CANTIGNY CONFERENCE SERIES

Conference Report

Counterterrorism Technology and Privacy

Following the attacks of Sept. 11, 2001, the U.S. government faced an important dilemma in addressing the issue of national security: to what extent should the government employ the use of counterterrorism technology, and might the use of this technology violate the privacy of U.S. citizens?

A elite group of experts met at a McCormick Tribune Foundation Cantigny Conference to address important issues regarding the responsible implementation of counterterrorism technology such as:

- Americans' expectation of privacy and how it creates challenges in achieving popular acceptance of the government's use of counterterrorism technology.

- Why Americans are more comfortable with the reality of corporate data mining than they are with the idea of government data mining.

- The extent to which the analysis of personal information does or does not violate a citizen's right to privacy, and under what conditions with regard to the Fourth Amendment.

- What steps could be taken at the legislative level to ensure the successful implementation of technology so that both protection of privacy and counterterrorism efforts are maximized.

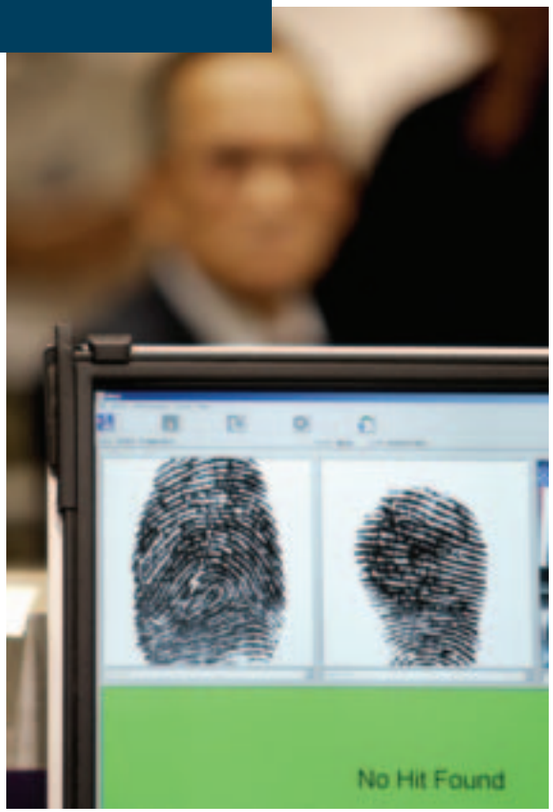
McCormick Tribune Foundation

CANTIGNY CONFERENCE SERIES

Counterterrorism Technology and Privacy

CANTIGNY CONFERENCE SERIES

Conference Report



Counterterrorism Technology and Privacy

McCormick Tribune Foundation

The Cantigny Conference Series is sponsored by the Robert R. McCormick Tribune Foundation.

The conference series offers the opportunity for collaboration between the foundation and other institutions or associations that are addressing issues consonant with the foundation's mission. Conferences are conducted on the grounds of Cantigny, the former estate of Col. Robert R. McCormick, located in Wheaton, Ill., approximately 35 miles from Chicago.

The McCormick Tribune Foundation is dedicated to a democratic society and its quality of life.

The mission of the McCormick Tribune Foundation:

- **To improve the social and economic environment.**
- **To encourage a free and responsible discussion of issues affecting the nation.**
- **To enhance the effectiveness of American education.**
- **To stimulate responsible citizenship.**

Cantigny Conference Series
Conference Report

Counterterrorism Technology and Privacy

Conference Rapporteur
Patrick J. McMahon

Sponsored by the McCormick Tribune Foundation

Counterterrorism Technology and Privacy

Published by the
McCormick Tribune Foundation
435 North Michigan Avenue
Suite 770
Chicago, Illinois 60611
312/222-3512
E-mail: rrmtf@tribune.com
Web site: http://www.mccormicktribune.org

All rights reserved

Copyright © 2005
McCormick Tribune Foundation

Table of Contents

Foreword

A national debate has flared over the last few years in the effort to reconcile two equally important—and sometimes conflicting—goals: keep the country safe from terrorism and protect citizens' expectation of privacy.

But does having more safety necessarily mean having less privacy? And in what ways has the emergence of high-tech tools in all facets of our society changed the very notion of anonymity?

To help clarify the issues at stake, the McCormick Tribune Foundation joined with the American Bar Association Standing Committee on Law and National Security to host a session entitled "Counterterrorism Technology and Privacy" as part of the foundation's Cantigny Conference Series. The series aims to facilitate in-depth discussions of major issues facing the country in the belief that an active and knowledgeable citizenry forms the backbone of American democracy.

This conference, held in June 2004 at the foundation's estate just outside Chicago, was attended by civil liberties experts, federal law enforcement and security agency officials, members of the media and former members of Congress. Participants engaged in passionate conversations about people's expectations about privacy and the ways that advances in technology have influenced those assumptions. They discussed emerging techniques in data mining and surveillance and explored the ways that technology could be used to protect civil liberties.

Ultimately, participants set aside differences of opinion to construct a series of principles to help inform future discussions.

On behalf of the foundation's board of directors, I would like to thank the American Bar Association; the National Strategy Forum for assembling the participants and structuring the agenda; and the participants themselves for addressing such a pertinent and controversial topic.

The conversation they engaged in is one that we hope will spark additional discussions—ones that focus on much needed balance—in our quest to overcome the threat of terrorism.

Richard Behrenhausen
President and Chief Executive Officer
McCormick Tribune Foundation

Conference Summary

The stakes could not be higher. Terrorists hope to cause mass casualties here in the United States. Finding the terrorists and stopping them are crucial jobs for government. Information technology is a tool with great promise in the fight against terror. At the same time, privacy is one of the freedoms that define what we are fighting for. Aggressive new uses of information technology raise questions about whether our privacy will be a casualty in the war on terror.

At first glance, the conflict between privacy and technology seems irreconcilable. If we must choose one or the other, the decision will be painful and divisive. Indeed, the last few years have seen numerous controversies (Total Information Awareness, CAPPS II and more) based on the assumption that new uses of technology will inevitably mean new limits on privacy.

In fact, that assumption is open to grave doubt. The objective of the conference was to identify the issues - and perhaps some common ground - on the use of counterterrorism technology. The conference attendees represented a cross-section of the debate. Some were officials from intelligence gathering or law enforcement agencies. Others came from civil liberties organizations and backgrounds. Participants included government officials; former Members of Congress; federal law enforcement and intelligence specialists; members of the legal, business and academic communities; and the media. The purpose was to explore the tension between technology and privacy in the war on terror, and to

get beneath the sound bites and bumper stickers that often dominate in Washington.

In two intense days, the participants did just that. The issues were debated with passion and in the end, resulted in a remarkable amount of agreement. Although the purpose of the meeting was not to produce a formal accord on the topic, and no one came with authority to do so, the fact remains that speaking off-the-record and in an atmosphere of candor and good will, a rough consensus was in fact reached on the principles that should apply as government seeks to bring information technology to bear on one of the most deadly challenges of the 21st century.

Following up on this surprising convergence, some of the participants produced a set of principles meant to capture the essence of the discussion. Without suggesting that every participant agrees with every one of the principles, we are pleased to be able to offer the principles as a way for men and women of good will to find common ground on this difficult yet vital issue. This publication presents not just the Cantigny Principles, but also a detailed summary of the proceedings that led to them. All of us who helped to organize or participate in the event are proud to have been associated with such a constructive dialogue on the part of so diverse a group.

Stewart Baker
Chair
Standing Committee on Law and National Security

Introduction to Statement of Principles

Technology permits governments and businesses to collect, store, analyze and disseminate enormously large amounts of routine and sensitive information about daily human transactions. This information is stored worldwide in open-source and limited-access databases controlled by governmental and commercial entities. Access to relevant information is critical for government and corporate decision making. However, simple access in a world of terabyte storage is often not enough. Automated tools can be used to effectively extract correlative and predictive analyses from multiple databases that will provide government officials and corporate executives information products to make important business, risk management and security decisions. Governments and businesses already use automated search and predictive tools for purposes that range from intelligence analysis and law enforcement to customer behavior and market analysis.

A government has no greater imperative responsibility than to use all available and lawful tools to protect its citizens from the illegal and depraved enterprises of terrorists. Powerful automated data mining applications that analyze a broad range of multiple, diverse databases may prove to be effective tools to fight terrorism and crime. Indeed, these analytical tools may help to "connect the dots" before another catastrophic act of terrorism occurs.

A government has no greater imperative responsibility than to use all available and lawful tools to protect its citizens from the illegal and depraved enterprises of terrorists.

