemed private.

The traditional conception of privacy as "the right to be left alone" fails to provide enough guidance on what constitutes privacy (Solove, 2008, pp. 15–18). Another conception, the view of privacy as "limited access to self," which recognizes an individual's need to be apart from others, does not discuss the degree of intrusion necessary to constitute an invasion of privacy (Solove, 2008, pp. 18–21).

The next conception, secrecy, involves the public disclosure of private information and often leads to the finding that once information is disclosed to a third party that information can no longer be treated as private, even if a person intends to make only a limited disclosure to some but not others (Solove, 2008). According to Solove (2008), using *secrecy* as the common element of privacy is too narrow because it fails to account for a person's desire to regulate the amount of disclosure desired; in other words, the difference is in protecting confidentiality rather than secrecy. The theory of control over personal

information addresses some of the flaws of the secrecy theory but is too narrow in that it concerns informational but not autonomy privacy. It is too vague in that it does not delineate the categories of information privacy that a person should have control of, and it fails to consider that the individual should not be the only party to decide what information should be protected; society should have a say as well (Solove, 2008).

Another theory is that of protecting the *personhood* of integrity of an individual's personality against invasion by government. This theory fails according to Solove (2008) because it fails to adequately define "personhood" and thus improperly leaves the definition up to the government to choose and then enforce. A final theory, protecting *intimacy*, is based on the assumption that privacy is important not only to individuals but to relationships. Solove (2008) believes this theory is at once both too broad, in that "intimacy" is insufficiently defined and without limitations of scope, and too narrow, in that it focuses on relationships to the exclusion of other realms in which privacy operates.

The issue with theories of privacy that are too narrow is that privacy issues are often overlooked by the law; theories that are too broad tend to have too little meaning to lead to constructive answers to problems (Solove, 2008). Instead, seeing privacy as a grouping of related, but distinct, matters means that "if we no longer must search for one unifying common trait in all privacy violations, we can identify many specific elements of privacy without sacrificing inclusiveness" (Solove, 2008, p. 44).

As Solove (2008) posits, the elusiveness of a single, widely accepted definition of privacy can be sidestepped by recognizing that there can be different forms of privacy that related in a familial sense, rather than by continuing the usual, but unavailing approach which seeks to isolate a characteristic of privacy that is common to all usages. The key to this taxonomic framework is that privacy is considered in a contextual manner by conceptualizing privacy by means of "focusing on the specific types of disruption" that a particular invasion of privacy engenders (Solove, 2008, p. 9; also see p. 47).

2. Federal Privacy Statutes

Several statutes govern the privacy of personal information that is collected and used by the federal government. The Privacy Act of 1974 places limitations on the collection, use, and disclosure of government records (called "systems of records") that include names of individuals or other personal identifiers. The Privacy Act also requires federal agencies to define the purpose for which the records are kept and to limit their use of the records to the stated purpose unless certain exemptions, such as for a criminal investigation, apply. The E-Government Act of 2002 requires federal agencies to analyze the privacy impact of the collection, storage, management, and sharing of information that they conduct. Known as Privacy Impact Assessments, this analysis is required to be conducted any time an agency is procuring or deploying new information technology or commences any new collection of data. However, other than a provision pertaining to the use of social security numbers, the Privacy Act applies only to the federal government and not to other participants in the ISE. Similarly, the Federal Information Security Management Act of 2002 addresses the protection of personal information through computer network security measures, but only applies to federal agencies.

Although these statutes codify privacy rights to a certain extent, their application is limited. Except for the isolated exception noted above, all three statutes apply only to the federal government and not to the other major actors in homeland security, namely state, local, and tribal governments. Furthermore, even within their application to the federal government, those statutes do not apply in all instances. In the Privacy Act, for example, the statute applies only to systems of records. If the personal information at issue is not kept in a system of records, then the Privacy Act's protections do not apply. Moreover, in the case of the E-Government Act, agency implementation of the Privacy Impact Assessment requirement has been inconsistent (GAO, 2007). In discussing the similarly uneven application of another federal privacy law, Schwartz (2008)

coined the term “privacy theater” to refer to laws that seek “to heighten a feeling of privacy protection without actually accomplishing anything substantive in this regard” (p. 310).

3. Selected General Approaches to Protecting Information Privacy Rights

Commentators have identified several possible methods by which to implement information privacy protections. However, there is no unanimity of opinion as to the best method to do so.

a. Legislation

Glover and Bhatt (2006) caution that that “overly aggressive” laws may limit technological innovation and that the needs of corporations (including, presumably, government needs) must be balanced against the needs of individuals (p. 203). Furthermore, they believe the need for special laws—as opposed to existing privacy laws—to promote privacy is not clear (Glover & Bhatt, 2006, p. 203). In a 2007 report, the Government Accountability Office noted the introduction of proposed legislation, entitled the “Privacy Officer with Enhanced Rights Act of 2007,” would provide privacy officers with direct report authority to Congress without prior comment by other parts of the Executive Branch. Simitis (1987) sees regulation of personal data processing as the “decisive test” for whether a society is willing to pay “the price necessary to secure the individual’s ability to communicate and participate” (p. 746). Some believe that legislation provides better protection than relying on the judge-made rules (common law) because the former can “act more quickly in the face of technological change than courts are able to do and to appreciate existing technology and the impact of different legal rules (National Research Council, 2008, p. 153).

b. Government Guidelines

Koontz (2007) states that consistent implementation of appropriate privacy protections require comprehensive guidance to channel the development and implementation of new technologies, such as Radio Frequency Identification (RFID). Koontz (2007) also notes that the 9/11 Commission recommended policy guidelines to closely control the types of information agencies should share and the types of protection that information must have. The Markle Foundation (2002) recommended the use of administrative rules in conjunction with training, technology, and congressional oversight.

c. Internal Agency Processes

Bamberger and Mulligan (2008) believe that privacy is often in conflict with the primary mandates of government agencies, largely due to a disinterested bureaucracy (p. 77). They believe that strong privacy officers, with the ability to report directly to Congress, combined with an effective privacy office staff, will help raise the relative importance of privacy protection in agency processes (Bamberger & Mulligan, 2008, p. 96)

d. External Oversight

Bamberger and Mulligan (2008) point to the relative success of institutionalization of Environmental Impact Studies in agency decision making (as mandated by the National Environmental Policy Act of 1967 [NEPA]), as a model for implementing the Privacy Impact Analysis requirement of the E-Government Act of 2002 (p. 84). They credit external oversight by the Council on Environmental Quality, which developed stringent implementation guidelines and by the active role of the judiciary in broadly construing the applicability of NEPA, with sanctions levied for agency compliance failures for success of the program (Bamberger& Mulligan, 2008, p. 84).

In summary, court cases concerning the extent of the right of information privacy are limited in scope and consider technology of several

decades ago. In general terms, the law of information privacy is not well-defined and its exact nature remains a matter of debate among legal scholars and others. Exacerbating the lack of a common definition of privacy is that the right itself is now affected by increased information sharing in the homeland security context, in particular, in the ISE.

Statutory attempts to plug the gap are only partially successful; their effectiveness is limited by each statute's jurisdictional boundaries and, furthermore, by imperfect implementation attempts by the federal agencies they are intended to regulate. As a result, commentators uniformly recognize the need to improve, or at least fine-tune, privacy protections to bolster their coverage and use, but they are divided as to the most efficacious means to do so.

E. METHODOLOGY

This thesis employs the policy options analysis methodology to compare three different approaches to protect privacy rights in the Information Sharing Environment. In essence, the analysis process as used in this thesis is, first, to define the problem and then select various criteria by which to evaluate the proposed policy options. Next, projected outcomes are compared and a recommendation is made.

However, in this field there are no commonly used theories or models to apply. In the absence of a particular theory or model to guide this analysis, the requirements of the Intelligence Reform and Terrorist Prevention Act and the stated goals of the ISE are used as a touchstone.

The existing ISE privacy protection system is evaluated in terms of the extent to which the ISE's stated goals—fostering collaboration, ensuring the sharing of information, and protection of privacy rights—are met. Thus, the selected policy should maximize privacy protections and the sharing of

information—or at least minimize negative externalities that would act as a disincentive to sharing information--among members of the ISE through collaborative means.

However, as is discussed in a later section of this thesis, the three identified goals of the ISE relevant to the issue of privacy protection—enhancing information sharing, encouraging collaborative efforts by ISE participants and protecting privacy rights—are not the only measures by which ISE privacy protection is considered. Other criteria—constitutionality, enforceability, consistency of application, and political acceptability—are also relevant and critical to this policy choice and, accordingly, are used in the evaluation.

In applying the selected criteria, the PM-ISE's current system of privacy protection through the use of voluntary guidelines is compared to two alternative policy approaches to addressing privacy rights. In other words, this thesis explores whether alternatives to status quo might provide better privacy protection while at the same time providing at least an equivalent amount of information sharing using the PM-ISE's current privacy protection regime as a baseline.

The first alternative policy choice involves voluntarily adopted uniform privacy standards as part of a European system for privacy protection of information sharing. As it shares a common legal heritage with the United States, the European experience with privacy protection is particularly relevant to the ISE. Specifically, this policy choice involves an examination of the European Convention of Human Rights and Fundamental Freedoms, selected decisions of the European Court of Human Rights, the Council of Europe Convention on Data Protection, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and associated Additional Protocol, and the Europol Convention.

The second alternative policy choice to the current ISE system, federally mandated privacy standards, is addressed by considering the use of such mandates in the realms of the protection of health information, motor vehicle records, and criminal intelligence systems. The federal mandates examined include the Health Insurance Portability and Accountability Act of 1996, Driver's Privacy Protection Act of 1994, and U.S. Department of Justice regulations entitled "Criminal Intelligence Systems Operating Policies."

F. SCOPE

This thesis necessarily covers only a small slice of the overall issue of privacy, as a full discussion of this topic would take a multi-volume book to adequately cover. As such, it would be helpful to consider Daniel Solove's (2008) taxonomic approach to privacy that focuses on particular activities that are impacted by privacy problems rather than the more common approach, historically at least, of attempting to define privacy by a single characteristic. Solove (2008) has created a taxonomy that divides the concept of privacy into four primary activity types: information collection (including surveillance and interrogation), information processing (aggregation and identification), information dissemination (disclosure and accessibility), and invasion (intrusion and decisional interference) (Solove, 2008).

For the purposes of this thesis, in order for the theoretical information to be shared, this researcher assumes that the necessary information collection and processing has been done in full accordance with all applicable laws, and that the resulting information is properly in the possession of an ISE participant. Also, the researcher assumes for purposes of this thesis that the issue at hand does not comprise a problem implicating what Solove (2008) deems and information "invasion." Hence, this thesis concentrates on the "information dissemination" activity. In other words, once information is legally within the control of a single ISE participant, what controls are in place—or should be in place—to ensure that privacy is adequately protected when that information is shared within the ISE?

Next, as is discussed later, the most pronounced gap in privacy protection in the ISE concerns state, local and tribal governments, and private sector participants. The various privacy guidelines issued by the ISE Program Manager have been made binding on federal agencies; and although individual agencies are permitted to promulgate their own standards, they are strictly voluntary for non-federal participants. Accordingly, much, though not all, of the analysis focuses on the issue of standards as it applies to state, local and tribal governments and, to a lesser extent, the private sector.

Finally, this thesis explores the need for uniform standards and the issue of possible governance and oversight mechanisms. However, the nuts-and-bolts of the actual standards themselves are beyond the scope of this research and, as is explained later, are probably best left to the ISE participants to determine.

II. THE INFORMATION SHARING ENVIRONMENT

As is discussed above, the Information Sharing Environment (ISE) was mandated by the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) and was intended to build on existing information sharing systems and promote increased information sharing through creation of a collaborative culture among a diverse group federal and non-federal participants. In the words of the ISE Program Manager:

> [T]he Information Sharing Environment (ISE) supports five communities—Intelligence, Law Enforcement, Defense, Homeland Security, & Foreign Affairs—by leveraging existing capabilities and aligning policies, standards and systems to ensure those responsible for combating terrorism have access to timely and accurate information. An improved Information Sharing Environment is being constructed on a foundation of trusted partnerships among Federal, State, local, and tribal governments, the private sector, and our foreign allies—partnerships based on a shared commitment to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the United States. (PM-ISE, n.d.)

The Government Accountability Office describes the ISE as follows:

> The ISE is not bounded by a single federal agency or component. While the Program Manager has been placed within the Office of the Director of National Intelligence, from an operational perspective, the ISE is to reach across all levels of government as well as the private sector and foreign partners. As such, the program is a broad-based coordination and collaboration effort among various stakeholders. In essence, the ISE can be viewed as a set of cross-cutting communications links—encompassing policies, processes, technologies—among and between the various entities that gather, analyze, and share terrorism-related information. (GAO, 2008, p. 10)

The following documents, discussed below, concern the historical context of the ISE, its statutory basis, its policy-based underpinnings, and the scope of duties of the ISE Program Manager.

A. 9/11 COMMISSION REPORT

Created by Public Law 107-236 (November 27, 2002) as a bipartisan group in the wake of the devastating and shocking attacks of September 11, 2001, the National Commission on Terrorist Attacks Upon the United States (more commonly known as the 9/11 Commission) was charged with determining why the United States was seemingly unprepared for the attacks of that day, and how such attacks could be avoided in the future. The group's findings, contained in the *9/11 Commission Report*, were eagerly anticipated.

The lack of information sharing played a big part in the failing of the United States to anticipate and respond to the 9/11 attacks. Consequently, one of the central recommendations of the commission was to unify "the many participants in the counterterrorism effort and their knowledge in a network-based information-based system that transcends traditional government boundaries" (9/11 Commission, 2003, p. 400). Although it focused on the foreign-domestic divide of intelligence information sharing, the Commission's recommendation that the intelligence community's work be held to a common standard for collection, processing, reporting, sharing, and analysis (9/11 Commission, 2003, p. 409) would seem to be equally applicable to the ISE as a whole as well.

In making its information sharing and other recommendations, the 9/11 Commission recognized that the protection of privacy rights was a key consideration, stating that a "shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life" (9/11 Commission, 2003, p. 394). The commission recommended that along with a change in how information is shared that adequate oversight and guidelines to protect civil liberties, in particular it recommended that an executive branch board be established to oversee compliance with those guidelines (9/11 Commission, 2003, p. 395).

B. INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

The *Intelligence Reform and Terrorist Prevention Act* of 2004 (IRTPA, codified at 6 U.S.C. 485) required the establishment of "an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties" (section 1016(b)(1)(A)). The "information sharing environment" is defined by the act as, in part as "an approach that facilitates the sharing of terrorism information" (IRPTA, 2004, section 1016(a)(2)). "Terrorism information," in turn, is defined as information regarding foreign or international terrorist groups, or domestic persons or groups with connections to transnational terrorism (though not to purely domestic terrorists) (IRPTA, 2004, Section 1016(a)(4)). Significantly, though, IRTPA does not define which privacy-related legal standards apply to the sharing of terrorism information, nor is privacy, itself, defined in the act.

The ISE is intended to facilitate the sharing of terrorism information among federal, state, local, and tribal governments, and the private sector through the "use of policy guidelines and technologies" (IRTPA, 2004, section 1016(b)(2)). The incorporation of privacy protections is provided for in section 1016 (b) (2)(H) (IRPTA, 2004). IRPTA (2004) mandated that the President issue guidelines, in consultation with the Privacy and Civil Liberties Oversight Board,[1] to "protect privacy and civil liberties in the development and use of the ISE" (section 1016(d)(2)).

The designation of Program Manager for the ISE is provided for in section 1016(f) of IRPTA (2004). The Program Manager, in consultation with the Information Sharing Council, is responsible, in part, for assisting in the development of "policies, procedures, guidelines, rules and standards" (section 1016(f)(2)(A)(ii)) that "ensure the protection of privacy and civil liberties" (section

[1] Established by section 1061 of IRPTA.

1016(f)(2)(B)(viii)). In turn, the Information Sharing Council is required to consider input from non-federal agencies and persons in providing advice to the Program Manager in the development of "policies, procedures, guidelines, roles, and standards" for the ISE (sections 1016(g)(2) and 1016(g)(3)).

C. IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007

Section 504 of the "Implementing Recommendations of the 9/11 Commission Act of 2007" (9/11 Commission Act) amended section 1016 of IRPTA. Among other things, the 9/11 Commission Act (2007) expanded the definition of "terrorism information" (section 504(1)(D)). The 9/11 Commission Act (2007) also authorized the Program Manager to identify and resolve information sharing disputes but only among federal agencies (section 504(6)).

D. EXECUTIVE ORDER 13388[2]

Executive Order (E.O.) 13388, entitled "Further Strengthening the Sharing of Terrorism Information to Protect Americans," was signed by President Bush on October 25, 2005. E.O. 13888 stipulated the President's policy for the design and use of information systems, including protection of the "freedom, information privacy, and other legal rights of Americans in the conduct of [information sharing activities]" (2005, section 1.(b)). Section 5 of the Executive Order established the Information Sharing Council, composed of representatives from various federal agencies with the mission to "provide advice and information" concerning establishment of the ISE and to carry out the relevant duties mandated by IRPTA (E.O. 13388, 2005). Under the section entitled "general provisions," E.O. 13388 (2005) stipulated that it be implemented consistent with "applicable law, including Federal law protecting the information privacy and other legal rights of Americans" (section 7).

[2] Other, earlier, Executive Orders concerning intelligence and information sharing include E.O. 12333, *United States Intelligence Activities,* E.O. 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties,* E.O. 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans*, and E.O. 13311, *Homeland Security Information Sharing*.

Again, as was the case with IRTPA's reference to "applicable legal standards relating to privacy and civil liberties," E.O. 13388 is silent as to exactly what information privacy law is applicable. Furthermore, as for all Executive Orders, E.O. 13388 has mandatory effect only on entities within the President's direct control, i.e., federal executive branch agencies.

E. NATIONAL STRATEGY FOR INFORMATION SHARING

The National Strategy for Information Sharing (NSIS), published in October 2007, put forth the Bush Administration's plan for envisioning and achieving improvements to information sharing. The NSIS expressly recognizes the importance of "trusted partnerships among all levels of government, the private sector, and our foreign allies" to improving the ISE (NSIS, 2007, p. 1). The NSIS promotes the incorporation of state and major urban fusion centers in the national ISE, which in the strategy's view, would require those fusion centers to achieve both "a baseline level of capability to gather, process, share, and utilize information and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws" (NSIS, 2007, p. 3).

Similarly, the NSIS speaks of the need to improve information sharing with the private sector and recognizes the need to "[e]stablish mechanisms and processes to ensure compliance with all relevant U.S. laws, including applicable information privacy laws" (NSIS, 2007, p. 22). The NSIS (2007) also discusses the need to develop information privacy standards and practices in conjunction with information sharing agreements with foreign nations (p. 26).

Significantly, the ISIS recognizes that with "proper planning we can have both enhanced privacy protections and increased information sharing—and in fact, we must achieve this balance at all levels of government, in order to maintain the trust of the American people" (NSIS, 2007, p. 27). Referring to the ISE Privacy Guidelines as a set of "core principles that federal departments and agencies must follow," the NSIS calls on federal agencies to disclose protected information to non-federal entities only when those entities provide privacy

protection that is comparable to that of the federal government (NSIS, 2007, p. 28). Although the ISE Privacy Guidelines are currently binding only on federal agencies, the NSIS contemplates making receipt of federal grants by state and urban area fusion centers conditional upon meeting certain unspecified, but presumably including privacy requirements and baseline operational standards (NSIS, 2007, p. A1-5 [Appendix 1]).

III. POLICY EVALUATION CRITERIA

For purposes of this thesis, the protection of privacy rights are evaluated using several criteria derived from the stated purposes of the ISE: fostering collaboration, ensuring information sharing and protecting privacy rights. The privacy rights criterion consists of three sub-criteria: constitutionality, enforceability, and consistency of application. In addition, political acceptability is relevant and critical to consider in any policy choice and, accordingly, is included as a criterion in the analysis process.

A. FOSTERING COLLABORATION

Does the policy encourage collaboration by ISE participants? The ISE's goals include promotion of increased information sharing through creation of a collaborative culture among a diverse group of participants. Similarly, the Intelligence Reform and Terrorism Prevention Act requires that the Information Sharing Council consider input from non-federal agencies and persons in providing advice to the ISE Program Manager in the development of "policies, procedures, guidelines, roles, and standards" for the ISE" (sections 1016(g)(2) and 1016(g)(3)). Policy options are evaluated on their expected impact on increased collaboration in the ISE. A related consideration is the effect of the policy choice on stakeholder participation in the ISE.

In its publications, the PM-ISE tends to address collaboration primarily in terms of technical tools to enable ISE participants to share information and data (see ISE Implementation Plan, p. 51, ISE Enterprise Architecture Framework, pp. 67, 73–74 and the ISE Common Terrorism Information Sharing Standards (CTISS) Program Manual, Version 1.0, *passim*). A succinct definition of collaboration in a broader, non-technical sense is nowhere to be found in ISE publications though. Such an omission is not surprising, for in a 2006 report on results-oriented government, the Government Accountability Office found that there was no widely accepted definition for collaboration. However, for the

purpose of the report, the GAO defined collaboration as “any joint activity by two or more organizations that is intended to produce more public value than could be produced when the agency acts alone” (GAO-06-15, 2006, p. 6). The GAO’s definition of collaboration is appropriate for the goals of the ISE and is used in this thesis.

In its report, the GAO (2006) identified “key practices that can help enhance and sustain collaboration” (p. 32). Although these practices, and the report itself, were focused on collaboration by federal agencies, there is no reason these practices could not, and should not, be applied to the ISE. The identified key collaboration practices are:

- Define and articulate a common outcome.
- Establish mutually reinforcing or joint strategies designed to help align activities, core processes and resources to achieve a common outcome.
- Identify and address needs by leveraging resources to support the common outcome and, where necessary, opportunities to leverage resources.
- Agree on roles and responsibilities, including leadership.
- Establish compatible policies, procedures and other means to operate across agency boundaries, including compatible standards and data systems, and communicate frequently to address such matters as cultural differences.
- Develop mechanisms to monitor, evaluate and report on the results of the collaborative effort.
- Reinforce agency accountability for collaborative efforts by using strategic and annual performance plans to establish complementary goals and strategies and by using performance reports to account for results.
- Reinforce individual accountability for collaborative efforts through performance management systems by identifying competencies related to collaboration and setting performance expectations for collaboration. (GAO, 2006, pp. 4-5 [best practice examples omitted])

This thesis also uses these factors to evaluate the collaborative impact of the selected policies.

B. ENSURING INFORMATION SHARING

Improved information sharing has been a consistent and important goal of the U.S. counterterrorism effort ever since the 9/11 Commission identified intelligence gaps as one of the reasons the United States failed to adequately anticipate and respond to the attacks of September 11, 2001. As is the case when looking for a definition of collaboration, the PM-ISE's various documents do not have a succinct definition of information sharing. However, the ISE Implementation Plan, in a discussion comparing the current and expected future states of the ISE, contains a useful summary of the ISE's information sharing goal:

> The challenge remains to improve coordination of sharing within and across the five Federal communities with counterterrorism responsibilities—intelligence, law enforcement, defense, homeland security, and foreign affairs—and with [state, local, and tribal] governments, the private sector, and foreign partners to **achieve the coordinated multi-agency perspective necessary for comprehensive analysis** as well as to **ensure dissemination of the right information to the right people at the right time** [emphasis added]. (ISE Implementation Guide, 2006, p. 26)

Accordingly, policy alternatives are evaluated as to the extent they promote improved information sharing (as defined above) from the viewpoint of privacy protection. In other words, does the policy option being analyzed permit the improvement, or at least a status quo level, of information sharing? Will the selected information privacy protection system be seen as a "drag" or as a disincentive to information sharing?

C. PROTECTION OF PRIVACY RIGHTS

As discussed above, the purpose of this thesis is to analyze various options for implementation of privacy standards in the ISE, rather the specific makeup of the privacy standards themselves. Therefore, the emphasis of this section is on determining the effect of the selected options on the overall privacy protection scheme.

1. Constitutionality

Is the policy constitutionally defensible? This thesis proceeds under the assumption that considerable latitude exists to amend existing statutes or to craft new statutes to implement virtually any system of privacy protection that could eventually be chosen to apply to the ISE as long as the selected method would withstand constitutional challenge. Thus, no matter which policy option of the three discussed here, or another, completely different option, the constitutionality of any such privacy protection system is a threshold issue that must be addressed first. Any privacy protection system that does not pass constitutional muster simply—absent a constitutional amendment—cannot be implemented, no matter how well it otherwise performs in meeting the remaining criteria.

Fortunately, for advocates of minimal interference with the free flow of information, current Supreme Court jurisprudence, as has been discussed, poses little restriction. As previously discussed, Supreme Court precedents, in effect, treat information as either entirely private or entirely public, with either relatively complete protection or virtually no protection, respectively. With limited exceptions for privileged communications, such as the attorney-client privilege, once information is communicated to a third party there ceases to be a reasonable expectation of privacy and, thus, no constitutional privacy protection.

Furthermore, to the extent that the court's *dicta* in Whalen v. Roe, 429 U.S. 589 (1977), (discussed *supra*) can be seen as a guide to future rulings, the court appears to be sympathetic to the necessity for law enforcement and other government functions to acquire and use vast quantities of often personal information, if accompanied by protection to avoid unwarranted disclosures.

However, to the extent that the chosen policy option operates to preempt state privacy law, the constitutionality of the privacy option must also be evaluated in terms of the constitutional concept of federalism, which essentially concerns the allocation of power between the federal and state governments. As is discussed *infra*, the Supreme Court has two parallel lines of cases pertaining

to this issue. In a case from the first line, the court has found unconstitutional a federal statute that mandated that a state enact a particular kind of law, thereby improperly overriding that state's legislative authority. In a second line of cases, however, the court in one case upheld a federal statute where the statute's effect was to regulate state activities rather than the means by which the state regulated private parties.

2. Consistency of Application

In a 2005 Presidential Memorandum entitled "Guidelines and Requirements in Support of the Information Sharing Environment," President Bush stated that "ISE must, to the extent possible be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE" (Bush, 2005, 2.a.).

This recognition mirrored the recommendation of the 9/11 Commission that the intelligence community's work be held to a common standard for collection, processing, reporting, sharing and analysis; a recommendation that is equally applicable to the ISE. Moreover, the ISE Implementation Plan (2006) recognizes that "laws, policies, and rules [used by the various ISE participants] differ and create both real and perceived impediments to information sharing" (p. 16).

In this regard, the evaluation of this criterion proceeds on the belief that privacy protections should not vary on the basis of geographical location or the type of agency that disseminates information. Privacy protection should be the same whether a given piece of data resides on a server in New York, a computer in Arizona or is disseminated from a federal agency to a state or from a state to a local government.

To what extent do privacy protections vary from ISE participant to participant? The policy options are evaluated as to the extent to which they encourage or require uniform standards for all ISE participants.

3. Enforceability

What procedures are in place to ensure that the adopted privacy standards are actually and properly implemented? In a 2005 Presidential Memorandum, the Secretary of Homeland Security and Attorney General were directed to jointly issue standards for use by state, local, and tribal governments, law enforcement agencies and the private sector "on a mandatory basis where possible and a voluntary basis where not (Bush, 2005, 2.a.).

In the ISE Implementation Plan (2006), the need for "[d]eveloping policies and procedures for reporting, investigating, and responding to violations of policies and procedures regarding the handling of protected information" is recognized as an objective of the ISE (pp. 21-22). Another ISE objective is the implementation of mechanisms to ensure that protected information handling complies with applicable legal requirements (ISE Implementation Plan, 2006).

Even the best privacy standards possible are without effect if they are disregarded without penalty. Thus, the enforceability of each policy option is an evaluative criterion.

D. POLITICAL ACCEPTABILITY

What is the expected political opposition to the policy? According to Bardach (2005), "a feasible policy must be politically acceptable, or at least not too unacceptable" (p. 32). Political unacceptability is comprised of either too much opposition or too little support (Bardach, 2005). When a proposal is considered in a legislative setting, Jansson (2000) divides political acceptability into three practical emphases: political considerations (opposition notwithstanding a proposal's merits), rational considerations (a cost/benefit calculation, for example) and values (such as religious beliefs) that may trump the other emphases in certain situations.

This criterion, in essence, goes to the feasibility of the policy option under consideration. Even if a certain policy option has the support of working-level ISE participants, can that support be translated into adoption of the measure?

Will the selected policy option require legislative action at only the federal level to implement, or will legislation have to be passed by every state? Consideration of this criterion has implications for the overall success or failure of the policy options under consideration.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ALTERNATIVE POLICY APPROACHES FOR THE ISE PRIVACY PROTECTION

This chapter examines three different approaches to privacy protection that are currently being used in the public policy sphere: voluntary guidelines, voluntarily adopted mandatory standards and federally imposed mandatory standards. First, the PM-ISE's current system of privacy protection through the use of voluntary guidelines is examined. Next, the European system of voluntarily adopted mandatory standards is analyzed. Finally, several examples of federally imposed standards, by means of either statute or regulation, are discussed. A summary of each policy option is followed by an analysis of how that option meets the criteria of fostering collaboration, ensuring information sharing, protection of privacy rights and political acceptability.

A. STATUS QUO: VOLUNTARY GUIDELINES

This discussion concerns the various documents that comprise the PM-ISE's privacy protection guidelines. Federal agencies are nominally subject to these guidelines. However, as discussed below, the guidelines are very general in nature and the actual privacy standards to be used by federal agencies are left up to each agency to develop on its own. Furthermore, although the PM-ISE is directed to "ensure" that non-federal ISE participants have privacy protections that are at least equivalent to the guidelines applicable to federal participants, there are, again, only very general guidelines to follow. In addition, there no authorities or procedures by which the PM-ISE can ensure a certain level of privacy protection actually exists.