Yet, the use of powerful new technologies also poses certain

concerns. Access to such a broad array of existing databases and a powerful capability to aggregate and analyze information on a specific person or groups of people raises serious privacy issues. For example, existing laws do not regulate the government's use of commercial data for counterterrorism purposes. When the ability to aggregate data is weak, members of the public consider themselves anonymous in their daily activities, reflecting a "practical obscurity." As we deploy new technologies that eliminate that obscurity, we must come to grips with the implications for Americans' sense of privacy and the lack of statutory guidance in this area, and establish strict guidelines to ensure that those facing adverse consequences as a result of those technologies have adequate redress mechanisms.

As we deploy new technologies that eliminate that obscurity, we must come to grips with the implications for Americans' sense of privacy and the lack of statutory guidance in this area, and establish strict guidelines to ensure that those facing adverse consequences as a result of those technologies have adequate redress mechanisms.

Information stands as our first line of defense, and determining the United States government's access to and its lawful yet effective use of information is the single most important core element of reorganizing our nation's defense infrastructure and counterterrorism efforts after Sept. 11, 2001. The purpose of the Statement of Principles is to provide guidelines to govern the government's use of information that will balance the responsibilities of our democracy in protecting the privacy and safety of all American citizens and resident aliens. These principles are intended to steer reorganization efforts and government policies to permit robust access and use of all available information for national security and law enforcement purposes while forcibly safeguarding an individual's interest in privacy. They are a distillation of the vigorous debate that occurred during the McCormick Tribune Foundation's Cantigny Conference on Counterterrorism Technology and Privacy, but they do not necessarily represent the agreed views of every participant.

Statement of Principles

Core Principles

1. Government should infringe on privacy only as an imperative to protect the safety of U.S. citizens and resident aliens.

2. The legislative and executive branches share the fundamental constitutional responsibility to protect the privacy and safety of all U.S. citizens and resident aliens - and should act in partnership.

3. The legislative branch should provide the statutory authority for the government to have appropriate, lawful access to and use of information stored in government and commercial databases for national security and law enforcement purposes. This authority should also protect privacy, differentiate between national security and law enforcement uses and establish a streamlined, robust congressional oversight mechanism to support its constitutional responsibilities.

4. The executive branch should have clear and robust statutory authority to access and use all relevant information stored in government and commercial databases in support of its constitutional responsibilities and subject to its constitutional limitations, and to share routinely that information as needed between law enforcement, intelligence and national defense agencies.

5. Both law and technology can and should be integrated to provide complementary protections for the privacy and safety of all U.S. citizens and resident aliens.

6. The government should maintain an open dialogue with domestic and international private sectors concerning access to and use of commercial databases.

7. The government should keep the public well-informed about how personal information is being collected and used for national security and law enforcement purposes and what safeguards are in place to protect their privacy.

The Collection and Storage of Information-A Distributed Network of Databases

8. Information collected and stored in government and commercial databases should be as reliable and accurate as practicable.

9. Regulatory guidelines should be established to ensure information stored in government and commercial databases remains as current, accurate and useful as practicable.

10. Regulatory guidelines should be established to provide for an adjudication process in the event any adverse consequences result from the use of information stored or used by the government. This regulatory process should not preclude eventual judicial review.

11. Best business practices should be established by regulatory guidelines to ensure the information maintained in government databases are adequately secure from theft or unauthorized access.

12. Best business practices should also be established for data retained or used by the government to ensure the continued availability of relevant information and to ensure that information that has lost its value over time is not used.

13. Personal information about U.S. citizens should be separately identified whenever possible and provided additional security and privacy protections.

14. Information stored in government databases and the use of new technologies should remain subject to the Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

15. Information stored in government and commercial databases that is relevant and useful for national security and law enforcement purposes should remain decentralized but be organized by a centralized directory within a distributed network with layered access levels so as to avoid consolidation into massive databases solely for the purposes of national security and law enforcement searches.

The Analysis and Dissemination of Information - Limited and Controlled Access

16. National security and law enforcement agencies have a diverse range of needs to access and analyze various types of databases, and should have ready access to databases depending upon their respective missions and specific requirements, but they should only be granted access to information directly relevant to their agency's mission.

17. To facilitate and control access, an infrastructure should be established by law and regulation that permits a cadre of specially cleared personnel throughout the federal, state and local government levels who are specifically authorized in the performance of their duties to use automated search and predictive tools on this distributed network of government and commercial databases for limited national security and law enforcement purposes.

18. The government should provide appropriate monetary compensation and preserve the confidentiality of commercial databases when it obtains access to such databases.

19. This infrastructure should not be a separate department or organization, but a cadre of personnel within federal, state and local government offices who have been granted access and requisite permissions to the centralized directory and distributed network of databases who will be authorized to use automated search and predictive tools only on the databases within this distributed network that are relevant for the mission of their organization, and who shall be subject to audits, rules and limits to this access.

20. A cadre of representatives within federal, state and local government offices is in the best position to identify the relevance, utility and reliability of the databases they desire to search from the range of databases within the network to which their office has been granted access.

21. This cadre of representatives should be able to choose what databases within this distributed network of databases are relevant to their search by having access to the centralized directories.

22. To the greatest extent possible, the centralized directory as well as automated search and predictive tools should be utilized in such a way to provide anonymity unless and until a particularized basis for piercing

the veil of anonymity is demonstrated.

23. The highest standards of security, logging, accountability and other best business practices should be applied to controlling access to and monitoring the use of this distributed network of databases to ensure all reasonably available policies and technologies are used to safeguard the privacy of individuals and security of the network.

24. Appropriate standards of business continuity and disaster recovery procedures and capabilities should also be applied to this distributed network of databases.

25. This infrastructure should have an inspector general responsible for the oversight of the privacy and security of the centralized directory and distributed network of databases and who should conduct periodic security and privacy inspections and audits.

26. This infrastructure should also have an ombudsman whose responsibility is to assist in the development of privacy safeguards.

27. All access and searches on this distributed network of databases should be electronically recorded in a permanent file that the cadre of specially cleared personnel does not have access to and that discloses tampering if impermissible access is attempted.

28. The executive branch should implement regulations ensuring that appropriate officials throughout the local, state and federal governments responsible for national security and law enforcement have appropriate and timely access to information and the analyses that result from automated searches of that information.

29. Once information has been lawfully collected and stored in a government or public database, no additional judicial authorization should be required for this cadre of specially cleared personnel to analyze or use automated search and predictive tools on that information for legitimate national security and law enforcement purposes.

30. Once information has been lawfully collected and stored in a commercial, nonpublic database, the cadre of specially cleared personnel should provide notice of access to the commercial data holder prior to analyzing or using automated search and predictive tools on that information for legitimate national security and law enforcement purposes.

31. This cadre of specially cleared personnel (including all others within the legislative and executive branches as well as state and local

officials with access to the centralized directory and this distributed network as well as the analyses that result from automated searches of that information) should receive periodic briefings and training on privacy issues and be subject to criminal prosecution and civil liability for the unauthorized release or use of that information.

Research and Development-Supporting Privacy, Security and Mission Functionality

32. The executive branch should develop and retain a robust research and development capability that aggressively focuses on emerging technologies to ensure the protection of privacy, security of information and access and capabilities in support of legitimate national security and law enforcement purposes.

33. Research and development initiatives should have the freedom to explore all conceivable technologies and tools, and no adverse consequences for individuals should result from their authorized research and development activities.

34. Research and development initiatives should be conducted in parallel with applicable implementing policy, including addressing privacy protections at each step of the development process. These policies should be vetted through a policy and technical review committee that should include experts from the following disciplines: technology, security, privacy and public affairs as well as representatives from the legislative branch and the private sector.

35. The legislative branch should be regularly kept informed of ongoing research and development initiatives and the corresponding policies under consideration.

36. The legislative and executive branches should institutionalize relationships and work hand-in-hand with the private sector, think tanks, universities, research labs, nongovernmental and intergovernmental organizations, foreign countries and other entities both domestically and internationally in establishing research and development initiatives.

Chapter One:
Introduction to Conference Report

Several years ago the FBI alerted the Department of Defense (DOD) Office of Counterintelligence that a person working in one of the department's laboratories had been identified as a spy. In the course of the investigation it was learned that the Defense Intelligence Agency had previously discovered that a foreign intelligence source was trying to infiltrate certain classes of DOD activities, including the activity where the spy was located. That information, which could have led to earlier detection of the spy, was not pursued. The case highlighted the reactive nature of DOD counterintelligence and caused a reappraisal of DOD practices in this area. In contrast to DOD procedures, it was noted that the intelligence community took a more proactive approach and made use of various analytical methods to try to anticipate security problems.