1. Presidential Memorandum: "Guidelines and Requirements in Support of the Information Sharing Environment"

Building on initial steps to implement the ISE-related provision of the Intelligence Reform and Terrorism Prevention Act of 2004, on December 16, 2005, President Bush directed the heads of federal executive departments and

agencies to implement various additional actions to implement the Information Sharing Environment (Bush, 2005). Although, as is discussed below, the memorandum made prominent mention of state, local, and tribal governments, law enforcement agencies, and the private sector, the memorandum was directed to and binding only on federal departments and agencies.

Among other requirements, the President directed that the "ISE must, to the extent possible be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE" (Bush, 2005, 2.a.). In that regard, the Director of National Intelligence, in coordination with various listed agency heads, was directed to issue:

> Common standards (i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use or disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that include the appropriate method for the Government-wide adoption and implementation of such standards. Such standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector. (Bush, 2005, 2.a.)

Furthermore, the Secretary of Homeland Security and Attorney General were directed to jointly issue standards for use by state, local, and tribal governments, law enforcement agencies, and the private sector "on a mandatory basis where possible and a voluntary basis where not (Bush, 2005, 2.a.). In addition, in directing the development of a common framework for information sharing, the memorandum recognized that state, local, and tribal governments, law enforcement agencies, and the private sector "must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws … and the protection of the information privacy rights and other legal rights of Americans" (Bush, 2005, 2.b.). The memorandum was criticized for

"undermining both statutory and Constitutional protections for privacy" and for not protecting the privacy of non-Americans at all (Rotenberg, 2007).

2. PM-ISE "Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment"

In a December 4, 2006 memorandum, PM-ISE Thomas McNamara issued the Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (McNamara, 2006). The Guidelines (2006) apply to "agencies," meaning federal executive agencies, as defined (section 13 and passim). The only reference to state, local, and tribal governments, law enforcement agencies, and the private sector is a direction to the PM-ISE to "work with non-federal agencies entities seeking to access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines" (Guidelines, 2006, section 11).

Federal agencies are required to adopt their own policies and procedures to ensure compliance with laws pertaining to the receipt, retention, and sharing of information and to change rules that "pose a risk to information privacy," "significantly impede" information sharing under an internal agency policy, or any other non-agency restriction that significantly impedes information sharing but does not appear to be necessary to protect information privacy rights (Guidelines, 2006, section 2). Protected information, as defined by the Guidelines (2006), can be shared in the ISE only if that information is terrorism information, homeland security information, or law enforcement information, as those terms are also defined in the Guidelines.

Agencies, in addition to have physical data security, are required to "have and enforce policies for reporting, investigating, and responding to violations of

agency policy relating to protected information" and implement audit and review mechanisms to verify compliance with the Guidelines (2006, section 7). Agencies are also directed to implement internal complaint redress procedures (Guidelines, 2006).

Several methods of governance are discussed in section 12 of the Guidelines (2006). First, each agency's senior privacy official is tasked with directly overseeing the agency's implementation of and compliance with the Guidelines (Guidelines, 2006, section 12.a.). Second, an "ISE Privacy Guidelines Committee" is to be established by the PM-ISE to provide implementation guidance, encourage consistent legal interpretations and serve as a forum for inter-agency issue resolution (Guidelines, 2006, section 12.b.). Next, the ISE Privacy Guidelines Committee is directed to consult with the Privacy and Civil Liberties Oversight Board concerning the protection of privacy and civil liberties in the ISE (Guidelines, 2006, section 12.c.). Finally, each agency, in consultation with the ISE Privacy Guidelines Committee, is required to implement its own written ISE privacy policy (Guidelines, 2006, section 12.d.).

3. PM-ISE "Privacy and Civil Liberties Implementation Guide"

About nine months after the Guidelines were issued, the PM-ISE released the "Privacy and Civil Liberties Implementation Guide" (Implementation Guide, 2007). The Implementation Guide was intended to help federal agencies implement the Guidelines, as a framework focusing on federal agency issues. The Implementation Guide, however, was "not specifically applied for use by nonfederal entities, notably state, local, and tribal entities" (2007, Overview at p. 1). Instead, non-federal entities were directed to refer to privacy guidance in Guideline 8 of the U.S. Department of Justice's *Fusion Center Guidelines* (Implementation Guide, 2007, Overview). The two-page Guideline 8 suggests that fusion centers develop, publish and follow a privacy and civil liberties policy that complies with the *National Criminal Intelligence Sharing Plan* and other sources of privacy protection practices (Fusion Center Guidelines, n.d.).

The Implementation Guide "describes best practices and a methodology to ensure implementation of the protections and safeguards required by the ISE Privacy Guidelines" (2007, Overview at p. 2). The Implementation Guide is not prescriptive but is to be used by each agency to develop its own privacy policy that reflects its "unique environment" (2007, Overview at pp. 2-3). The implementation process is described as "iterative" in recognizing that reevaluation may be needed if new requirements or sharing arrangements are implemented (Implementation Guide, 2007, Overview at pp. 3-4). After a brief review of the authorities forming the basis for the ISE, the Implementation Guide (2007) discusses a two-stage implementation process. The first stage concerns the identification and assessment of applicable policies and law and assuring that there are no gaps in the coverage of privacy policy protections (Implementation Guide, 2007, p. 7). The second stage uses the same "identify, assess, protect" process for agencies to demonstrate their compliance with the ISE Privacy Guidelines (Implementation Guide, 2007, pp. 7-8). A graphic showing the implementation stages appears below (Figure 1).

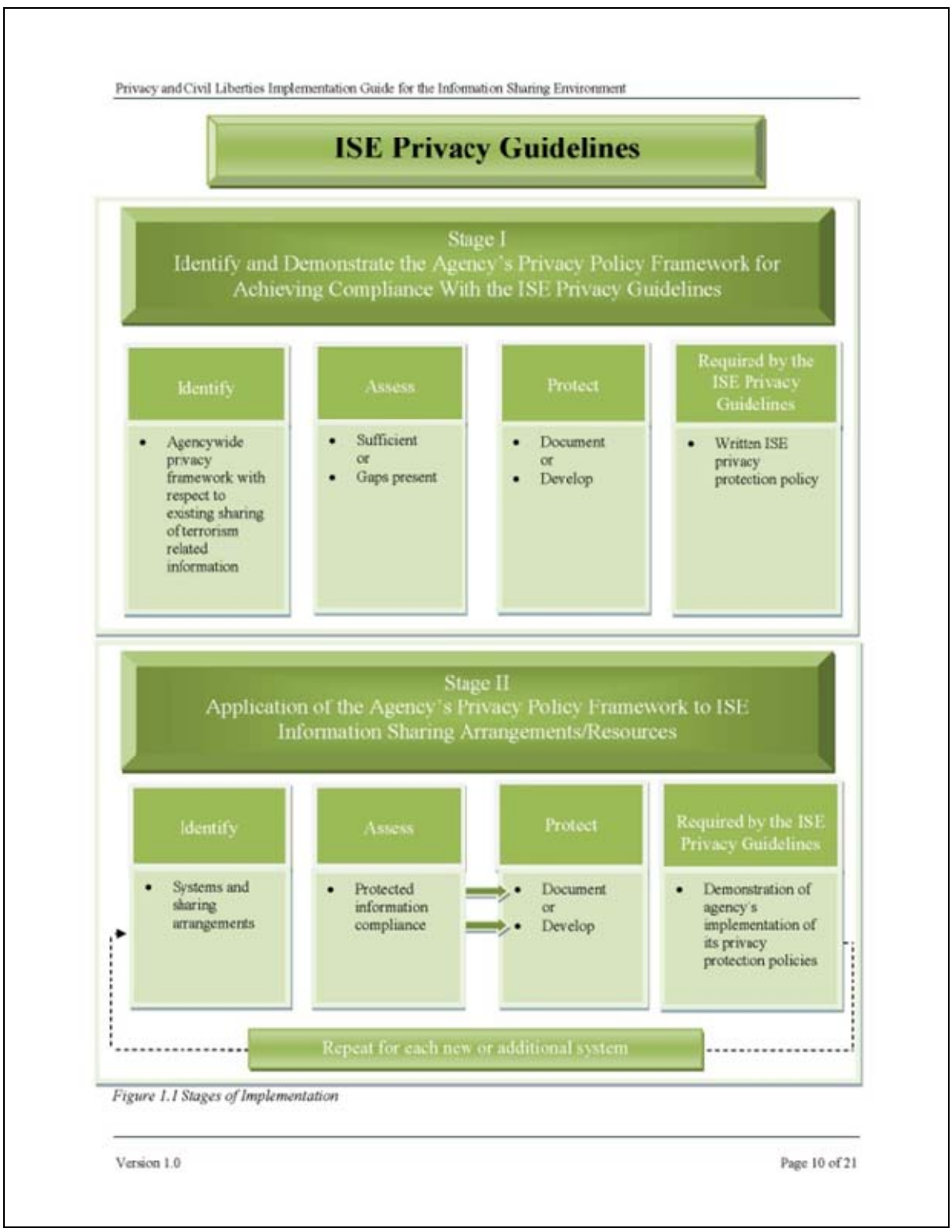

Figure 1. Implementation Guide (From Implementation Guide 2007, p.10)

The remainder of the Implementation Guide (2007) contains detailed, step-by-step instructions for using the two-step implementation process.

4. PM-ISE "Privacy and Civil Liberties Implementation Manual"

In 2008, the PM-ISE released the *Privacy and Civil Liberties Implementation Manual*, an online compendium of tools and resources to assist efforts to implement the Privacy Guidelines. The *Implementation Manual* (2008) consists of six Web-based sections, entitled, "Overview," "Senior Leadership," "Agency Privacy Officials," "Federal Employees," "Non-Federal Entities," and, finally, "Resources."

a. Overview

In addition to an issuance memorandum from the PM-ISE to federal department and agency heads, this section includes an Executive Summary, which covers the creation and function of the ISE, the role of the PM-ISE and ISE privacy guidelines (Implementation Manual, 2008). Also included is an online document entitled "Background on Protecting Information Privacy and Other Legal Rights in the context of the ISE," which includes, as the document's title implies, a discussion of the meaning of information privacy and civil rights and liberties, followed by a summary of the ISE Privacy Guidelines.

b. Senior Leadership

This section discusses the key role senior leadership plays in implementing the ISE and its attendant Privacy Guidelines and reiterates the privacy protection policies that each agency must implement and follow (Implementation Manual, 2008).

c. Agency Privacy Officials

Directed to the agencies' senior officials with "overall responsibility for information privacy issues," this section includes various documents relating to the role and composition of the Privacy Guidelines Committee, in addition to

providing a direct link to the Implementation Guide (Implementation Manual, 2008). This section also includes an online document entitled, "Key Issue Guidance: (Implementation Manual, 2008). The Key Issues Guidance provides additional, in-depth guidance and optional "exemplary" privacy protection elements concerning several privacy protection issues, including redress, notice mechanisms, data quality, data security, accountability, enforcement and auditing (Implementation Manual, 2008).

d. Federal Employees

This section highlights the essential "front line" role of federal employees in implementing the Privacy Guidelines (Implementation Manual, 2008).

e. Non-Federal Entities

A statement is made in this section that the "materials on this Web page currently focus on …sharing between federal agencies and do not specifically apply to non-federal entities, such as State, local, and tribal entities or the private sector" (Implementation Manual, 2008). However, a linked page entitled "Working with State, Local, and Tribal Governments" (http://www.ise.gov/pages/privacy-slt.html) notes that the ISE Privacy Guidelines Committee has set up a State, Local, and Tribal Working Group to develop privacy protections for information sharing with the federal government (Implementation Manual, 2008). The state, local and tribal government page also includes links to the aforementioned Fusion Center Guidelines, Department of Justice privacy policy development guide, National Criminal Intelligence Sharing Plan, 28 CFR Part 23 (privacy standards for fusion centers that receive certain types of federal funding; discussed *infra*) and guides for state, local and tribal law enforcement on civil rights, law enforcement intelligence and the intelligence fusion process (Implementation Manual, 2008).

f. Resources

This section includes links to various ISE background information, including Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, Executive Order 13388, the ISE-PM Privacy Guidelines Memorandum, Section 504 of the Implementing Recommendations of the 9/11 Commission Act of 2007, and the National Strategy for Information Sharing—all of which are discussed *supra*. The section also includes links to various privacy protection implementation tools.

5. State Privacy Laws

A full survey of the myriad of state privacy laws is beyond the scope of this thesis. Suffice it to say for purposes of this thesis that state privacy law is a balkanized conglomeration of hundreds of laws and regulations found in countless nooks and crannies of various volumes of state statute books—called a "bewildering assortment" of protections (Solove,2002, p 1172) and referred to as "uncharted territory" (Schwartz, 1995, p. 604). According to Schwartz (1995), although some data protection is on the books everywhere, "no two states have adopted exactly the same system of regulation" (p. 604) and, furthermore, this lack of comprehensive laws at the state level "creates gaping weaknesses" in data protection (p. 605). Finally, most states lack a statute equivalent to the Privacy Act (Solove, Rotenberg, 2003).

This uneasy combination of state and federal laws leads to "a rather haphazard and unsatisfactory response to each of the privacy concerns" (Reidenberg, 1992, p. 208). Reidenberg (1992) goes on to say that "[d]ifferences in privacy protection among the states could readily have adverse or distorting effects on interstate commerce and international data flows" leading to his recommendation that "it may be most appropriate to adopt any new rights at the federal level" (p. 238).

Solove (2002), recognizing that information no longer remains localized, concurs, believing that the most efficient and effective method to regulate data

flows is through “a strong national information policy rather than widely diverging state public record regimes” (p. 1200). He believes that this “federal baseline” would provide a minimum level of uniform protection to public records but should permit states to enact stricter requirements (Solove, 2002, p. 1200). Solove (2002) suggests that this uniform, nationwide privacy protection could be done either by extending the federal Privacy Act to the states or by requiring each state to enact its own law equivalent to the Privacy Act. Although Schwartz (1995) agrees that federal mandates can be beneficial where national uniformity is needed or state laws are deficient, he asserts that omnibus state laws are also needed to ensure full protection.

6. Analysis

a. Fostering Collaboration

The current PM-ISE privacy program clearly makes privacy protection a central and common goal of entire ISE community. Privacy protection is a recurring theme in PM-ISE documents, including the Implementation Plan. The plan for achieving privacy protection is essentially reliant on the voluntary efforts of the ISE members to bring their own protection programs into alignment. There is no plan for leveraging ISE member privacy programs to produce an outcome greater in value than any single privacy program in isolation.

Furthermore, although several ISE documents refer to the need to ensure by all ISE participants with applicable information privacy laws the current system is mandatory only for federal agencies. Although the NSIS calls on the federal government to share information with non-federal parties only when those parties have privacy protection comparable to the federal protections, that document is aspirational rather than binding for any ISE participant.

There exists, at present, no established cross-boundary agency standards for privacy protection. In addition, there is currently no ISE-wide plan to ensure organizational or individual accountability for collaborative privacy

protection. Despite the recognition on the part of the federal government of the need to ensure privacy protection at a certain base level, the current PM-ISE system for privacy protection is, in essence, a completely voluntary system with little control. Collaboration is not fostered by the current voluntary privacy guidelines.

b. Ensuring Information Sharing

The potential impact of voluntary privacy protection standards could arguably been seen to have either positive or negative effects on information sharing itself—getting the right information to the right people at the right time. Where ISE participants are not actually required to ensure that the recipient of the information shared has compliant privacy standards, the resultant time savings from skipping this step would help speed the exchange of information.

However, having each participant operate under its own set of privacy rules would run counter to, or at least not improve, coordinated multi-agency information sharing. Furthermore, as discussed above, some ISE participants may be more reluctant to share information if they believe information recipients have inadequate protections in place or are unsure if protections are adequate. Also, public support for information sharing may suffer if privacy concerns exist, and as public support often correlates with political support, overall support for information sharing may decrease.

On balance, the lack of uniform privacy protection standards would seem to have a negative effect on information sharing.

c. Protection of Privacy Rights

1) Constitutionality. As discussed above, the Supreme Court, on the whole, seems to be well disposed to the use of personal information for certain government functions—presumably including counterterrorism purposes. However, support for that use is predicated upon the existence of adequate statutory or regulatory protections. The current system of

voluntary guidelines results in privacy protection that could conceivably range from very extensive to less than optimal. The variability of this voluntary system may lead to a court's finding that the wide disparity in privacy protection among the various ISE participants provides insufficient privacy safeguards.

The Supreme Court has treated federal efforts to impose requirements on states in one of two ways—either as an impermissible usurpation of state legislative authority or a permissible exercise of power to regulate state activities. Neither line of reasoning would come into play in the current ISE system of voluntary guidelines, however, as there are effectively no federal requirements at play.

2). Consistency of Application. Although ISE participants are encouraged to adopt the PM-ISE's privacy guidelines, there is no requirement to do so. As demonstrated in this thesis, the extent of privacy protection provided by state law is highly variable. In addition, no state has a comprehensive statute equivalent to the Privacy Act of 1974, which is applicable only to federal agencies. Thus, the consistency of application must be considered very low.

3). Enforceability. Again, although many NSIS and other documents speak of ensuring adequate privacy protection by all ISE participants, including by withholding information to participants with insufficient protections, there is no practical means by which to enforce the PM-ISE privacy guidelines. There is currently no system to enforce privacy protections by means of withholding information and no procedures for reporting, investigating or responding to failures, or apparent failures, to follow the privacy guidelines.

In sum, the current system of voluntary privacy standards appears to provide inconsistent application, no means of enforcement and may be susceptible to constitutional challenge. Thus, the current system offers insufficient privacy protection.

d. Political Acceptability

One benefit of the current voluntary guidelines system is that because it, in effect, does not require federal agencies to do anything beyond what they were already required to do to protect privacy, and because it does not impose any mandates on other, non-federal ISE participants, little political opposition is likely to be encountered. Indeed, this author is unaware of any ISE participant challenges to the PM-ISE's voluntary privacy guidelines. Thus, the current program of voluntary guidelines is deemed highly politically acceptable.

B. VOLUNTARILY ADOPTED MANDATORY STANDARDS

One potential policy choice for ISE privacy protection, involving voluntarily adopted uniform standards, is contained in the Europol Convention and the Council of Europe Convention on Personal Data Processing. These two European Conventions are potentially applicable to the U.S. ISE because, as liberal democracies, the U.S. and Europe share an enlightenment heritage, and legal systems that have a common basis (Bignami, 2007).

In one illustration of that shared legal heritage, Europe and the United States draw on each others' conception of privacy. At their core, both Europe and the U.S. systems of law value privacy, defined as "a certain freedom from scrutiny of others and a certain amount of autonomy in making life decisions" (Bignami, 2007). In fact, the European Data Processing Convention's framework is based on the "Fair Information Practices" contained in a 1973 U.S. Department of Health, Education and Welfare report that also formed the basis for the U.S. Privacy Act of 1974 (Solove, 2008, p. 186).

Counterterrorism measures in Europe have raised strong and widespread concerns about the relationship between privacy and security, especially as those factors relate to ensuring accountability by government authorities (European Security: High Level Study on Threats, Response and Relevant Technologies Consortium [ESSTRT], 2006). Of particular interest is the "strong feeling across Europe that if [counterterrorism] responses are excessive, the

values of democratic societies could be undermined—thereby weakening the struggle against terrorism" (ESSTRT, 2006, p. 20). Thus, there is recognition on the part of many Europeans that the optimal response to terrorism is neither too much nor too little—that privacy and security must be balanced. Within that milieu, the privacy of personal data is seen as a fundamental right (Bignami, 2007; Kochems, 2006). The following documents reflect that recognition.

1. European Convention of Human Rights and Fundamental Freedoms

European concern with privacy long predated the current struggle against terrorism, however (Bignami, 2008). Shortly after the end of World War II, on November 4, 1950, the Council of Europe adopted the world's first legal document to protect human rights, the Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe, n.d.). Article 8 of the Council of Europe Convention of 1950 firmly established privacy protection as a critical human right (Solove, Rotenberg, 2003, p. 688).

> **Article 8—Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (European Convention on Human Rights and Fundamental Freedoms, 1950)

The first requirement of Article 8 is that any interference with the right of privacy be lawful. Once the interference has been determined to be in accordance with law, that interference must be found to be both necessary and intended to further one of the listed permissible purposes, which include national security, public safety and crime prevention (European Convention on Human Rights and Fundamental Freedoms).[n.d.] Article 8 recognizes that protecting

national security and public safety are legitimate purposes for interference with personal privacy rights, but it also recognizes that that legitimate interference with privacy must be proportional (Bignami, 2007).

Proportionality, in turn, requires an examination as to whether action in question will achieve the stated purpose, whether alternative actions would impose a lesser burden on privacy and whether the least burdensome alternative nonetheless has an intolerable impact on privacy such that the action will not be permitted (Bignami, 2007). In the end, in determining proportionality, the more important the right the higher the burden on the government; the more important the public purpose, the lower the burden on the government (Bignami; 2007).[3]

2. European Court of Human Rights and the Council of Europe Convention on Data Protection

Article 8 of the European Convention of Human Rights and Fundamental Freedoms does not exist in a vacuum, however. The provision is "given effect by the decisions of the European Court of Human Rights and also by the Convention on Data Protection established by the Council of Europe in 1980" (Solove, Rotenberg, 2003, p. 688).

In a 2008 paper examining the protection of privacy in counterterrorism, the Council of Europe's Commissioner for Human Rights examined the case law of the European Court of Human Rights (ECHR) and found that data protection

[3] Article 10 of the European Convention of Human Rights and Fundamental Freedoms, which includes elements concerning the free flow of information, presents a further counterpoise to Article 8.
Article 10—Freedom of Expression
1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. (European Convention on Human Rights and Fundamental Freedoms, 1950).

principles are well developed. According to the Commissioner for Human Rights (2008), for any use of Article 8 to interfere with privacy rights the ECHR requires a specific legal basis, with specific procedures, rather than allowing reliance on a broadly written statute. However, interference with privacy rights is not automatically permitted just because public safety or another listed purpose is implicated (see Rotaru v. Romania, E.C.H.R., 2000). The ECHR applies "necessity" and "proportionality" considerations (discussed *supra*) and requires that "hard" (factual) and "soft" (intelligence) data should be clearly distinguished, especially when privacy rights of contacts and associates of a suspect, rather than of the suspect himself are at issue (Commissioner for Human Rights, 2008). Information coming from private parties (such as credit reference agencies) requires additional safeguards and, furthermore, access to personal information should only be allowed on a case-by-case basis (Commissioner for Human Rights, 2008).

3. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and associated Additional Protocol

Drawing on the European Convention of Human Rights and Fundamental Freedoms, and recognizing the immense growth of electronic data processing, in 1981 the Council of Europe promulgated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Processing Convention).As its title implies, the purpose of the Data Processing Convention is, in particular, the protection of privacy with regards to automated processing of personal data, without regard to nationality or state of residence; in that regard, the signatory parties to the Convention are required to apply various data protection principles and safeguards (Data Processing Convention, 1981, Articles 1-8). State parties are allowed to derogate from the Convention for "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences" (Bignami, 2007; Data Processing Convention, 1981, Article 9). Parties to the convention are obligated to cooperate with each

other in implementing the convention's provisions (Article 13), and in extending protections of the convention to data subjects residing abroad (Article14) (Data Processing Convention, 1981). Parties are permitted to refuse requests for assistance in certain circumstances, including where such requests are incompatible with a party's sovereignty, security or public policy (Data Processing Convention, 1981, Section 16).

In late 2001, in recognition of ever-increasing cross-border information flows, including to and from countries that were not parties to the convention, improvements to the Data Processing Convention were proposed (Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data on Supervisory Authorities and Transborder Data Flows (2001); Additional Protocol [2001]). Although it has not yet come into force, the Additional Protocol (2001) would set up a system of supervisory authorities set up by each party to ensure that its nation's laws comply with the Data Processing Convention, and to hear claims by any person pertaining to privacy protection under the convention (Articles 1 and 2, respectively).

4. Europol Convention

Europol, the European Police Office, was created pursuant to a provision in the Maastricht Treaty on European Union of 1992 and commenced limited operations in 1994 (Europol Web site, 2008). Its original mission was to fight drugs, but that mission was later expanded to cover other types of crimes, including international crime as codified by the Europol Convention adopted in October 1998 (Europol Web site, 2008).

As a primary component of its crime-fighting mission, Europol gathers, analyzes and shares information about criminal organizations among its member

nations (DiPaolo, A. and Stanislawski, B., n.d.).[4] A majority of provisions of the Europol Convention pertain to the computerized information sharing system used by the organization. In particular, Article 14(1) of the Europol Convention states that a member country shall

> under its national legislation, take the necessary measures in relation to the processing of personal data in data files in the framework of this Convention to ensure a standard of data protection which at least corresponds to the standard resulting from the implementation of the principles of the Council of Europe Convention of 28 January 1981 [Article 14(1) of the Europol Convention]

Furthermore, member nations are not permitted to transfer personal data under the convention until the recipient member has promulgated the requisite national legislation (Europol Convention, Article 14(2), 1998). Article 18 of the Europol Convention addresses the communication of data to third countries and bodies. Personal data may be shared with third countries or bodies for the preventing or combating criminal offenses, where the third party has ensured an adequate level of data protection (Europol Convention, Article 18, 1998).[5] To determine whether a third party's data protection is adequate, Article 18(3) lists the considerations to be addressed, including "the nature of the data," "the purpose for which the data is intended" and "the duration of the intended processing" (Europol Convention). Article 23 mandates the designation of a national supervisory body to independently monitor the rights of individuals pertaining to data input, retrieval and communication, and it provides an express a right of redress petition to the national supervisory body by affected individuals.

---

[4] Statewatch, a European civil rights and watchdog organization notes that the Europol information system includes data on convicted and suspected persons, as well as "persons who there are serious grounds for believing will commit criminal offences," in other words "not-yet-but-soon-to-be suspects" (Statewatch, p. 2).

[5] In a December 2001 agreement, and a December 2002 supplemental agreement, Europol and the U.S. agreed to exchange strategic, technical and personal data relating to certain criminal activities, including terrorist activities (Agreement between the United States of America and the European Police Office, 2001; and Supplemental agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information, 2002).

To further protect individual privacy rights, Article 24 of the Europol Convention provides for a independent, joint (i.e., multistate) supervisory body, which reviews Europol's activities, including "monitor[ing] the permissibility of the transmission of data originating from Europol" [Article 24 of the Europol Convention, 1998]

5. Analysis

As previously discussed, although Europe and the United States share a common legal heritage and once had similar approaches to privacy law, the two regions of the world more recently have taken a divergent course in protecting the right of privacy, as evidenced by the various European privacy measures discussed *supra*. Although American Fair Information Practices influenced European privacy concepts, European law expanded and adapted as technology became more advanced, but American privacy law did not (Bignami, 2007).

Since the 1970s, U.S. privacy law has focused on protecting specific sectors of the economy, such as financial information, while European privacy law has broadened in scope, applying to all personally identifiable information without distinguishing between either the type of data uses or the public or private nature of the party involved in the data use in question (Bignami, 2007; and Solove, Rotenberg, 2003). Both systems distinguish between the content of communications and the incidents of communications (e.g., lists of phone numbers dialed), with the U.S. protecting only the content, and Europe protecting both content and incidents with the proviso that surveillance of content is considered more intrusive than incidents in the European system (Bignami, 2007).

Nonetheless, "[d]ivergences between the ways different societies protect privacy do not necessarily stem from conceptual differences about privacy" (Solove, 2008, p. 185). Solove (2008) goes on say that in the end "the degree to which so many countries recognize the same set of privacy problems is more significant than the divergences" (p. 186). He also recognizes that there is a cross-fertilization of nations' "cultural understanding of privacy" at work (Solove,

2008, p. 186). Similarly, at least one commentator has argued that an increased convergence of approaches to the conception of privacy makes it more likely that the U.S. will increase its privacy protections to approach the protections provided by Europe (Shaffer, 2000).

Given the common underpinnings in the conceptual understanding of privacy between Europe and the United States, this analysis will evaluate the likely effects of a theoretical implementation of a system of voluntarily adopted, mandatory privacy standards based on the European system.

a. Fostering Collaboration

Privacy is clearly, and succinctly, recognized as a critical human right by the Council of Europe. The various European agreements that touch on privacy all flow from that central holding.

In addition, the European agreements discussed above generally have well-developed procedures for cross-agency implementation. Roles and responsibilities are likewise relatively well-defined. Cultural differences between countries are recognized by allowing each country to interpret on its own application of the listed exceptions to the conventions—at a potential cost to consistency, as discussed below.

A key component of the European system is the presence of supervisory authorities, which are "privacy agencies that are responsible for investigating privacy complaints, issuing annual reports, and serving as a privacy ombudsman" (Solove, Rotenberg, 2003, p. 731). This system serves as both as a tool for monitoring the collaborative effort and as a means for enforcing accountability. Under this policy option, collaboration is enhanced through common standards of privacy protection, and procedures, including supervisory authorities, for implementing those standards.

b. Ensuring Information Sharing

A requirement that ISE ensure that the recipient of the information shared has compliant privacy standards would entail an additional responsibility when sharing information, although the compliance status of many information recipients, especially ones with which the information-providing agency frequently shares, would likely be known in advance. Exceptions to information sharing mandates and mandates to share information regardless of recipient privacy protections (such as in matters of national security) would also add to transactional costs.

Having each participant operate under a common set of enforceable privacy rules that are mandatory in effect would probably improve coordinated multi-agency information sharing. ISE participants may be more likely to share information if they believe information recipients have adequate privacy protections in place. For those reasons, uniform protections would also tend to increase public and political support (and concomitantly, resources) for the ISE.

In summary, the European system of voluntarily adopted, mandatory requirements that are applicable to all information-sharing participants appears to have a positive effect on information sharing.

c. Protection of Privacy Rights

1). Constitutionality. To the extent that ISE participants voluntarily agree to mandatory privacy standards, courts are more likely to find that adequate privacy protection is in place to permit the acquisition and use of personal information for law enforcement and other necessary government functions. One key to challenges on this ground would be the reasonable and constrained use of exceptions to the prohibition of information transfers to parties without sufficient privacy protections in place.