In the aftermath of that case, DOD undertook an experiment to test analytical methods, including pattern identification, with the goal of developing techniques that would help identify spies, the areas on which spies might be focused and which DOD activities might be vulnerable to penetration. The results of the experiment were unsettling. Using an approach that identified hostile intelligence sources and national security secrets that needed protection, the exercise produced some 30,000 worrisome correlations. Though marginally designed, the experiment made clear that the technology was powerful and that to be successful, management discipline from the earliest stages of any similar investigation would be essential to maintaining control.

The Effective Use of Technology

Americans are ambivalent about the government's use of technology, even to locate terrorists, because of concerns that personal privacy will be compromised. These concerns are not diminished by the knowledge that the commercial sector already possesses large amounts of personal information, since it is generally believed that private sector use of such information might be an annoyance, but for the government to have that kind of information could be a real threat.

Americans are ambivalent about the government's use of technology, even to locate terrorists, because of concerns that personal privacy will be compromised.

So this atmosphere, where the government is charged with protecting citizens but where those citizens are loath to allow the government to use the tools necessary to carry out that responsibility, presents a challenge. It was suggested that the only way to bridge the gap is to restructure the government's rules for oversight and accountability. It was argued that, for citizens to support government use of powerful surveillance technologies, the public must first be persuaded that they are protected from government abuse by equally strong oversight and accountability procedures.

Oversight and Accountability

There are three primary areas of oversight and accountability:

1. Environmental oversight exists in the institutions that link government and the citizens. In the executive branch, this means the Office of the President and the other offices in the administration with responsibility in this area. In Congress, the relevant institutions include the House and Senate Intelligence Committees and the Judiciary Committees, which have jurisdiction over the law enforcement community.

It was argued that environmental oversight, and particularly the functions connected to the congressional committees, is in some disarray. The committees are too large and too partisan to be managed properly, they are run by the staff instead of members and they are preoccupied with micromanaging details that would be better left to professionals in the field. The changing nature of the issues has outstripped the ability of Congress to respond with effective oversight. Also, it was noted that the Department of Homeland Security reports to 87 different committees and that the entire system of committee oversight should be revised.

2. Structural oversight refers to the structures created by organizations charged with accountability. These structures would include the Foreign Intelligence Surveillance Act (FISA) court, the President's Foreign Intelligence Advisory Board (PFIAB), the inspector general offices and the various sets of guidelines that govern domestic surveillance activities.

It was argued that the structural elements of oversight, such as the PFIAB and the FISA court guidelines, are weak and enforced inconsistently. For example, the FISA court handled petitions requesting wiretap authority in different ways, with the result that the threshold for approval of petitions from those who had successfully submitted them previously was too low and the threshold for those who had not had petitions approved before was too high.

3. Transactional oversight refers to the accountability required for specific activities, such as securing of court orders authorizing wiretaps. To strengthen oversight and accountability at this level, it was argued that privacy protections should be embedded as policy restrictions in the technical system from the system's inception.

As a system with improved oversight and accountability, the following example was offered: a structural oversight operation, like a PFIAB, with a group of inspectors general reporting to it, approves the policy guidelines for operation of a data collection system. To ensure accountability during operations, special masters would be appointed to

work with analysts to oversee and receive questions from them about operations, such as when an analyst who has reached a certain point in an investigation can be authorized to take the next step. The special masters, who would have access to the FISA court, would be in a position to respond to analysts' inquiries more rapidly, ensuring an improved level of accountability, without unnecessarily slowing down the investigation. The system would also require a more aggressive training program for all analysts. The people who receive technical training required to operate the system then must also receive training regarding privacy compliance requirements. It was suggested that the model for this type of employee training is the National Security Agency (NSA), where employees at all levels train continuously. It was suggested that inspectors general might be used to monitor training and certify analysts/employees according to their level of competency. It was emphasized that training would be especially important in the proposed system, given its powerful capabilities and because results of investigations would be distributed to law enforcement agencies from the federal to the local level. Discipline in handling information would be critical and must be made part of the structural system.

Discipline in handling information would be critical and must be made part of the structural system.

It was acknowledged that it would be difficult to construct a system based on the understanding and commitment of employees that they will be accountable for its operation. There will be mistakes, but the danger faced by the nation demands a response the American people will respect and accept. The challenge will be to construct the system and, at the same time, persuade the American people that they will be protected from government abuse by the system's own oversight and accountability procedures.

Discussion then focused on the following issues:

Citizen participation in the oversight process was argued as the only way to ensure the acceptance of the system by the American public. It was suggested that the judiciary would not accept a role in providing

oversight because that would be viewed as an imposition on the executive branch. It was argued, however, that the concept of the ombudsman, the independent observer who is not a government employee but is appointed without government approval, should be considered. As long as people in government service completely control the process, it is not likely to be trusted or accepted. In response, the speaker emphasized that the goal was not to make the judiciary participate in the system but to have the oversight structure more integrated into agency operations so independent rulings could be received when necessary, earlier in the process, to prevent mistakes by analysts and otherwise expedite system procedures.

Another participant asked why, if the proposal was to build a rule-based processing system, the speaker did not suggest a technical solution for dealing with rulings. It was noted that in the corporate world 24/7 online customer service was commonplace, and judicial rulings could be handled in a similar way. The special master could receive and respond to queries from analysts online as well as requesting warrants. Such technical solutions could be incorporated into the system.

A participant who supported the idea of building privacy protections into the system from the beginning raised the question of how to protect the privacy rules once they are in place.

A participant who supported the idea of building privacy protections into the system from the beginning raised the question of how to protect the privacy rules once they are in place. It was noted that there would be pressures to change rules and that such changes can often be accomplished with little fanfare. It was suggested that apprehension over what might happen later was causing opposition to the new systems now, in their entirety, because of concerns that the rules would be quietly changed later on. It was acknowledged that this could be a problem especially when one political party controls both ends of Pennsylvania Avenue, but it was argued that obstruction of all changes carried real risks because the environment is now too dangerous.

But is it possible to write rules adequate to the task of protecting privacy? It was noted that government privacy offices currently focus on the question of whether there have been violations of the Privacy Act and suggested that a better way to guarantee protections was to create new government offices whose sole responsibility would be to address civil liberties problems. Such offices would require access to classified information, because an advocate without access to internal agency workings would be useless. It was agreed that concerns about whether new rules would be adequate to the task of securing privacy were justified, but the speaker argued that the development of new technical systems to protect society and individual privacy was a challenge that had to be accepted as the government's first responsibility. It was agreed that both sides that the people who focus on national security and those who want protection from our own government must focus on this problem.

Chapter Two:
Expectation of Privacy

The Use of Technology vs. the Expectation of Privacy

To establish a context for the discussion, the moderator offered observations about privacy and what citizens expect in the way of privacy today. While the concept of privacy may have changed in the aftermath of Sept. 11, 2001, the government needs to intrude on its citizens' expectations of privacy to pursue the War on Terror remains one of the most important elements of the debate. At the theoretical level, it was suggested that current notions of the right of privacy could be summarized as:

- Absolute rights, such as a citizen's right to counsel in criminal proceedings, with the understanding that a defendant's communications with counsel in these circumstances should remain confidential.

- Rights attached to persons under particular suspicion, such as requiring the government to demonstrate probable cause before it can obtain warrants for searches and wiretaps. It was suggested that requiring the government to demonstrate probable cause before gathering information on individuals suspected of membership in terrorist groups operating in the general population would be inappropriate.

- Rights to privacy in personal information. It was suggested that there is less agreement on the extent of an individual's right of privacy in personal information. At least with respect to the government's use of such information, the expectation of privacy is high, but the government

can access such information through searches/seizures authorized by the Fourth Amendment. Outside the criminal context, the issue of government access to a citizen's personal information is considered a threat to privacy because of the possibility that the information could be used to embarrass or blackmail citizens.

Outside the criminal context, the issue of government access to a citizen's personal information is considered a threat to privacy because of the possibility that the information could be used to embarrass or blackmail citizens.

• Reasonable access to personal information. The standard of reasonableness, which also derives from the Fourth Amendment, balances the government's interest in access to information against the citizen's privacy interest in the same information. The concept of reasonableness is especially pertinent here because it bears directly on the government's right to obtain and review information about citizens collected by the private sector and maintained in commercial data banks.