The relationship of multiple nations within Europe can be analogized to federal relationship of national to state governments in U.S. One

potential issue with the European system that could also arise in the U.S. pertains to the tension between police cooperation and sovereignty. In the area of internal security—presumably including threats to that security by terrorism—European countries have been especially protective of their sovereignty (Storbeck, 1999). As discussed by Storbeck (1999), the tension arises from the fact that maintaining internal security is too big a task for a country to provide on its own, but the resulting need for international cooperation requires a country to give up some control of its sovereignty in order to cooperate successfully. To Hijmans (2006), the tension stems from a "constitutionally enshrined distrust of another country's legal system" (paragraph 12). Skinner (2002) characterizes the tension as being between sovereignty and the protection of policing traditions; he believes that the tension inherent in police cooperation treaties may represent the limits of cooperative efforts in the EU. Interestingly, Skinner also believes that this tension has led to European police cooperation having been "approached through political initiatives and information sharing frameworks, which are deemed helpful but not damaging to sovereignty" (2002; p. 206).

In the U.S., states also tend to be protective of their sovereignty. Although this option concerns voluntarily adopted mandatory standards, sovereignty may become an issue in at least two ways. First, an argument might be made that although adoption of the standards is nominally voluntary, the effect of prohibiting information sharing with non-complying entities—except for certain narrow exceptions—would be mandatory in nature and preemptive in effect. As previously discussed, the two lines of Supreme Court cases concerning federalism and federal regulatory efforts would have to be considered. Second, sovereignty tensions may give rise to cooperation issues in effectuating the standards. Accordingly, constitutional issues are a possible concern with this option.

2). Consistency of Application. Another issue with the European system concerns how information is treated in the three pillars(i.e., broad policy areas) (Skinner, 2002). The first pillar addresses social and

economic issues, where information sharing privacy is heavily regulated. The less-regulated nature of the second (foreign and security policy) and third (justice and home affairs), is reflected, as discussed above, in exceptions to privacy protection provisions for security, public safety and criminal enforcement in the Convention on Human Rights and Fundamental Freedoms and the Data Protection Convention and national interest in the case of the Europol Convention. Countries are permitted to interpret the application of the exceptions using their own laws, thereby potentially leading to inconsistency in application (Guymon, 2000). Another potential consistency issue with use of the European system for national supervisory bodies in the ISE context is that although at least nominally independent, their powers vary (Bignami, 2007).

Even in the case of the more heavily regulated first pillar data flows, the issue of "the lack of enforcement action appears to be creating a gap between law and practice" in the area of cross-border privacy protection (Organisation for Economic Co-operation and Development [OECD], 2006, p. 19). The gap stems from "insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints" (OECD, 2006, p. 3).

In summary, the European system suffers from certain inconsistencies that should be considered when implementing privacy protections standards for the ISE.

3). Enforceability. The European system is based on common standards, which once voluntarily adopted by means of becoming a party to a convention, are mandatory in effect. Nations are required to amend their domestic law to the extent necessary to meet the common privacy standard. Compliance is effectuated by several methods. First, countries are required to have an internal independent supervisory body to monitor privacy rights and to act as a place where requests for redress can be heard. Second, a joint multilateral supervisory body is empowered to ensure compliance with the common standards and resolve disputes between signatory parties. Finally,

individual parties are restricted from transferring data to any party or non-party who has insufficient privacy protections in place, with limited exceptions where national interest necessitates such a transfer notwithstanding privacy considerations (Bignami, 2007).[6]

Privacy protections in the European system are highly enforceable. Beyond the general mandatory effect of the privacy standards, compliance with those standards is enforced through an internal supervisory body, a multilateral supervisory body and restrictions on data transfer to non-complying parties.

d. Political Acceptability

Although mandatory in effect, privacy standards under this policy option would still be implemented on a voluntary basis by each ISE participant. To the extent that this voluntary system would be seen by ISE participants as, in reality, mandatory in effect, political resistance is likely to be increased. The issue of political acceptability under this policy option would be compounded by the necessity for each ISE participant to agree to the mandatory standards. In other words, the political acceptability of the program to each implementing jurisdiction would have to be ascertained.

Would the resultant system, in Bardach's words, at least not be "too unacceptable?" As with any such undertaking, the answer to that question would depend on the totality of factors at work at the time the system is considered.

C. FEDERALLY MANDATED PRIVACY STANDARDS

The following three federal statutory or regulatory schemes are illustrative of programs where the federal government has mandated the use of uniform privacy protection by non-federal entities, including other forms of government.

[6] It should be noted that this exception concerns the transferor nation's interest and not the interests of the putative transferee nation.

Two of the schemes specifically provide for preemption of state law in certain circumstance, and all three schemes provide examples of various methods to enforce compliance with their provisions.

1. Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1301, *et seq*.)

a. Background

Similar to the current situation concerning privacy law, until the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed, "personal health information was protected by a patchwork of federal and state laws" (Gosfield, 2002). HIPAA was the "first comprehensive federal protection for the privacy" of certain health information (Gosfield, 2002).

Title II of HIPAA, known as the Administrative Simplification provisions, *inter alia*, required that the U.S. Department of Health and Human Service (HHS) promulgate national standards for health care information privacy (HHS, 2003).[7] The resultant privacy standards, known as the Privacy Rule, came into effect starting in 2003 (HHS, 2003).

The Privacy Rule applies to any person or organization ("covered entities") and persons or organizations ("business associates") that perform certain activities or functions for covered entities, involving individually identifiable health information (called "protected health information" or "PHI") (HHS, 2003). PHI covers a broad range of health information, including a patient's name, social security number, date of birth or any information that could be used to identify a patient (Gosfield, 2002). Health information that has been "de-identified" may be used or otherwise disclosed without restriction (HHS, 2003).

[7] This requirement would only come into effect if Congress did not enact its own privacy legislation within three years of HIPAA's passage. Congress did not do so; accordingly, HHS's Privacy Rule was later issued.

In essence, the Privacy Rule is designed to limit the circumstances under which covered entities may disclose PHI. A basic principle of the Privacy Rule is that a covered entity may only use, disclose or request only the minimum necessary amount of information that is needed to accomplish its purpose (HHS, 2003). PHI may only be used or disclosed if the Privacy Rule allows or requires it, or if the subject of the PHI give written authorization to do so (HHS, 2003). Disclosure is required when requested by the subject of the PHI (or the subject's representative), or to HHS for compliance investigation and reviews or enforcement action (HHS, 2003).

Disclosure is permitted in several cases, including for treatment or when it is in the public interest (HHS, 2003). Disclosure is also permitted in response to court order or to law enforcement officials for law enforcement purposes (HHS, 2003). In addition, authorization is not required to use or disclose information for certain essential government functions, including military missions and intelligence and national security activities (HHS, 2003).

b. State Law Preemption

HIPAA, through the Privacy Rule, generally preempts contrary state laws (HHS, 2003). For the purposes of the Privacy Rule, "contrary" means that compliance by the covered entity with both the state law in question and federal requirements would be impossible, or the state law is "an obstacle to accomplishing the full purposes and objectives" of HIPAA (HHS, 2003, p. 17). There are some exceptions to preemption of contrary state law, though. State laws that provide greater privacy protections or rights with respect to PHI are permitted, as are state laws that pertain to the reporting of "disease or injury, child abuse, birth, or death," for certain public health reasons or for certain health plan reporting (HHS, 2003, p. 17). Other reasons include HHS determinations that the state law at issue, for example, "is necessary for serving a compelling

public health, safety, or welfare need," and, if a privacy rule provision is involved, the HHS Secretary determines that, on balance, the privacy intrusion is warranted (HHS, 2003, p. 17).

c. Compliance

In enforcing the Privacy Rule, HHS first seeks the cooperation of covered entities, in some case providing assistance to promote voluntary compliance (HHS, 2003). Persons are permitted to file complaints under the Privacy Rule, and covered entities must cooperate in the investigation or review of those complaints (HHS, 2003). Failure to comply with a requirement of the Privacy Rule may subject a covered entity to a civil penalty of $100 per violation, up to $25,000 per year for multiple violations of the same Privacy Rule provision (HHS, 2003). Civil penalties are not imposed where the "violation is due to reasonable cause and did not involve willful neglect," and the covered entity corrects the violation in a timely manner (HHS, 2003, p. 17). Criminal penalties of up to a year in prison and a $50,000 fine are reserved for case where a person knowingly obtains or discloses PHI in violation of HIPAA (HHS, 2003).

2. Code of Federal Regulations, Title 28, Part 23, Criminal Intelligence Systems Operating Policies (28 C.F.R. Part 23)

a. Background

Promulgated in 1993, the Criminal Intelligence Systems Operating Procedures (28 C.F.R. Part 23; Part 23) were intended to ensure that all criminal intelligence systems receiving federal funds under the Omnibus Crime Control and Safe Streets Act of 1968 protected the privacy and other constitutional rights of individuals. "Criminal Intelligence Systems, for the purposes of Part 23, includes "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information (§ 23.3(b)(1)). "Criminal Intelligence Information" is defined, in turn, as evaluated data that meets system submission criteria and is

"relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity" (§ 23.3(b)(3)).

Part 23 justifies policy guidelines for federally funded projects on the grounds that "the collection and exchange of intelligence data necessary to support control of serious criminal activity may represents potential threats to the privacy of individuals to whom such data relates" (§ 23.2).

b. Privacy Principles

Among the provisions of Part 23 (1993) pertaining to privacy and information sharing is a prohibition of information which is in violation of any federal, state or local law (§ 23.20(d)). In multi-jurisdictional systems, the funded system is responsible for ensuring that no violative information enters the system, either by examining supporting information from the submitting agency, or by properly delegating the responsibility to a participating agency, who is subject to inspection and audit procedures ((§ 23.20(d)). Dissemination of criminal intelligence information is on a "need to know" or "right to know" basis (§ 23.20(e)). Furthermore, dissemination is permitted only to agencies that agree to follow information procedures consistent with Part 23, except when necessary to "imminent danger to life or property" (§§ 23.20(f)(1) and (f)(2)). The grant-making agency must approve a formal information exchange procedures with other information systems (§ 23.20(j)).

c. Enforcement

Sanctions must be adopted for unauthorized use or disclosure of information in the system (§ 23.20(m)), and the system must conduct inspections and audits of participating agencies (§ 23.20(n)). However, the Attorney General is permitted to waive any requirement in Part 23:

> upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that

such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law (§ 23.20(o)).

In order to receive funding, intelligence systems must agree to adhere to all requirements in § 23.20 (§ 23.30). In addition, funded projects must meet certain criteria, including that they be multi-jurisdictional ((§ 23.30(b)(3)) and that a designated official will retain control and supervision of information collection and dissemination (§ 23.30(c)). In addition, the designated official must certify in writing that the official takes full responsibility and accountability for any information used or shared (§ 23.30(c)). Similar requirements apply to actions taken on behalf of a joint entity (§ 23.30(d)). Funded systems are subject to monitoring and audit, and funding requires compliance with the provisions of § 23.20 (§ 23.40).

3. Driver's Privacy Protection Act of 1994 (18 U.S.C. §§ 2721-2725)

a. Background

Passed as an amendment to the Violent Crime Control and Law Enforcement Act of 2004, the Drivers Privacy Protection Act (DPPA) was originally intended as an anti-stalking measure (Electronic Privacy Information Center, n.d.). The DPPA prohibits a state department of motor vehicles (or employee or contractor thereof) from knowingly disclosing or making available any personal information obtained in connection with a motor vehicle record, subject to certain exceptions (DPPA, § 2721(a)(1)). The release or use of "highly restricted" personal information requires express consent, subject to a more limited number of exceptions than for non-highly restricted personal information (DPPA, § 2721(a)(2)).

"Personal information" includes any information that identifies an individual, except information on a person's ZIP code, accidents, driving violations or driver's status (DPPA, § 2725(3)). "Highly restricted personal information" refers to a person's photograph, social security number or a

person's medical or disability information (DPPA, § 2725(4)). "Motor vehicle record" means any record pertaining to a driver's license, vehicle title or registration or motor vehicle division-issued identification card (DPPA, § 2725(1)). "Express consent" is defined as written consent, including electronic signatures (DPPA, § 2725(5)).

b. Privacy Principles

The DPPA provides for several exceptions to the general prohibition of release and use of certain motor vehicle records. Permissible uses for both "personal information" and "highly restricted personal information" include use for government functions (§ 2721(b)(1)), use in legal proceedings (§ 2721(b)(4)), use in certain insurance matters (§ 2721(b)(6)) and use related to a commercial driver's license (§ 2721(b)(9)) (DPPA). Permissible uses of "personal information" add such matters as motor vehicle or driver safety or theft (§ 2721(b)(2)), use by legitimate businesses for verifying the accuracy of information submitted by the individual (§ 2721(b)(3)) and other use specifically authorize by state law, if that use is related to motor vehicle operation or public safety (§ 2721(b)(14)) (DPPA). Resale and redisclosure of personal information is restricted (DPPA, § 2721(c)). Requests for uses not otherwise provided for may be permitted if a state motor vehicle department requests and receives an individual's privacy waiver DPPA, § 2721(d)). States are not permitted to condition issuance of an individual's record on receiving express consent DPPA, § 2721(d)).

c. Enforcement

DPAA makes it unlawful to obtain or disclose information for any use not permitted (§ 2722(a)) or by means of a false representation (§ 2722(b)). Knowing violations of DPAA are subject to a criminal fine (§ 2723(a)). In addition, the U.S. Attorney General is authorized to impose a civil penalty of up to $5,000 for "substantial noncompliance" with DPAA by a state department of motor vehicles (§ 2723(b)). DPAA also provides for a private right action to bring

a civil suit in a U.S. District Court and allows that court to award actual damages, punitive damages, attorney's fees and other litigation costs and preliminary and equitable relief (§ 2724(a) and (b)).

d. Constitutional Challenge

Not too long after its effective date, DPPA was the subject of several state challenges, one of which reached the U.S. Supreme Court. The state of South Carolina challenged DPAA as violative of the Tenth and Eleventh Amendments of the U.S. Constitution.[8] In Reno v. Condon, a unanimous U.S. Supreme Court reversed a decision of the Fourth Circuit of Appeals that had held that DPAA violated constitutional principles of federalism,[9] thereby upholding the validity of DPPA (528 U.S.141, 147-148 (2000)). South Carolina's law conflicted with DPPA's provisions in that the state law permitted dissemination of motor vehicle records upon written request and a confirmation that the requested records would not be used for telephone solicitation (528 U.S. at 147).

The court found that because drivers' personal information sufficiently impacts interstate commerce, a "constitutional base for federal legislation" was created (528 U.S. at 148-149), but that finding, in itself, did not resolve the issue of DPPA's constitutionality (528 U.S. at 149). The court recounted prior cases which invalidated federal statutes on the ground that, as related in one such case, "Congress commandeered the state legislative process by requiring a state legislature to enact a particular kind of law" (528 U.S. at 149).

Nonetheless, the court held that a decision in another case, South Carolina v. Baker (485 U.S. 505 (1988)), actually governed the case at hand (528

[8] The Tenth Amendment, also known as the "Reserved Powers Clause," reads, "The powers not delegated to the United States by the Constitution, not prohibited by it to the States, are reserved to the States respectively, or to the people." The Eleventh Amendment, pertaining to State sovereign immunity, states, "The Judicial Power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State." [Tenth Amendment to the U.S. Constitution].

[9] The U.S. system of government where power is divided between the federal government and the states.

U.S. at 150). In Baker, the court upheld a federal statute prohibiting states from issuing unregistered bonds "because the law 'regulated state activities,' rather than 'seeking to control or influence the manner in which States regulate private parties'" (528 U.S. at 150 [internal citation omitted]). In that case, the court stated, "[a]ny federal regulation demands compliance. That a State wishing to engage in certain activity must take administrative and sometimes legislative action to comply with federal standards regulating that activity is a commonplace that presents no constitutional defect" (528 U.S. at 150-151 [internal citation omitted]).

The court likened DPPA to the statute at issue in Baker, stating:

> DPPA does not require the States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as the owners of databases. It does not require the South Carolina Legislature to enact any laws or regulations, and it does not require state officials to assist in the enforcement of federal statutes regulating private individuals. (528 U.S. at 151)

Thus, the court also found that DPPA was not at odds with the line of cases that prohibit "commandeering" of the state legislative process (528 U.S. at 151). Finally, the court stated that it did not need to address the state's argument that "Congress may only regulate the States by means of 'generally applicable' laws" because the court found DPPA to be generally applicable in that it does not regulate states exclusively (528 U.S. at 151).

4. Analysis

a. Fostering Collaboration

If judged by the criteria adopted from those used by the GAO, this policy option has the potential to increase collaboration, though perhaps not voluntary collaboration *per se*. In imposing mandatory privacy protection standards, the federal government would have at least some latitude in deciding on the common outcome sought along with the strategies used to achieve that outcome. Roles and responsibilities—including, presumably, a federal agency or

executive in a leadership role—could be specified. Because there would be one set of procedures, they would, by definition, be compatible—at least internally. Reporting and evaluative mechanisms, as in the Justice Department regulations, could be used to ensure individual and agency accountability. By these measures, federally imposed mandatory standards would increase collaboration.

In a broader sense, though, collaboration relies to a significant degree on the voluntary cooperation of parties to work together. This relates to the GAO collaboration criterion concerning agreement on roles and responsibilities. Mandatorily imposed standards by their very nature do not rely on voluntary cooperation to either promulgate or implement. As unilateral standards, in effect, act to impose the will of the federal government rather than reflect the agreement of all ISE participants on their roles and responsibilities, such standards may actually work to decrease collaboration in the ISE.

b. Ensuring Information Sharing

On their face, federally imposed mandatory privacy protection standards would seem to have at worst a neutral effect on information sharing. As with the collaboration criterion, though, while mandatory standards might be fully capable of ensuring a coordinated multi-agency perspective and efficient and effective dissemination of information—at least on paper—in practice it might not be as effective. Would ISE participants be as motivated when working under a system of a federal unilateral mandate as they would in a system where they would set their own standards to actually, in the ISE-PM's words, "*achieve* a coordinated multi-agency perspective?" [emphasis added]. Again, the term "sharing" seems to imply a sense of inherent "voluntariness" that might not be realized if standards are imposed on a resistive ISE membership.

c. Protection of Privacy Rights

1). Constitutionality. It is likely that uniform, mandatory privacy protection standards, at least if they are based on commonly accepted protection principles, will be upheld by the courts as a necessary exercise of

government power. At the very least, the federal government's reasonable exercise of authority in issuing standards should be treated with considerable deference by the courts.

Just as likely, is that there will be challenges to the standards on federalism grounds. As previously discussed, the Supreme Court has treated federal efforts to impose requirements on states in one of two ways—either as an impermissible usurpation of state legislative authority or a permissible exercise of power to regulate state activities. Arguments similar to those in Reno v. Condon should be anticipated. Treatment of the mandatory standards by the courts will depend on many factors, not the least of which will be the operative effect of the standard itself.

2). Consistency of Application. This policy option, by its mandatory nature, would maximize the consistency of privacy protection standards used by ISE participants. As stated before, however, consistency in actual application may have practical limits, depending on, for example, whether exceptions to the standards are allowed and how those exceptions are interpreted. Also, if the HIPPA approach to preemption is followed, states would be permitted to retain their own privacy rules unless specifically contrary to the federal act.

3). Enforceability. Drawing on the three examples used to illustrate this policy option, the federal government has a range of enforcement options from which to choose. HIPPA uses civil and criminal penalties are provided for, although voluntary cooperation is encouraged. The Part 23 regulations rely on participating systems to adopt their own sanctions program, and the regulations also require adherence to all regulatory requirements in order to receive federal funding. There is also a monitoring and audit program for funded systems. Enforcement of DPPA is based on a system of criminal fines, civil penalties and a private right of action in federal court for aggrieved parties.

4). Political Acceptability. Strictly speaking, adoption of this policy option would require implementation by only one entity, either the U.S. Congress for a statute, or a federal agency in the case of a regulation. However, this policy option could, like DPPA, potentially be the subject of resistance by non-federal members of the ISE. This resistance could take the form of intense political pressure pre-passage (statute) or pre-adoption (regulation) or post-implementation court challenges, as discussed above.

Again, the question is whether this option is not "too unacceptable?" And, again, the answer to that question would depend on the totality of factors at work at the time the system is considered.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PROJECTED OUTCOMES

Given the widely recognized need to share information, it is reasonable to believe that a certain level of information sharing will occur regardless of the policy option chosen. Nonetheless, sharing might be maximized where participants will know that the information they share will be treated by the recipient in compliance with uniform standards, which could simultaneously increase the security of the information in addition to protecting privacy.

Because the intent of the ISE is to share information among all ISE participants, shared information should not be subject to varying levels of privacy protection dependent upon which ISE participant is in possession of that information at any given time. Thus, all ISE participants should be subject to the same privacy protection standards.

Specifically, instead of general guidelines for piecemeal implementation by the various members of the ISE, there should be uniform privacy protection standards that apply to all parties that make up the ISE. Second, in order to be effective, compliance with the privacy protection standards should be mandatory rather than optional, thus ensuring that the standards are not only uniform in and of themselves, but are consistently implemented.

The projected relative outcomes of the ability of the three policy alternatives analyzed to meet these criteria are summarized in the following table (Table 1).

Table 1. Projected Relative Outcomes for Three Alternative Privacy Protection Systems for the Information Sharing Environment

ALTERNATIVES / Evaluation Criteria	Voluntary Guidelines	Voluntarily Adopted Mandatory Standards	Federally Imposed Mandatory Standards
Net Effect on Fostering Collaboration	Negative	Positive	Neutral
Net Effect on Ensuring Information Sharing	Neutral	Positive	Neutral
Constitutionality*	High	High	Medium
Consistency of Application	Low	Medium	High
Enforceability	Low	Medium	High
Political Acceptability	High	Medium	Low

*Indicates the overall likelihood that the alternative would withstand constitutional challenge.

As can be readily seen from Table 1, no policy alternative has established dominance, defined as an alternative that is expected to achieve a better outcome for every criterion measured. However, the voluntarily adopted mandatory standards alternative shows a better outcome than the status quo voluntary guidelines alternative for every criterion except for that of political acceptability.

The criteria used present a classic multi-attribute problem in that they are not susceptible to commensurable weighting units across the criteria. Nonetheless, the political acceptability criterion, while important to the analysis, does not in itself go to the core of the desired outcome for the ISE. Instead, the political acceptability criterion goes to how difficult a particular alternative would be to bring into force. As such, the political acceptability criterion can be given less relative weight than the other criteria.

Given that the voluntary guidelines alternative rates lower than the voluntarily adopted mandatory standards alternative for all other criteria, the voluntary guidelines alternative is clearly dominated by at least the voluntarily adopted mandatory standards alternative and justifiably can be eliminated as a weaker alternative. Nonetheless, the projected outcomes of the voluntary guidelines alternative can serve as a benchmark, or "base case," for the remaining two alternatives.

Leaving aside political acceptability, a clear delineation between the alternatives of voluntarily adopted mandatory standards and federally imposed, mandatory standards emerges. In two of the primary criterion espoused as central to the ISE, fostering collaboration and ensuring information sharing, voluntarily adopted mandatory standards is projected to have a better outcome. Conversely, the federally imposed mandatory standard has an overall better outcome for the majority of the criteria that comprise the ISE goal of privacy protection: constitutionality, consistency of application, and enforceability.

It seems almost axiomatic that a single set of privacy protection standards, mandatory in effect and promulgated by a single entity—in this case the federal government—would provide greater consistency in the application of those standards. Similarly, given the range of enforcement mechanisms available to the federal government, a single-source enforcer of privacy standards would also seem to maximize the outcome of the enforceability criterion.

Of the three criteria that make up overall privacy protection goal of the ISE, only in susceptibility to constitutional challenge would the federally imposed mandatory standards alternative cede any ground to voluntarily adopted mandatory standards. And even in that regard, a carefully crafted regulation or statute should be able to obviate many if not all federalism concerns. This could be accomplished through careful characterization of the standards scheme so that it would fall within the line of Supreme Court cases upholding federal regulation.

As previously mentioned, the main superiority of the voluntarily adopted mandatory standards lies, in essence, in maximizing the inherent *raison d'etre* of the ISE—fostering collaboration and ensuring information. These are the very elements found to be deficient by the 9/11 Commission and other commentators and widely acknowledged to be critical to responding to future terrorist threats.

The areas of relative weakness of the federally imposed mandatory standards—in the final assessment—all revolve around the potential impact of the alternative on the relationship between the federal government and the state, local and tribal governments that constitute a large portion of the ISE as a whole. It seems incongruous to impose unilateral requirements on a community, for that is what it is, that is intended to be operated on the basis of cooperation and, at least impliedly, also on the basis of the comity that is intended to be the essence of the federalist system of government.

Admittedly, the voluntarily adopted mandatory standards alternative would not promise the same level of consistency and enforceability that the federally

imposed mandatory alternative offers. However, even without resorting to its relative superior political acceptability, *in toto* the balance of all the other criteria weighs in favor of the voluntarily adopted mandatory standards alternative.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. RECOMMENDATION

This thesis recommends that the ISE implement uniform national privacy standards that once voluntarily adopted by ISE participants would become mandatory in application. In particular, ISE privacy standards should include:

1. Uniform standards that apply to all ISE participants;
2. Restrictions on data transfer by ISE participants to other parties that do not have adequate privacy protections in place and
3. Provisions that are legally enforceable in the courts.

As stated by Bignami (2008), "[b]ecause human rights inhere in individuals as human beings, not as citizens of one nation or another, they should not vary depending on geography. They should give rise to the same treatment everywhere" (p. 247). The principles of human rights—including privacy rights—that apply to citizens of the various nations should likewise apply to the citizens of the various states within the United States. One's privacy rights as an American citizen should not depend on whether one is a resident of California, or New York or Texas.

Instead of general guidelines for piecemeal implementation by the various members of the ISE, there should be uniform privacy protection standards that apply to all parties that make up the ISE. These standards, preferably developed by the ISE members themselves, would, as previously discussed, be voluntarily adopted.

However, to ensure that the voluntary uniform standards are consistently applied, compliance with the privacy protection standards should be made a condition of participation in the ISE. Information sharing with non-participating entities would be restricted.[10] In addition, as part of the implementation process,

[10] Restrictions could include, for example, redacted or scrubbed information, use restrictions, or technical controls.

consideration should be given to setting up an independent, joint (i.e., multistate) supervisory body to oversee compliance with the standards and to address disputes between ISE participants.

It is possible, that despite being voluntarily adopted, that some members of the ISE will object to having mandated privacy standards on the grounds that the standards would impose an unreasonable burden on their sharing of information and, possibly, as a violation of the Tenth Amendment to the U.S. Constitution, which concerns powers reserved to the states.

The response to these potential challenges would be multi-fold in nature. First, ISE members' support of the ISE privacy standards would be enhanced, if those members have a say in the formulation of the standards. A possible model for a collaborative and inclusive approach to setting standards, discussed further *infra*, is the Capabilities-Based Preparedness Process, a part of the National Preparedness Guidelines (2007).

Another response to challenges to the proposed privacy standards would include an appeal to interests of the ISE members—namely, by ensuring that the members have a clear understanding of the benefits that uniform privacy protection standards would provide to the ISE. First, one could argue that by increasing the protection of information for one purpose, privacy in this case, that protection of that information for another purpose—operational or tactical security—is simultaneously advanced, at least to the extent that disclosure for any reason is better controlled. Second, a robust, effective and mandatory system for ISE privacy protection would likely mitigate potential resistance from privacy advocates regarding how information is being obtained, used and shared by ISE members. Third, uniform privacy protection standards would thus simultaneously increase public trust in the purpose and actions of the ISE as a whole.

Similarly, privacy standards would also assuage any related concerns by the various legislative bodies controlling ISE members, possibly paving the way

for even better support of ISE by that branch of government. In addition, an effective system of privacy protection would assist ISE members in defending their actions impacting privacy in a court of law, thereby reducing legal challenges that could sap their agency's resources in defending, and that could also result in potential adverse rulings. In addition, some members of the ISE might be more likely to share information with other members of the ISE if privacy protection of that information is assured by uniform and enforceable standards. Most importantly, standardized privacy protections would help ensure that constitutional values are not sacrificed or compromised. A concomitant benefit of privacy standards would be to help define the still unsettled jurisprudential concept of informational privacy—with potential benefits far beyond the confines of the ISE.

Benefits of a uniform system of privacy protection could also be seen in the sharing of information with the nation's international counterterrorism partners. As a general matter, European nations do not believe that the U.S. currently meets European personal data-privacy protection requirements (Kochem, 2006). This has led to "strained relations between Europe and the United States and ha[s] frustrated transatlantic cooperation in the fight against terrorism" (Bignami, 2007, p. 662). Indeed, even the U.S. Department of Homeland Security has noted increased pressure to cooperate with international anti-terrorism partners and has recognized the need to build trust between nations with different privacy regimes (DHS Privacy Office, 2007).

Finally, the privacy protection standards should be legally enforceable. Judicial redress for violations of the standards should be available to both aggrieved members of the ISE as well as individuals, the latter known as a private right of action. Federal courts should have exclusive jurisdiction over actions brought to enforce the privacy standards, as those standards will apply nationally; and this would avoid possibly conflicting rulings if the actions were allowed to be brought in the various state courts.

Courts should be able to choose from an array of possible sanctions, as appropriate to the case at hand. The available remedies should include monetary sanctions, declaratory relief (a determination of rights under the standards), damages to the aggrieved party, injunctions to halt violative behavior and orders of specific performance (orders to a party to perform a specific act, such as comply with a statute). In addition, in the case of private litigants, the courts should have the authority to award attorneys' fees where an ISE member is found to have violated the standards.