The discussion focused on the following issues:

Defining and Protecting the Right of Privacy

The question of whether the government is capable of using the new technological tools required to fight the war on terror and still protect the public's expectations of privacy was raised. Some argued that the protection of privacy should be paramount, but that it was possible to use these tools under rules that could protect both security and civil liberties.

Some argued that the protection of privacy should be paramount, but that it was possible to use these tools under rules that could protect both security and civil liberties.

On the question of what privacy means to Americans today, it was noted that, while the concept of privacy involves elements of secrecy and confidentiality, it also involves concepts of control and fairness. The government's use of personal information is seen as more threatening than the similar use by private entities. This is

because citizens see the government's use as threatening, while similar use by private entities is merely annoying. It was argued that new rules are needed to control government access and use of such personal information.

It was suggested that the elements of the new rules can be found in the Privacy Act of 1974. The concepts of privacy established in the statute are based on fair information principles that remain relevant. The principles include: notice to an individual before personal information can be collected; the collection of only so much information as required for the task at hand; use of the information only for the purpose for which it was collected; insistence on data quality, accuracy, completeness and timeliness; access for citizens to their own information and an opportunity to correct errors; redress for citizens who suffer adverse consequences as a result of the use of their data; and security and enforcement mechanisms commensurate with the sensitivity of information that is in the system. Since 1974 this language has also been incorporated into other privacy statutes, such as the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., and it can be argued that the private sector is subject to more stringent regulation to protect privacy than the government.

The need to control how the government handles information and uses it to make decisions about citizens calls for new rules to eliminate the conflict between privacy and national security interests. The new rules should require that no data can be collected on an individual until the individual has been notified that information is being collected, that all such data be of good quality (since inaccurate information serves no useful purpose), that the data be relevant to the task at hand (i.e., no fishing expeditions and that the data be subject to audit/security protections (to prevent unauthorized access/distribution).

When Congress passed the E-Government Act of 2002 (H.R. 2458), it enhanced personal privacy by requiring, in Section 208, that federal agencies should publish Privacy Impact Assessments before deploying new information technology programs for the collection of personally identifiable data. Section 222 of the Homeland Security Act (H.R. 5005) contains new privacy protections including the establishment of a privacy

officer in a cabinet level department. Congress directed the privacy officer to promote best practices with respect to privacy and ensure that the use of technology by government enhances privacy protections for personally identifiable data. It was argued that the existing structure for protecting privacy, especially as modified by recently passed legislation, is a sound basis for ensuring that personally identifiable information collected by the government is protected.

Participants posed a number of questions, including whether the "mere viewing" of personal records violates a person's right of privacy in those records, even if there is no consequence from the inspection and even though the person may not have been aware that the inspection took place? A number of views were expressed in response: some felt that because the act of collecting and retaining personal information in an electronic database creates the "opportunity for abuse" that unauthorized inspection would constitute a violation of a person's rights. It was said that the collection and maintenance of personal information creates a "general sense of chill" that may alter a person's behavior.

Focusing on the potential for abuse, a participant offered this example: while collecting information on potential terrorists the government collected information on Muslim immigrants solely because they were Muslim. On the belief that the government always uses data it collects, the challenge to civil liberties comes from the risk that government will use the data against people who may be included in that group (i.e., peaceful Muslims) but who, while not terrorists, may be vulnerable to prosecution for other reasons. It was argued that a system for collecting and analyzing data must be designed that, in searching for terrorists, allows data about groups to be collected but prevents the government from using that data against members of the group who are not terrorists.

But citizens are aware that personal information is collected about them every day, it was suggested, and their expectation of privacy must be balanced against society's need to protect itself.

But citizens are aware that personal information is collected about them every day, it was suggested, and their expectation of privacy must

be balanced against society's need to protect itself. "It is rational to have some additional level of scrutiny of people from terror-sponsoring countries," and while there is always a risk that law enforcement action will be too broad, it was argued there are other ways to use privacy rules to protect the group being investigated.

Participants discussed whether an inspection of records when there are no consequences for a citizen violates that citizen's right of privacy. But people make judgments every day balancing their privacy against their convenience. Citizens understand that when they use a credit card, for example, information about them and/or the purchase goes into a commercial database. However, they use the card anyway. The voluntary surrender of personal information in return for the convenience of using a credit card is a balancing judgment that affects the person's expectation of privacy in that information.

A clear definition of privacy rights was called for because of the need to balance the consequences of taking action to solve a societal problem, such as terrorism, against the possible encroachment on concepts of privacy and individual liberties. However, this is complicated by the requirement of working across jurisdictional lines, each with its own set of equities regarding deterrence versus prosecution. It was suggested that the failure to provide a working definition would undermine the effort to establish rules and procedures that will allow the balancing to proceed.

Ensuring that Information Gathered for One Purpose Is Only Used for That Purpose

Concerns were expressed about the temptation to use information collected for one purpose to be used for another. "Mission creep" in cases involving potential terrorists was cited, but it was generally agreed that effective safeguards, with public notice and invitation for comment when an expansion of the use of personal information was contemplated, would allow the problem to be managed successfully.

Recent problems with a Department of Justice counterterrorism

initiative were then described. People from certain countries (Muslim countries in this case) were asked to come in and register and, when they did, some were arrested for unrelated violations. It was suggested that a "hold harmless" rule, where a person who cooperates in a terrorism investigation would be held harmless from other consequences of being investigated, might be necessary. General consensus was that such a rule would be likely to increase the effectiveness of such an investigation by encouraging participation.

Effective Use of Data Mining

Concerns were also expressed that an irrational fear of computer technology, as evidenced by the conflict that engulfed the Total Information Awareness (TIA) program, threatens to diminish information gathering in the war on terror.

The recent Technology and Privacy Committee (TAPAC) report, intended to give the secretary of defense guidance on the use of data mining in the war on terror recommended: (1) before using computers to analyze intelligence data that may contain personal information on a U.S. person, the department should obtain the approval of the FISA court; and (2), defense analysts be required to get head of agency approval before using Google or other web-surfing tools.

Data mining is no more than the automation of human data analysis, it was argued, not an unconstitutional method of law enforcement that gives the government too much power to investigate citizens. It was suggested that when data mining is used it simply changes the medium of observation from the street to a database but does not change the purpose of the investigation-looking for suspicious patterns of behavior. Pattern identification has always been part of preventive policing and keeps law enforcement from being purely reactive.

It was argued that using computers to analyze data is similar to a police officer examining the same information and does not violate personal privacy. Computers can be programmed to perform searches in ways that preserve the anonymity of those being investigated more

effectively than humans. The speaker objected to opponents of data mining who focus exclusively on worst-case scenarios and ignore other possible outcomes, thereby undermining public confidence. Instead, it was suggested that acceptable privacy controls on data analysis systems should be devised so that all of the nation's technical capabilities can be focused on defeating terrorists.

Two principles were offered as guides to the development of counterterrorism and crime technology: (1) the government should be allowed to use all available technologies to combat terrorism; and (2), the burden of proof to justify the use of technology to analyze personal data should be no higher than human access to such data.

But citizens remain skeptical of the government when it comes to their privacy and, after the demise of TIA, are still suspicious about the government's intention to further intervene in their lives to combat terrorism. General agreement was that the government must do a better job of explaining its intentions, so it will be able to secure the authority to use innovative technologies and do so in a way that honors the Constitution and protects civil liberties.

General agreement was that the government must do a better job of explaining its intentions, so it will be able to secure the authority to use innovative technologies and do so in a way that honors the Constitution and protects civil liberties.

Others raised concerns about data mining, specifically because of the risks to citizens from the Middle East, framing the issue in terms of law enforcement searching for patterns of suspicious activity and following those patterns to create lists of suspicious people. The question was raised: if the objective of using data mining is to produce lists of suspicious people, how can that be accomplished without simply coming up with lists of Muslims? In response one participant with a background in technology suggested that, if the result of a pattern search is "nothing more than a list of Muslims," the search was flawed from the outset. The issue in such cases is what the technician programming the computer tells the computer to do. There is an important difference between a

computer that is searching a large database and one that is searching that database under the control of a narrowly crafted set of instructions.

Another participant offered guidelines for use in analyzing pattern search results: Were the persons in control of the computer responsible? Was their training effective? What rules guided their activities? How were they overseen? Most importantly, what were the consequences of any misbehavior? Using the National Security Agency as an example, the participant pointed out that people will always be at risk of doing the wrong thing but, with proper training and direction, they can also do it right. Finally, the participant noted that if we cannot get beyond the risk that people may do the wrong thing (and therefore violate someone's privacy), we risk handicapping the whole effort to use technology to find terrorists before they strike.