These procedures could possibly be combined with a process to quickly resolve cases where an ISE member is found by the court to have fully complied with the privacy standards, perhaps through an expedited summary judgment process. Perhaps this proposal could be implemented by an external commission—composed of representative ISE members and other stakeholders, such as privacy watchdog groups—that would both guide ISE members' implementation of the standards and resolve conflicts in implementation of those standards by ISE members.

In summary, by successfully identifying appropriate privacy protections and ensuring the uniform and mandatory application of those protections to all members of the ISE, homeland security and the protection of individual rights and liberties can both be advanced.

B. FUTURE RESEARCH

This thesis recommends use of voluntarily adopted mandatory privacy standards, based on privacy protection systems used by several European conventions and agreements. As discussed *supra*, the United States and Europe share a common legal heritage, which includes recognition of the need to protect privacy rights. However, protection standards have diverged in the U.S. and Europe since the 1970s, with European law generally providing broader privacy protection.

Underlying the European system is the general right for individuals to seek damages granted by the various conventions, whereas in the United States privacy-based actions are more often grounded in general tort (i.e., non-contractual wrongs) law (Solove, Rotenberg, 2003). The issue with pursuing privacy actions under a tort theory is that damages commonly suffered in such cases are not of a type normally recognized in tort jurisprudence (Solove, Rotenberg, 2003).

Thus, research is needed to determine whether a U.S. system of privacy protection for the ISE could, or should, account for differences in the underlying treatment of privacy rights in the two systems.

Next, as discussed in the "Scope" section, this thesis does not prescribe what the privacy standards themselves should look like. Nonetheless, future research should consider, as part of the privacy standards-setting process, whether information privacy as it is used in the ISE should be specifically delineated. Appendix A contains a short discussion of a proposed new classification of information privacy for the ISE.

Finally, research is needed on the means by which a collaborative process could be most effectively used to enable ISE participants to create a set of privacy standards. A discussion of the complexities of privacy protection standards and the ISE and the use of a multi-lateral approach to address those complexities is proposed in Appendix B.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. CLASSIFYING INFORMATION SHARING ENVIRONMENT PRIVACY

As uniform privacy protection standards are developed, the ISE should consider including in those standards a new classification of information privacy. Similar to HIPAA's use of the term Personal Health Information (PHI) to delineate a specific set of personal information that is subject to the privacy protection provisions of the statute, specifying and classifying the information to be protected in the ISE would help advance privacy protection efforts.

First, as there is no commonly accepted definition of privacy, by concentrating on the types of information that need protection, the often unavailing debate of what privacy as a general concept means can be avoided and on the focus can turn to the specific privacy problems to either avoid or address. Such a classification is beneficial both in the creation of ISE privacy standards and in their eventual implementation and enforcement by providing a concrete and common base for interpretation of the standards.

Once the type of information sought to be protected in the ISE is classified, consideration should be given to the type of protection this classification of information warrants. In this regard, the thesis proposes a new concept of information privacy tailored to the ISE. This classification, in effect, would be a hybrid, containing legal characteristics of both public information and private information.

This concept, which this author terms "Information Sharing Privacy" or "ISP," will provide more privacy protection than is currently accorded to information considered "public," but at the same time it would permit limited sharing of information necessary for law enforcement or homeland security purposes. In essence, ISP will respect the concept of a reasonable expectation of privacy—and, in fact, somewhat expand its coverage—while recognizing a countervailing and compelling governmental interest in sharing homeland

security information. This concept, along with the proposal for classification of information to be protected in the ISE, would be fruitful topics for further development and study.

APPENDIX B. ADDRESSING ISE COMPLEXITIES THROUGH A MULTI-SECTOR COLLABORATIVE EFFORT

The lack of consensus about the definition of privacy and the operational parameters of the right of information privacy together comprise an issue where "multiple perspectives jostle for prominence" (Snowden, Boone, n.d.). Thus, in applying the Cynefin framework, as discussed in Bellavita (2006) and Snowden, Boone (n.d.), this issue falls squarely within the "disordered" domain of that framework. Similarly, this is a place where there is "insufficient stakeholder agreement about how to make sense of a particular homeland security issue" (Bellavita, 2006, p. 6).

Must this issue be addressable only in the relatively intractable realm of disorder? Not necessarily. As Solove (2008), posits, the elusiveness of a single, widely accepted definition of privacy can be sidestepped by recognizing that there can be different forms of privacy, related within each form in a familial sense, rather than by continuing the usual, but unavailing approach that seeks to isolate a characteristic of privacy that is common to all usages. The key to this taxonomic framework is that privacy is considered in a contextual manner—by conceptualizing privacy by means of "focusing on the specific types of disruption" that a particular invasion of privacy engenders (Solove, 2008, p. 9).

If, as Solove argues, one can conceptualize privacy from the bottom up by focusing on privacy *problems* (2008, pp. 8–9), can the reader then feel free to "agree to disagree" on the exact definition of privacy, and just concentrate on addressing its attendant problems, thereby avoiding the disordered realm altogether? Not only is this approach possible, at least in the present context, but perhaps this approach would avoid inefficient and unnecessary conflict in the ISE. As Bellavita recognizes, the first leadership task is to determine "whether an issue can be ordered … or whether the issue's organic state is unorder, and we are wasting our time and resources trying" to do so (2006, p. 15). Snowden and Boone (n.d.) implicitly recognize this approach in suggesting that disordered

problems might be avoided by “break[ing] down the [disordered] situation into constituent parts and assign[ing] each to one of the other four realms” (p. 6 of printout).

Applying that suggestion to the issue of the lack of mandatory privacy standards in the ISE, several domains are at play. Applying the Solove model of a contextual, problem-based privacy conceptualization, perhaps then privacy problems and concomitant effects could be reduced to the “simple” realm where cause and effect is known. For example, if the privacy of one’s social security number is not adequately protected, one stands to be the victim of identity theft.

The remaining constituent parts are considered next. According to Bellavita, some “knowable,” also known as “complicated,” issues would also be implicated by this issue, namely “fusing intelligence information” and “creating collaborative networks” (2006, p. 8). In addition, the various issues attendant to standards—such as those concerning their development, adoption and enforcement—fall within the “complex” realm: the domain of emergent problems.

Homeland security is commonly recognized as a complex adaptive system. In the author’s view, homeland security is actually a system of complex adaptive systems or subsystems. As demonstrated, the arena of privacy and the ISE could fairly be considered to be one of those complex subsystems.

Thus, although the topic of privacy and the ISE falls within the “disordered” realm, the topic can be broken down into “simple,” “complicated” and “complex” parts. Nonetheless, the complex realm is the dominant feature of the components because the ultimate issue within this topic is that of standards. The other realms involved, “simple” and “complicated,” represent the bases for the desired end product—privacy standards.

A. MULTI-SECTOR IMPERATIVE

How, then, should privacy standards in the ISE be approached? In the complex realm “best practice is replaced by smart practice, emergent practice, or

novel practice" (Bellavita, 2006, p. 15). Also drawing on the concept of emergence, Snowden, Boone (n.d.) believe that the "right approach for a complex context" is to allow "solutions to emerge from the community itself rather than try to impose them" (p. 5 of printout). In addition, they believe that there are instances in which a leader must share power and rely on group wisdom, patiently allowing the solution to emerge (Snowden, Boone, n.d.).

According to the authors of *Megacommunities*, relying on group wisdom, known as the *megacommunity approach*, is particularly appropriate for dynamic issues that do not have a clear solution (Gerencser, Van Lee, Napolitano, and Kelly, 2008). The megacommunity approach, as its name implies, takes an expansive view of group involvement by bringing together government, business and non-governmental organization (referred to as "civil society" in the book) sectors.

Each sector brings its own strengths and weaknesses to the community and the resultant grouping gets its energy from the inherent tension between the groups—so-called "swarm intelligence"—that allows the creation of novel or emergent practice (Gerencser et al., 2008, pp. 66-67). A megacommunity in action thus provides an illustration of the benefits of Bellavita's (2006) admonition to use the properties of complexity to advantage in addressing HLS process and strategy.

The goal of the megacommunity approach is provide a model of collective leadership that fully involves the three sectors, where no single person or group is in charge, but all benefit from addressing issues and the concomitant reduction in complexity that none can accomplish alone (Gerencser et al., 2008). As defined by the authors:

> A megacommunity is a public sphere in which organizations from three sectors—business, government, and civil society—deliberately join together around compelling issues of mutual importance, following a set of practices and principles that make it easier for them to achieve results without sacrificing their individual

> goals. We chose the term megacommunity to reflect such a sphere's character as a gathering place, not of individuals, but of organizations. (Gerencser et al., 2008, p. 53)

Although Gerencser et al., (2008), emphasize the role of organizations rather than individuals in their megacommunity approach, the involvement of individual leaders in guiding change for their own organizations, as well as the megacommunity as a whole, is critical. Marcus, Dorn and Henderson (n.d.) see the key role of leaders as prompting organizational change that is more responsive—both in content and in timeliness—to critical issues than is often the case with organizational change. Translated to cross-agency endeavors, a distinct subset of leaders are "metaleaders" that connect "the purposes and the work of different organizations or organizational units" to engender a "shared course of action and a commonality of purpose" (Marcus et al., n.d., p. 44).

For multiagency efforts, metaleaders cannot rely on the authority inherent in the position they hold in their own agencies but instead must use their skill to "envision a sum that is larger than its parts and then find a way to communicate, inspire, and persuade broader participation" (Marcus et al., n.d., p. 44 [internal cite omitted]). Marcus et al., (n.d.), however, recognize the personal sacrifices metaleaders must often make, as well as the difficulty that often attends joint efforts, particularly where, as is potentially the case for privacy standards, "shared purposes require sacrifice, the reduction of autonomy and independence, or a change in culture or operating procedures" or when "creating new relationships among traditionally competitive agencies" (Marcus et al., n.d., p. 45). Clearly, metaleaders, a special breed of leader, are critical to the multi-sector approach to developing uniform privacy protection standards.

B. ADAPTATION OF THE CAPABILITIES-BASED PREPAREDNESS PROCESS

In the process of setting privacy standards, the megacommunity to be involved should include every sector that is a part of the Information Sharing

Environment—federal, state, local and tribal governments, the private sector, and foreign partners—as well as stakeholders, or representatives of stakeholders, such as privacy advocacy groups.

Known as the Capabilities-Based Preparedness Process, this approach—discussed in more detail *infra*—"emphasizes collaboration to identify, achieve, and sustain target levels of capability that will contribute to enhancing overall national levels of preparedness" (National Preparedness Guidelines, 2007, p. 33; Guidelines). The process emphasizes the early formation of an inclusive working group to "identify, analyze, and choose options" for filling an identified capability gap (Guidelines, 2007, p. 34).

As suggested in the Guidelines (2007), membership in the working group should draw from a wide variety of organizations, including private sector and non-governmental organizations. Although the Capabilities-Based Preparedness Process, as written, focuses on physical emergency response capabilities, this author believes that the robust collaborative aspects of the process would be useful as part of any strategic planning process where the voluntary collaboration of various stakeholder groups is required.

There is no reason the process could not be applied to determine appropriate responses to gaps of a legal nature—such as determining the proposed ISE privacy standards to be adopted. The benefit of applying the Process will have lasting impact—the collaborative effort needed to develop privacy protection standards will set the stage for future collaborative efforts as those standards are implemented on a day-to-day basis in the ISE.

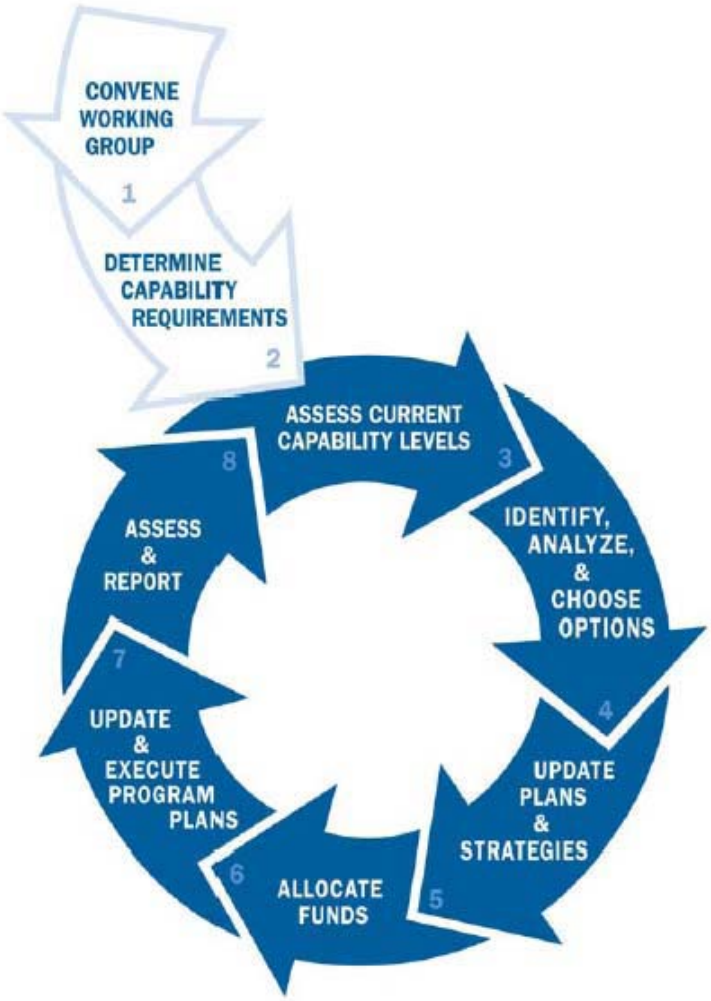

Figure 2. Capabilities-based Preparedness Process (From National Preparedness Guidelines, 2007, Figure B-2).

This capabilities-based process "emphasizes collaboration to identify, achieve, and sustain target levels of capability that will contribute to enhancing overall national levels of preparedness" (National Preparedness Guidelines, 2007, p. 33; Guidelines).

Broken into simple, discrete steps, the process could also be used to regularize and optimize development and implementation of a selected strategic policy.

In application, the first step would be to convene a working group. As suggested in the Guidelines, membership in the working group should draw from a wide variety of organizations, including private sector and non-governmental organizations. Having a wide range of membership will assist in the technology adoption process by helping ensure that future users of the system are fully informed of the program, thereby concomitantly decreasing resistance to the chosen strategy.

One of the most critical steps would be next. The working group would "identify, analyze, and choose options" for filling the identified capability gap—or in this case, privacy protection gap (Guidelines, 2007, p. 34). Updating plans and strategies is the next step in the process and includes amending agency and joint work plans, along with budgeting considerations. Allocating resources through reviews of funding sources and return maximization is followed by updating and executing program plans. Another critical step, assessing and reporting, is the last step in the circular process, and is intended to provide a "continuously validated baseline for preparedness [or privacy protection]" to ensure that resources and capabilities remain in proper balance (Guidelines, 2007, pp. 38).

The capabilities-based process would thus lend itself to Bellavita's counsel that strategic change in the complex homeland security environment requires working at the level of patterns that may require the benefit of a retrospective viewpoint for their innate coherence to become evident (2006). In turn, working at the level of patterns requires establishing boundaries, promoting beneficial patterns, supporting desired patterns and intercepting incipient undesirable patterns (Bellavita, 2006).

In summary, by successfully harnessing the value of megacommunities and metaleaders to address the complex issue of identifying appropriate privacy protections and ensuring the uniform and mandatory application of those protections to all members of the ISE, homeland security and the protection of individual rights and liberties can both be improved.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data on Supervisory Authorities and Transborder Data Flows (opened for signature on 8 November 2001). Retrieved February 4, 2009, from http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm

Agreement between the United States of America and the European Police Office. (2001). Retrieved April 7, 2009, from http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf

Agreement between the United States of America and the European Union on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), (2007). Retrieved April 3, 2009, from http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf.

Bamberger, K., Mulligan, D. (2008). *Privacy decisionmaking in administrative agencies.* University of Chicago Law Review. Retrieved September 3, 2008, from Lexis-Nexis database.

Bardach, E. (2005). *A practical guide for policy analysis* (2nd ed.). Washington, D.C.: CQ Press.

Bellavita, C. (2006). *Changing homeland security: Shape patterns, not programs*. Retrieved June 9, 2009, from www.chds.us [course materials for NS4755 Strategic Planning and Budgeting for Homeland Security, Naval Postgraduate School. Originally published in *Homeland Security Affairs, II*(3) (2006)].

Bignami, F. (2008). The case for tolerant constitutional patriotism: The right to privacy before the European courts. *Cornell [University] International Law Journal* [41 Cornell Int'l L.J. 211]. Retrieved February 25, 2009, from LexisNexis database.

Bignami, F. (2007). European versus American liberty: A comparative privacy analysis of anti-terrorism data mining. Boston College Law Review [48 B.C. L. Rev 609]. Retrieved February 25, 2009, from LexisNexis database.

Bignami, F. (2007). Towards a Right of Privacy in Transnational Intelligence Networks. *University of Michigan Journal of International Law*. [28 Mich. J. Int'l L. 663] Retrieved December 19, 2008, from Lexis-Nexis database.

Bush, G. (2005). *Memorandum for the heads of executive departments and agencies; Subject: Guidelines and requirements in support of the Information Sharing Environment.* Retrieved June 20, 2009, from http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

Commissioner for Human Rights, Council of Europe. (2008). *Protecting the right to privacy in the fight against terrorism.* Retrieved February 25, 2009, from www.crowell.com/pdf/FederalContracts_Privacy.pdf

Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Europol Convention). Retrieved February 4, 2009, from http://www.europol.europa.eu/index.asp?page=legalconv

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28.i.1981). Retrieved February 4, 2009, from http://conventions.coe.int/treaty/en/treaties/html/108.htm

Council of Europe website (n.d.), *Key dates*. Retrieved March 14, 2009, from http://www.coe.int/T/E/Com/About_Coe/dates.asp.

Department of Homeland Security Privacy Office. (2007, April). *Cross border sharing and privacy*, PowerPoint presentation for the International Public Safety/Counterterrorism Conference, Quebec City, Canada. Retrieved February 25, 2009, from www.rebootconference.com/publicsafety2007/ppt/Kropf_John-Public Safety2007.ppt

DiPaolo, A. & Stanislawski, B.(n.d.). *Information sharing: The European experience*. Retrieved March 14, 2009, from www.insct.syr.edu/events&lectures/Information%20Sharing%20Conf/DiPaoloStanislawski.pdf.

Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725.

E-Government Act of 2002, 44 U.S.C. § 101.

Electronic Privacy Information Center. (n.d.). The Drivers Privacy Protection Act (DPPA) and the privacy of your state motor vehicle record. Retrieved June 16, 2009, from http://epic.org/privacy/drivers

European Convention on Human Rights and Fundamental Freedoms. (1950). Retrieved March 12, 2009, from http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf

European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America [P6-TA-2007-0347]. Retrieved April 7, 2009, from http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0347&language=EN&ring=P6-RC-2007-0278

European Security: High Level Study on Threats, Response and Relevant Technologies Consortium (ESSTRT). (2006). *New European approaches to counter terrorism*. Retrieved February 25, 2009, from www.cmi.fi/files/ESSTRT_final_report.pdf

Europol website. (2008). *Fact sheet on Europol*. Retrieved March 14, 2009, from http://www.europol.europa.eu/index.asp?page=facts

Executive Order 13388. (2005). Further Strengthening the Sharing of Terrorism Information to Protect Americans.

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541.

Gerencser, M., Van Lee, R., Napolitano, F., & Kelly, C. (2008). *Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together*. New York: Palgrave McMillan.

Glover, B, Bhatt, H. (2006). *RFID essentials*. Sebastopol, CA: O'Reilly Media.

Gosfield, A. (2002, November/December). The HIPAA Privacy Rule: Answers to frequently asked questions. *American Academy of Family Physicians, Family Practice Management* [newsletter]. Retrieved June 16, 2009, from http://www.aafp.org/fpm/20021100/35theh.html.

Government Accountability Office. (2008). *Information Sharing Environment: Definition of the results to be achieved in improving terrorism-related information sharing is needed to guide implementation and assess progress* (GAO-08-492). Retrieved June 26, 2009, from http://www.gao.gov/new.items/d08492.pdf

Government Accountability Office. (2007). *Progress made but challenges remain in notifying and reporting to the public* (GAO-07-0522). Retrieved September 3, 2008, from Lexis-Nexis database.

Government Accountability Office. (2005). *Results-oriented government: Practices that can help enhance and sustain collaboration among federal agencies* (GAO-06-15). Retrieved June 26, 2009, from http://www.gao.gov/new.items/d0615.pdf

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment. Program Manager-Information Sharing Environment. Retrieved June 2, 2009, from http://www.ise.gov/pages/privacy-implementing.html

Guymon, C., 2000, *International legal mechanisms for combating transnational organized crime: The need for a multilateral convention.* Berkeley Journal of International Law [18 Berkeley J. Int'l L. 53]. Retrieved April 3, 2009, from LexisNexis database.

Harris, E., 2007, *Personal data privacy tradeoffs and how does a Swedish lady, Austrian public radio employees, and transatlantic air carriers show that Europe does not have the answers.* American University International Law Review [22 Am. U. Int'l L. Rev. 745]. Retrieved April 7, 2009, from LexisNexis database

Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1301, *et seq*.).

*Implementing Recommendations of the 9/11 Commission Act of 2007 (*6 U.S.C. § 101 note, 110 Pub. L. 53).

Intelligence Reform and Terrorist Prevention Act of 2004, Pub.L.No. 108-458, 118 Stat.3638.

Interagency Threat Assessment and Coordination Group.(n.d.). [informational brochure]. Retrieved April 3, 2009, from http://www.ise.gov/docs/misc/ITACG-brochure.pdf.

Jansson, B. (2000). Policy Analysis. In J. Midgley, M. Tracey, & M. Livermore (Eds.), *The handbook of social policy* (chap. 4; J. Midgley, M. Tracy, M. Livermore (Eds.), Thousand Oaks, CA: Sage Publications. Retrieved June 26, 2009, from http://books.google.com

Kochem, A. (2006). *EU privacy directive could prohibit information sharing with U.S. law enforcement*. Retrieved February 25, 2009, from www.heritage.org/research/europe/em992.cfm.

Koontz, L. [Director, Government Accountability Office] (2007). *Testimony before the House Appropriations Committee, Homeland Security Subcommittee, on privacy and civil rights in homeland security*. Retrieved September 3, 2008, from Lexis-Nexis database.

Kramer, D.T. (2007). Constitutional law: Fundamental Rights and Privileges. *American Jurisprudence, Second Edition.* Retrieved May 27, 2008, from Lexis-Nexis database. [16B Am Jur 2d Constitutional Law §§ 603, 604].

Marcus, L., Dorn, B., & Henderson, J. (n.d.). *Meta-leadership and national emergency preparedness*. Retrieved June 9, 2009, from www.chds.us [course materials for NS4755 Strategic Planning and Budgeting for Homeland Security, Naval Postgraduate School, Monterey, CA].

Markle Foundation Task Force on National Security in the Information Age. (2009). *Nation at risk: Policy makers need better information to protect the country*. Retrieved April 3, 2009, from http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf

Markle Foundation Task Force on National Security in the Information Age. (2002). *Protecting America's freedom in the information age*. Retrieved April 3, 2009, from http://www.markle.org/downloadable_assets/ntsf_full.pdf

McNamara, T. (2006). *Memorandum: Privacy guidelines for the Information Sharing Environment.* Retrieved June 2, 2009, from http://www.ise.gov/pages/privacy-implementing.html

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks Upon the United States* [Official Government Edition]. (2004). Retrieved June 15, 2009, from http://www.gpoaccess.gov/911/Index.html

National Research Council, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. (2008). *Protecting individual privacy in the struggle against terrorists: A framework for program assessment.* Retrieved February 25, 2009, from The National Academies Press Website: http://www.nap.edu/catalog/12452.html

National Strategy for Information Sharing. (2007). Retrieved June 2, 2009, from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf

Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

Program Manager-Information Sharing Environment. (2008). *Information Sharing Enterprise Architecture Framework*. Retrieved June 26, 2009, from http://www.ise.gov/docs/eaf/ISE-EAF_v2.0_20081021.pdf

Program Manager-Information Sharing Environment. (2008). *Privacy and Civil Liberties Implementation Manual*. Retrieved June 2, 2009, from http://www.ise.gov/pages/privacy-fed.html

Program Manager-Information Sharing Environment. (2007). *Common Terrorism Information Sharing Standards (CTISS) Program Manual* (Version 1.0). Retrieved June 26, 2009, from http://www.ise.gov/docs/ctiss/CTISSprogramManual20071031.pdf

Program Manager-Information Sharing Environment. (2007). *Privacy and Civil Liberties Implementation Guide*. Retrieved June 2, 2009, from http://www.ise.gov/pages/privacy-implementing.html

Program Manager-Information Sharing Environment. (2006). *Information Sharing Environment Implementation Plan*. Retrieved June 26, 2009, from http://www.ise.gov/docs/reports/ise-impplan-200611.pdf

Program Manager-Information Sharing Environment (n.d.). Information Sharing Environment website [*passim*]. Retrieved October 16, 2008, from http://www.ise.gov/

Public Law 107-236 (November 27, 2002), creating the National Commission on Terrorist Attacks Upon the United States

Reidenberg, J. (1992). *Privacy in the information economy: A fortress or frontier for individual rights?* Federal Communications Law Journal [44 Fed. Comm. L.J. 195]. Retrieved June 15, 2009, from Lexis-Nexis database.

Richards, N.M. (2006). The Information Privacy Law Project: Reviewing *The Digital Person: Privacy and Technology in the Information Age, by Daniel J. Solove*. *Georgetown Law Review* [94 Geo. L.J. 1087] Retrieved May 27, 2008, from Lexis-Nexis database.

Rotaru v. Romania, European Court for Human Rights. (2000). retrieved March 12, 2009, from http://www.echr.coe.int/eng/Press/2000/May/Rotaru.eng.htm.

Rotenberg, M. (2007). *Recent privacy developments in the United States, particularly with respect to travelers using air transport*. European Parliament (statement from a hearing on March 26, 2007). Retrieved March 17, 2009, from http://www.europarl.europa.eu/hearings/20070326/libe/rotenberg_en.pdf

Schwartz, P. (2008). *Reviving telecommunications surveillance law*. University of Chicago Law Review [75 U. Chi. L. Rev. 287]. Retrieved December 19, 2008, from Lexis-Nexis database.

Schwartz, P. (1995). *Privacy and participation: Personal information and public sector regulation in the United States*. Iowa Law Review [80 Iowa L. Rev. 553]. Retrieved June 15, 2009, from Lexis-Nexis database.

Securities and Exchange Commission v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).

Shaffer, G. (2000) *Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards,* Yale Journal of International Law [25 Yale J. Intl. L. 1]. Retrieved March 12, 2009, from LexisNexis database.

Simitis, S. (1987). *Reviewing privacy in an information society*. University of Pennsylvania Law Review [135 U. Pa. L. Rev. 707]. Retrieved June 15, 2009, from Lexis-Nexis database.

Skinner, S. (2002). *The Third Pillar treaty provisions on police cooperation: Has the EU bitten off more than it can chew?,* Columbia Journal of European Law [8 Colum. J. Eur. L. 203]. Retrieved April 3, 2009, from LexisNexis database.

Smith v. Maryland, 442 U.S. 779 (1979).

Snowden, D. & Boone, M. (n.d.). *A leader's framework for decision making.* Retrieved June 9, 2009, from www.chds.us [course materials for NS4755-Strategic Planning and Budgeting for Homeland Security, Naval Postgraduate School, Monterey, CA].

Solove, D. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Solove, D. (2002). *Modern studies in privacy law: Notice, autonomy and enforcement of data privacy legislation.* Minnesota Law Review [86 Minn. L. Rev. 1137]. Retrieved June 15, 2009, from Lexis-Nexis database.

Solove, D., Rotenberg, M. (2003). *Information Privacy Law.* New York: Aspen Publishers.

Solove, D., Rotenberg, M., Schwartz, P. (2006). *Privacy, Information, and Technology.* New York: Aspen Publishers.

Statewatch. (n.d.). *Statewatch analysis: The dream of total data collection—status quo and future plans for EU information systems*. Retrieved February 25, 2009, from www.statewatch.org

Stimson. (2008). *New information and intelligence needs in the 21st century threat environment*. Retrieved February 25, 2009, from the Henry L. Stimson Center Web site: http://www.stimson.org/domprep/pdf/SEMA-DHS_FINAL.pdf

Storbeck, J. (1999). *Organized crime in the European Union—The role of Europol in international law enforcement co-operation.* Retrieved April 3, 2009, from http://www.police-foundation.org.uk/files/POLICE0001/speeches

Supplemental agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information. (2002). Retrieved April 7, 2009, from http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf

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

U.S. Constitition Amend I, III, IV, V, IX, XIV, *passim*.

U.S. Department of Health and Human Services. (2003). *Health information privacy: Summary of the HIPAA Privacy Rule*. Retrieved June 16, 2009, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

U.S. Department of Homeland Security. (2007). *National Preparedness Guidelines*. Retrieved October 3, 2008, from http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf

U.S. Department of Justice, Global Justice Information Sharing Initiative. (n.d.). *Fusion Center Guidelines: Developing and sharing information and intelligence in a new era.* Retrieved June 2, 2009, from http://www.ise.gov/pages/privacy-slt.html

Whalen v. Roe, 429 U.S. 589 (1977)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Richard Bergin
   Naval Postgraduate School
   Monterey, California

4. Robert Josefek
   Naval Postgraduate School
   Monterey, California

5. Francine Kerner, Chief Counsel
   Transportation Security Administration
   Arlington, Virginia

6. Margot Bester, Principal Deputy Chief Counsel
   Transportation Security Administration
   Arlington, Virginia

7. Robert Vente, Assistant Chief Counsel
   Transportation Security Administration
   Arlington, Virginia