In the early stages of the investigation, if the terms of a search were devised so there was no identification of individuals, pattern searches using data mining could be conducted and individual privacy could be protected. In response to a question about why the government was not already using such techniques to track individuals traveling between the U.S. and Middle Eastern countries, for example, it was noted that the government does not search flight data because it does not have access to it. Such information is only available from the airlines with their cooperation. It was further mentioned that federal law enforcement does not now regularly receive information on individuals from either U.S. Customs or the Immigration and Naturalization Service.

Regarding whether government agencies would use data mining to search data bases to develop lists of people fitting certain patterns, a participant commented that law enforcement usually starts with a known individual and works back from that point, using data (e.g., credit cards, phone records, frequent flyer numbers) to connect the individual with others. With data mining, the effort would reverse, beginning with general questions and working back to individuals. However, law enforcement agencies are more concerned about automating data it already has. The goal is greater efficiency in using data already collected, not collecting more data because it may be needed in the future.

Another participant described data mining as a method of identifying behavioral characteristics of people already identified as terrorists. As more such characteristics are collected, patterns emerge that can be applied to larger pools of data to identity others as targets for further investigation. At the first level such searches have no consequence because no actions are taken except to establish that some individuals should be the focus of more penetrating examination at the next level. Data mining was merely the technological enhancement of what police officers do every day and, while it is likely that some groups will be more represented among those identified for further investigation, it was suggested that the result constituted "correlation as a matter of effect, not as a matter of intent."

But this shift of operational method that makes people uncomfortable. Instead of focusing, as the criminal justice system usually does, on punishing conduct that has already occurred, we now look for prevention. However, this is a different environment and the response called for is not criminal justice. It is "war, or close to war," and for the participant, that is the defining issue. For adherents to be successful, it was recommended that data mining and people's discomfort with it should be discussed in the context of fighting terrorism, that is, the necessity to take preventive action to intercept and neutralize people who have not yet committed a crime but who are part of an effort by the enemy to wage war against us.

Preventing the Government from Abusing Personal Information

The risk to privacy from the abuse of personal information was a general concern and a participant suggested that since data is now ubiquitous and will be available to the government for analysis eventually, we should prepare to deal with potential abuse, misuse and mistakes in the handling of such information by government representatives. The focus on whether to take action reactively (after events) or preemptively (before events) misses the point, because intelligence cannot know ahead of events what will be actionable. Participants called for a new set

of rules to instruct government employees about how new technologies can be used. It was argued that, if the government is not permitted to use the new tools, the private sector will respond to the opportunity to gather and analyze information and government agencies will end up buying information that the agency is not allowed to collect on its own.

For some people the concept of privacy confuses secrecy with anonymity. Privacy may not have disappeared, but the ability to live in secrecy largely has. So it is time to create new rules of privacy that will dictate to government agencies the consequences of improper use of personal information.

There was general agreement that, while we must be alert for abuses, it would be a mistake to let the fear of abuse prevent the government from taking action. Also, that the risk of abuse must be balanced against good results. Regarding the overreaction to TIA, it was noted that work was suspended before it was understood what the system was capable of doing. As a system, TIA may have proved to be inadequate and would have led to the elimination of TIA. However, it was agreed that the emphasis should remain on balance, and it was generally agreed that a workable balance between privacy and the uses of technology was possible and necessary.

There was general agreement that, while we must be alert for abuses, it would be a mistake to let the fear of abuse prevent the government from taking action.

Finally, it was pointed out that, since Sept. 11, 2001, the government has assumed significant new powers over personal information that affect privacy, but that the use of those powers has been largely hidden from public view. One participant raised a question about the lack of information on detainees taken into custody after Sept. 11. For example, it was alleged that the government declined to make any information available about the detainees. That characterization was disputed, however, and it was argued that because there must be some secrecy in the war on terror, "complete transparency" in everything the government does should not be expected. Conferees were also reminded that, under the Patriot Act (H.R. 3162), the government is required to report to the

House of Representatives on its activities. Finally, it was suggested that at some level it must be acknowledged that this is war, not a criminal prosecution, and the expectation that the government will disclose everything it is doing may not be realistic.

Chapter Three: Law Enforcement vs. Intelligence / Preemption

The Need for Collaboration

Before Sept. 11, 2001, the demand for more effective action against global organized crime and drug trafficking had focused attention on the need for greater collaboration between the law enforcement and intelligence communities. Sept. 11 caused a total reevaluation of that relationship. The reevaluation continues, but clearly the old distinctions between international threats to national security and domestic threats from terrorists have lost much of their meaning.

Closer collaboration between the two communities is the goal, but conferees were reminded that the two communities have very different methods of operation. Intelligence tends to collect information from numerous sources, often of varying quality, and bases its recommendations on that imperfect information. Law enforcement tends to insist on real proof and hard evidence and usually excludes information that fails to meet that standard. The difference in methods arises from the fact that law enforcement must ultimately subject its results to the criminal justice system, while the intelligence community does not.

Interaction between Law Enforcement and Intelligence

Many are now demanding that the Central Intelligence Agency assist in the collection of intelligence on U.S. persons. In response, the

legal principles guiding the CIA were reviewed, starting with the National Security Act of 1947 (50 U.S.C. 404), the CIA's fundamental legal authority. The act authorized the CIA to gather intelligence, but specifically prohibited the agency from exercising any domestic police, subpoena, law enforcement or internal security functions. The act is silent on the issue of CIA collecting, retaining or otherwise handling information about U.S. persons. Those principles are found in Executive Order 12333, issued by President Reagan in 1981. Executive Order 12333 grants those authorities to the agency, but only under procedures approved by the attorney general. It was then noted that CIA still operates under procedures established by the attorney general 22 years ago, and it was suggested that those procedures have handicapped the agency's ability to accommodate today's emerging technological capabilities.

The CIA has provided intelligence it discovers about domestic criminal activity to the law enforcement community for years, but now, for the first time, the Patriot Act requires the law enforcement community to provide the CIA with foreign intelligence that is discovered during the conduct of domestic criminal investigations.

The Patriot Act significantly altered the intelligence landscape. The CIA has provided intelligence it discovers about domestic criminal activity to the law enforcement community for years, but now, for the first time, the Patriot Act requires the law enforcement community to provide the CIA with foreign intelligence that is discovered during the conduct of domestic criminal investigations. This means intelligence now flows both ways and that the CIA can now collect intelligence on U.S. persons, as long as it complies with the attorney general's rules. In this changing environment the CIA now labors to take advantage of the latest technologies to accomplish its objectives while conforming to restrictions placed in its governing rules years ago.

Distinctions between law enforcement and intelligence methods of operation were then discussed. While law enforcement is traditionally viewed as looking backward to reconstruct crimes that have already occurred, intelligence gathering is regularly

done by law enforcement as part of its investigative work. Real distinctions were noted, however, in the way the communities are motivated. Law enforcement is judged by whether investigations lead to the successful arrest and prosecution of criminals. Because that process usually leads to a trial, officers are motivated to follow the rules. Otherwise, the prosecution is likely to fail. Intelligence investigations are conducted with the expectation that the actions of investigators will remain secret. This does not mean intelligence investigations ignore the privacy interests of their targets, but it does mean that a target's privacy rights are likely to receive more attention in a criminal investigation. It was argued that, because of these distinctions, the objectives of the intelligence and law enforcement communities should not be combined, but that the exchange of information authorized by the Patriot Act should continue and expand.

The issue of whether the Federal Bureau of Investigation stands as the agency still to lead domestic counterterrorism investigations was then raised. Should a new entity, similar to the United Kingdom's security intelligence agency (MI5), might now be necessary? It was noted that the FBI has a history of refusing to share information developed in its investigations with other agencies. In the past this refusal was based on the restriction against sharing Title III information outside of law enforcement or on the restriction against sharing grand jury material. The Patriot Act removed these barriers, but it was noted that the change had not yet resulted in the full sharing of information. It was suggested that the creation of a new agency would only increase the number of parties that should participate in the sharing of information and was argued that a more effective solution would be to leave the agencies alone but change the internal culture so that more sharing actually occurs.

Rather than create a new agency, it was argued that new attitudes requiring the sharing of information would allow for more effective use of new technologies that would make the entire system more effective, while protecting civil liberties. There was general agreement that the creation of a limited purpose agency, like an MI5, risked establishing new walls of separation between law enforcement agencies. A better solution would be to improve the working relationship between the existing

communities.

Legal Status of the "U.S. Person" Distinction

The issue of whether the U.S. person distinction was now obsolete, at least in the context of data analysis, was raised. Participants expressed a number of views and there was general agreement that there are no rules that now require a differentiation between U.S. persons and non-U.S. persons with respect to data analysis. The difficulty in dealing with commercial databases is that such collections contain personal information on U.S. and non-U.S. persons, but the national status of those persons is not a data attribute. Therefore, the rights those persons are entitled to under U.S. law differ according to their status. A participant raised the additional issue of data sharing with international agencies and the difficulties that arose from different rights accorded to persons under differing legal systems. This person called for new international rules to deal with the issue and suggested that such rules could allow for the review of data without tying the data to a particular person until a later stage of the investigation.

Inadvertent Collection of Information

However, while information sharing among law enforcement agencies was an attractive idea, certain kinds of investigatory authorities, such as warrants, are granted because they are limited. It was also urged that the sharing of too much information between agencies could undermine search limitations and lead to the violation of privacy rights. Another participant suggested that, while the issue of how to handle incriminating information that is gathered inadvertently is a policy question, the decision could be used to make the extension of search authorities more acceptable to the public. It was argued that agencies should not be forced to ignore evidence of significant criminality inadvertently discovered and that the best way to prevent abuse was to limit the use of evidence collected on a search to the prosecution connected with the original purpose of the search.

Selective Prosecution

The issue of selective enforcement was also raised in the context of pursuing the results of investigations. For one participant, the pursuit of particular individuals or groups was simply a decision about where to concentrate limited prosecutorial resources. Such decisions could always be justified, as long as defendants were being prosecuted for real crimes. Others were less convinced, arguing that as long as the focus was on particular groups, such as Muslims, the decision to prosecute those individuals or that group was inherently suspect. As an example of selective prosecution, a participant offered the federal "absconder program," which is intended to find and deport aliens whose papers have expired, but who have remained in the country. With an estimated 300,000 absconders in country, the majority of whom are thought to be Hispanic, the enforcement agency placed a priority on Arab and Islamic absconders. It was argued that this was an instance where ethnicity was unlawfully used by the government to focus an investigation.

Liability for Funding of Terrorist Activities

The question arose of how a U.S. financial institution can protect itself from the liability associated with the handling of funds that appear to be owned by legitimate organizations (i.e., Muslim charities), but which turn out to be funds used to underwrite terrorist activities. In the context of sharing information, the question was whether the government should ever share information it has about these "charities" with the financial institutions. It was suggested that government agencies were not likely to share such information with private sector financial institutions, but it was noted that such information was available from private sector data aggregators. This growing number of data aggregators made one participant speculate that the day is coming when government agencies would purchase information from these services. Another person pointed out that government agencies are already purchasing information from such services.

The question was refined to whether there is a point at which

banks can be judged to have sufficiently investigated suspected individuals and "charities" to the extent that they would not be found liable if it turns out those customers are laundering money for terrorists. It was agreed that financial institutions are taking steps to protect themselves and that the government is not yet involved. One participant estimated that private sector financial institutions will spend more than $10 billion on customer compliance issues over the next 10 years. Another pointed out that the financial industry recently formed the Regulatory Data Corporation to sell "know your customer" services to the U.S. financial industry. These services intend to help the industry avoid the criminal and civil liability they are now exposed to in several statutes. While it was generally agreed that the financial industry must protect itself, participants raised concerns about the outsourcing of data analysis and surveillance to private companies. It was argued that the outsourcing trend might be moving too much of this business into the private sector, away from government and outside the protections of the Privacy Act (and related statutes).

Chapter Four: Surveillance Technology

Technology Threatens Privacy Rights

This discussion addressed the issue of available technologies and how their use threatens personal privacy. The moderator took issue with the premise that there was no difference between data pattern analysis performed by computers and humans. While both perform the same analysis in theory, it was suggested that the power of the computer allows for the analysis of so much data that its use alone makes our privacy less secure.

While both perform the same analysis in theory, it was suggested that the power of the computer allows for the analysis of so much data that its use alone makes our privacy less secure.

Expanding on the relationship of technology and privacy, a recent Supreme Court opinion, the Kyllo case (KYLLO v. UNITED STATES (99-8508) 533 U.S. 27 (2001), 190 F.3d 1041), was discussed. The issue in the Kyllo case was whether the Fourth Amendment required a warrant for law enforcement to use an infrared camera to take pictures of the exterior of a house in an effort to determine if marijuana was being grown in the garage using special lamps. The court held that a warrant was required and relied on separate rationales in reaching its decision. One rationale was based on traditional privacy and sanctity of the home principles. The other rationale, which could have ramifications for the future use of technology, held that a warrant was required because technology was being used to

obtain information about an individual's personal activities that could not have been obtained without the use of that technology. Where the court will go in future opinions is, of course, unknown, but it was suggested that the court could define "privacy" as the ability to be insulated from technical intrusion. Such a line of reasoning could say to law enforcement that it is free to analyze any information, as long as it is not gathered using prohibited technology.

Total Information Awareness-Can Surveillance Guarantee Privacy?

The Total Information Awareness (TIA) program was meant to develop technologies to address emerging national security problems and the decision-making issues associated with them. TIA's goal was to develop technologies that could provide security and protect privacy. But the TIA program encountered significant public relations problems and was terminated. Nonetheless, it was argued that, even in failure, TIA has provoked essential discussion about the nature of the problem we face-how to effectively use our technology to find terrorists who may be planning attacks in the United States.

Finding terrorist cells requires that law enforcement have the ability to pick up the signals the cell inevitably uses, to isolate the signal and to terminate the cell. Al-Qaida cells are presumably operating in the United States now and will continue to do so. Those cells are the target. The challenge for a system developed to penetrate such cells is to model that target and determine how it reacts to its environment. A cell's reactions to its environment are crucial. If reactions can be picked up and identified, investigators will have located their signal. To do this, investigators must be able to conduct pattern-based searches. Pattern-based searches were distinguished from the subject-based searches that are the usual focus of data mining, and it was suggested that, because terrorist sleeper cells work to avoid leaving a data trail, pattern based searches are critical to investigators' efforts to locate and destroy the cells.

Pattern-based searches focus on previously identified worldwide databases containing information that conforms to certain patterns of

behavior. One of the first tasks undertaken by TIA identified these databases. At the same time an effort was initiated to develop "privacy appliances" that would filter the results of the searches and place the resulting information in government-owned repositories. The role of the "privacy appliance" was to confirm the identity and authority of the person requesting the search; to determine if the request was proper; and, presuming it was, to execute the search. Then the appliance would anonymize the data and deliver it to the party that made the request. As a case is built, more details would be revealed until, at the end, individuals would be identified. Finally, the appliance would create an audit trail. The development of the appliance was interrupted by the demise of TIA, but interest in the concept was stimulated and work continues in the classified budget of the Defense Department.

Whether such an appliance can be built remains unknown, but it was strongly urged that the research continue. It was argued that any such appliance should have the following characteristics: the ability to conduct pattern-based and subject-based searches; the ability to establish and authenticate the authority of the person making the request; and, most importantly, the language must be machine-understandable so that the system can be automated. Because large volumes of data must be reviewed rapidly if an attack is to be thwarted, it was argued that the system will not work unless it is automated.

Other Technologies-More Threats to Privacy

Data mining stands as one of many information gathering technologies developed in recent years. The implementation of these technologies has produced the flood of information we now deal with. The flow of information has been stimulated by the introduction of (1) inexpensive and easily dispersible sensors that can be placed almost anywhere and have the ability to locate by detection; (2) new storage devices that have dramatically reduced data storage costs; (3) broadband and wireless communications with the ability to transmit large volumes of information at high speed and with high reliability; (4) dramatic increases in computational processing power; (5) the development of advanced algorithms that allow for the development of data mining; (5) global posi-

tioning system technologies in cell phones, vehicles and personal digital assistants; and (6) the Internet, which makes all this data accessible at any time from any place.

Given the growth of these technologies and their inherent impact on privacy, the following ground rules were offered for consideration by those making technology choice decisions:

- Objectives and applications. These are thresholds at which the technology is set to capture and identify signals and distinguish them from the large amounts of background noise, while balancing false positives (which can net the innocent) against false negatives (which allow terrorists to escape the net). It was emphasized that these thresholds are matters of choice so that, if maintaining privacy was paramount, the threshold would be set at a higher level than it would be if the goal was to find terrorists. But the choice carries its own risks in that, for each level the threshold is raised and privacy is more protected, the likelihood of finding terrorists is lowered.
- Legal regimes. There are several and they have their own sets of standards.
- The quality of the target. Depending on whether the target is cooperative or uncooperative, different surveillance technologies may be called for.
- The sources of required information. Is the information coming from public records or private databanks? Are warrants required? It was emphasized that the data is out there, in government or private hands, and that the question of how it is obtained and for what purpose must be seriously considered.
- Accessing the data. Will the effort to access the data be covert or transparent? Must the targets of the surveillance be notified?
- Will the surveillance be asymmetric? That is, is the government watching you? Or bilateral, where both the government and the target have access to the data stream?

A separate problem arises when trying to sort large amounts of data to identify terrorists. When the amount of data is very large, the challenge is to identify patterns of activity suggesting that the people connected with those activities are planning a terrorist attack without being

sidetracked by false positives or negatives. Dealing with the issue of false signals is crucial to gain public support, and it was argued that methods are available to combat the problem.

It was suggested that data mining was only one of many surveillance technologies currently in use, accumulating vast amounts of data on each of us. Systems of human identification and location; vehicle identification and tracking, including Global Positioning System (GPS) tags, OnStar systems and red light cameras; cell phones and security cameras; and remote sensing were discussed. The unavoidable conclusion is that wherever we go, we leave a trail and, unlike in the past when such information may have been accumulated on tape that was eventually erased, information is now generated online, meaning it will not be erased and is accessible to anyone who can get into the system. Each of these systems can contribute to the war on terror, and each one affects privacy in its own way. The world is changing and the challenges to protecting privacy are significant.

The Age of Transparency

The availability of technology has democratized the gathering of intelligence. It was suggested that citizens participate in the gathering of personal information when they participate in the use of certain systems. The use of technologies like GPS and Global System for Mobile Communications (GSM) cell phones, for example, carries an explicit understanding of surveillance, while the use of credit cards, for example, carries an implicit understanding.

The availability of technology has democratized the gathering of intelligence.

It was argued that the evolution of technology causes dramatic change in the intelligence community. Intelligence has emerged from its traditional role supporting the other national security functions, diplomacy and military operations, into a coequal instrument of power. New forms of intelligence are emerging that must be effectively merged with existing practices. The changes are also reaching intelligence sources and methods. In the current environment there is much discussion about the

need to share information. It was suggested that, because of the need to accommodate new recipients, the sharing of information will require adjustments in the ways intelligence is gathered to protect sources. Moreover, it was emphasized that these changes are occurring at a time when the intelligence community needs more analysts. The shortage of analysts is critical because, with the vastly increased information flows, many more hypotheses must be analyzed every day. The shortage of analysts means this challenge is not now being met, and we risk another intelligence failure if this problem is not addressed.

Another challenge for the intelligence community is to find a way to convey information about these complex issues to decision makers who may not have the background or training to understand this complex information. This challenge is crucial because the principle of transparency has created a new competition for intelligence information and has made rapid decision-making capability a priority. Many of the same technologies and much of the same data are available to our adversaries and, because they have different, perhaps less precise standards, maintaining an advantage in information and technology will require greater effort.

The discussion focused on the following questions.

Will Anonymizing Data Protect Privacy?

Would the collection of data in anonymized form constitutes an invasion of privacy? It was agreed that, even if parties to such scrutinized communications were anonymous to begin with, it did not mean that investigators would not be able to identify them later. A participant returned to the issue of whether a person doing something in a public place has an expectation of privacy in that action. It was generally agreed that different levels of expectations attach to different levels of activity and that perceptions of privacy continue to evolve.

Another participant objected to the characterization of any data as anonymized because that process can be easily reversed. It was suggested that the only way to protect the anonymity/privacy of those who

are involved with scrutinized communications is to adopt procedures that carry punitive sanctions for their violation that are painful enough to persuade the agency that it would be better to follow procedures.

A more technical question about privacy expectations concerned legal distinctions between the content of electronic communications and the address information (i.e., above the subject line of an e-mail). It was noted that, in domestic cases at least, courts have held that there is no expectation of privacy in the address information. In those cases it was held that there is an expectation of privacy in the content of such communications; there is no such expectation in the fact that the communication took place.

The issue of anomalies in the law was brought up. It was noted that one of the functions of the Patriot Act was to eliminate such anomalies and correct the way different modalities of communication were treated under the law. As soon as that was accomplished, however, another set of anomalies emerged. It was agreed that the appearance of anomalies will continue, simply because the evolution of technology moves faster than the law, and it was generally agreed that anomalies will not disappear and that they are a problem to be managed, not solved.

It was agreed that the appearance of anomalies will continue, simply because the evolution of technology moves faster than the law, and it was generally agreed that anomalies will not disappear and that they are a problem to be managed, not solved.

Pattern-based Searches and the Problem of False Positives

Critics have suggested that pattern-based research is a waste of time and resources because the problem of false positives cannot be overcome. One participant responded that some research in this area was promising but cautioned that, thus far, all the research had been based on simulated data. Simulated data does avoid privacy problems for researchers but can also be misleading. Still, it was noted that preliminary tests with simulated data indicated that it was possible to find the simulated terrorists.

Asked to describe the research, the participant described the process of designing a "pattern template" identifying several actions a terrorist cell would take if planning an attack. Terrorist cells are small and that they do things in certain ways; that is, they exhibit patterns. These patterns can be discovered through the application of pattern analysis. It was further noted that the techniques of pattern analysis have been in use for years and their effectiveness has been enhanced by the application of technology to what would otherwise be intimidating volumes of material. Pattern searches can also be thwarted by the cells, whose leaders are intelligent and experienced. They can be expected to vary their patterns to mislead investigators, so the effective use of pattern searches will invariably be painstaking and difficult.

Chapter Five: Data Mining Technology-Retention and Dissemination

Policy Implications of Data Mining

A criticism that surfaced after Sept. 11, 2001 concerned the amount of information on how terrorists financed their activities that had been collected by law enforcement agencies, but which was not integrated for purposes of tracking the terrorists more effectively. Methods used by terrorists to move money, pay for their activities and transfer money from one cell to another can be tracked and data mining technologies will be part of that effort.

Methods used by terrorists to move money, pay for their activities and transfer money from one cell to another can be tracked and data mining technologies will be part of that effort.

The primary technical challenge is to identify the terrorists' signals and separate them from the background noise, but before solving that problem, decisions must be made about the technologies to be used, the targets, the agencies that will conduct the investigations and the rules under which the investigations will be conducted. Some of those decisions are technical, but others are policy decisions.

The TAPAC Report

During the controversy over TIA, the Technology and Privacy

Advisory Committee (TAPAC) was appointed by the secretary of defense to examine the legal issues related to TIA, but it was also charged to consider the current state of American thinking about privacy values. The committee quickly moved past the legal questions, especially after Congress prohibited work on TIA, but spent considerable time on the question of how technologies like data mining, with all of their implications for privacy rights, related to American values. The committee quickly discovered that government agencies were already using data mining and that, because no one was tracking those activities, it could not determine how much data mining was going on.

The committee also discovered that the laws governing the use of these programs were outdated and inconsistent with one another. It was noted, for example, that the Homeland Security Act, passed in November 2002, required the Department of Homeland Security to engage in computerized data mining. Two months later Congress specifically prohibited the Defense Department from doing the same thing.

The TAPAC committee's report was presented to the secretary of defense in May 2004 and contained the following conclusions:

- Data mining was critical to success in the war on terror and that the only issues should be the types of data mining permitted and the rules under which the data mining should be conducted.
- In directing the Defense Department to cease all research on data mining, Congress had taken a step that should be reversed, because further research was immediately required on data mining, other related technologies and the policies that would guide such programs.
- Policy-level privacy officers should be placed in cabinet-level departments, with the ability to access external advisors who would help to develop rational privacy policies.
- Audits should be conducted on a regular basis to assure compliance with departmental policies on privacy.

The committee also recommended that agencies and personnel engaged in data mining be covered by a framework of rules requiring legal and technical training for the personnel and oversight responsibilities for the agency. Under the proposed framework, an agency would be

required:

- to secure written authorization from the head of the agency before engaging in any form of data mining.
- to comply with technical procedures regarding the security and audit trail of data.
- to comply with specified data minimization and data anonymization procedures.
- to comply with special procedures called for when seeking to move data to another area for which the data was not originally obtained (e.g., a different investigation).
- where appropriate, to seek the authorization of the FISA court before taking any action requiring such authorization.

The committee also suggested that since so much data mining was already being done by federal agencies, the framework should apply not only to the Department of Defense and law enforcement agencies but also to all government departments and agencies. The committee also called for a coordinated federal government privacy policy, which would include:

- Privacy training for federal employees having responsibility for decisions with privacy implications.
- Clearer and more sensible rules on the uses of data mining.
- Expanded oversight of such activities by senior agency officials and external advisors.
- More explicit accountability within federal agencies undertaking data mining activities.
- Clarification of the role of congressional oversight including the rationalization of the congressional committee structure to accommodate this responsibility.

It was noted that institutional resistance to the committee's proposals has emerged and is expected to continue, but it was argued that the recommended changes should be adopted, because the changes would lead to enhanced respect for personal privacy and enhanced national security.

The MATRIX Program

The Multi-State Anti-Terrorism Information Exchange (MATRIX) program is designed to use technology and data mining in support of law enforcement. The discussion focused on the partnership to develop MATRIX between Florida law enforcement officials and the federal government. According to program documents MATRIX was designed with the capacity to search as many as 20 billion "public/private" record files as part of the effort to find terrorists. It was noted that, while MATRIX officials had declined to identify what was included under the category public/private records, MATRIX documents made clear that records searched would include "telephone calling records, cell usage and location data and financial transaction data." Program documents were cited to demonstrate that the program used data mining techniques to search personal records in order to find individuals with a "high terrorist factor." The same documents claimed to have identified 120,000 such individuals, which led to "scores of arrests."

It was argued that the suggestion that there were 120,000 "high terrorist factor" people seemed far-fetched, but it could not be determined from the MATRIX documents whether that number was supposed to represent suspects in Florida only or in the entire country. It was particularly noted that MATRIX was not authorized by Congress nor by any of the states in which it did or still operates. While there are guidelines in the contract between MATRIX and the states specifying how the states can use the data, there are no restrictions in the contract about how the MATRIX program itself can use the data. The program was further criticized for lacking clarity about which state officials were authorized to contract for the use of MATRIX, having no system that allowed for the examination of government data bases and for separating information that identified individuals from the rest of the information that was subject to data mining analysis, and having no means of protecting individual anonymity. Neither does the program provide mechanisms for correcting false positive identifications or inaccurate information. It was finally argued that the MATRIX program is a good example of how not to run a data-mining program, and it was gratefully noted that, of the

16 states that originally joined MATRIX, 11 have withdrawn.

It was finally argued that the MATRIX program is a good example of how not to run a data-mining program, and it was gratefully noted that, of the 16 states that originally joined MATRIX, 11 have withdrawn.

Is Greater Use of Data Mining Inevitable?

Conferees discussed the question of whether the increased use of data-mining technology remains inevitable, even after the risks of data mining are considered. It was noted that the same arguments being used against data mining now, mostly based on the potential for abuse, were used in the 1960s to thwart the development of technology to eavesdrop on telephone conversations. Then the subject was privacy in our conversations, and now it is privacy in our personal information. It was asserted that now, as then, the key to the effective use of the technology is the prevention of abuse.

The use of data mining is already common in some federal agencies (the Centers for Disease Control routinely uses it to look for patterns indicating the outbreak of disease). Continued technological developments, including enhanced databases and less expensive storage, are certain to encourage the trend. It was argued that, while preventing the use of an investigative tool like data mining may be satisfying, it is unlikely to stop the use of the technology in the end.

The technology is also commonly used in the private sector and it was suggested that, if the government refuses to use data-mining technology, the private sector and government agencies will be forced to buy information from private sector data miners, who would use different standards with respect to privacy. It was also noted that, because the technology is Internet-based, people outside the United States should be expected to continue development of the technology. The Chinese, for example, are working hard to develop data mining skills to locate dissidents in their country. Having mastered the technology, however, it was suggested that the Chinese should be expected to use the technology to research patterns of activity in the United States.

As a policy issue, it was suggested that data mining will not go away, and the only choice for government agencies is whether they should get in now or later. The advantage to joining the process now, of course, is that the government can guide the development of a framework for a responsible data-mining system. If the government waits until later, it will be required to use the system but will have lost the opportunity to structure the framework. But the government cannot afford to allow the private sector to develop this technology and that, the sooner the difficult job of deciding what the environmental, structural and transactional mechanisms are for controlling this technology is undertaken, the better.

But the government cannot afford to allow the private sector to develop this technology and that, the sooner the difficult job of deciding what the environmental, structural and transactional mechanisms are for controlling this technology is undertaken, the better.

Concerns about the potential for abuse will always exist, it was suggested, but our political structures form an important check on the unhindered advance of the technology. It was noted that partisan politics has always been a tool for limiting abuse by government and that, even though the structure for oversight has its flaws, it is largely in place. It was argued that the challenge will be to enhance oversight by adding structural and transactional mechanisms that make data mining value neutral and disassociating it from the debate over privacy while simultaneously keeping the protection of privacy as a high priority.

American expectations of privacy are under continual assault from constantly developing technologies. It was put forth that the best way to protect personal privacy in this atmosphere is to focus on underlying rules for the protection of privacy, thereby reaching general conclusions about the circumstances in which it is appropriate to violate personal privacy for investigative purposes. It was argued that these general principles should then be applied to all technologies, whether in use now or under development.

The discussion focused on the following issues:

Use of Data Mining (and MATRIX) in Law Enforcement Cases

The question of whether it would be appropriate and more effective to use data mining technology in conventional (i.e., nonterrorist) cases was raised. Using the example of a case involving serial child abductions, a case was made for using data mining to analyze quickly the evidence available in public record databases to move the investigation toward a successful conclusion more rapidly. It was generally agreed that the use of data mining as described in the hypothetical would be appropriate, and it was noted that the operators of the MATRIX program similarly describe their methods of operation. However, it was alleged that MATRIX routinely searches many more records, public and private, some of which should require a warrant, and in so doing violates reasonable expectations of privacy.

The allegation that MATRIX used similar, but more elaborate techniques to identify 120,000 people with "high terrorist factors" was raised again. This time, the focus was on its effectiveness. That is, if MATRIX used reverse-engineering techniques in order to find the 19 hijackers and came up with a list of 120,000 people, but only 8 of the hijackers, how could it be said that MATRIX was effective? Worse yet, what about the 120,000 people? What happens to that list and how will the lives of those people be affected because of it?

Other participants objected to the claim that MATRIX was engaged in data mining. Rather, MATRIX is really using link analysis after a crime, not pattern analysis. Link analysis builds on available evidence by searching public records to make connections that tie suspects to a crime. Participants also expressed a number of views about whether the MATRIX research had stopped after the list of 120,000 names was developed. It was claimed that the list was reduced to 1,200 names, which was then used by the FBI for further investigation. It was argued that no one was arrested simply because his name was on the list of 1,200 and that, because the technique quickly and efficiently developed

numerous leads for further investigation, the use of the technology in this case worked exactly as it is supposed to. It was agreed that the dispute about how much information should be made public must be addressed, but another participant argued that not all information can be made public. In the absence of full disclosure, the participant called for a "calibrated transparency" under which all information might be available to some groups and less information available to others. It was suggested that the need for security, always balanced against the public's right to know, must trump that public right in some cases.

The key issue is how the data was collected and how accurate it is, another conferee noted. If the underlying method for selecting data is flawed, the results will be flawed, even if the system is valid. Concerns were also raised about the prospect of intrusive surveillance of the Muslim community, leading to higher rates of prosecution for nonterrorist offenses in the future.

Are Existing Privacy Protections Sufficient?

Given the capability of these new technologies to analyze data, had the TAPAC committee specifically considered how else the government might use these new capabilities? It was noted that the government's ability to access effectively more and more data would raise levels of discomfort and apprehension for many people, and these capabilities have so dramatically changed the landscape that a different type of privacy risk must be addressed. It was argued that the new technologies have created a need to completely revisit and upgrade privacy laws and those developing the technologies should integrate privacy policy from the early stages of development.

It was argued that the new technologies have created a need to completely revisit and upgrade privacy laws and those developing the technologies should integrate privacy policy from the early stages of development.

Another conferee noted the distinction between the use of data mining to speed up traditional detection work and using it, as contemplated by the TIA program, to predict the future. It was argued that, out-

side of the existence of a conspiracy, the use of data-mining technologies to predict future behavior was inherently risky and had very different implications for privacy.

A Formal Process for Developing Privacy Standards

Was it possible to develop a process similar to the systematic process used by the medical community to authorize new drugs? It was suggested that such a process, designed to address privacy and public relations issues as technologies are developed, was likely to result in greater public acceptance of the technologies. Another participant agreed but noted the difficulty of asking technical people developing technology to also develop the policy that would guide the use of that technology, especially when it is not yet known what the technology can do. The group expressed a number of views on whether such procedures could be effective, but it was agreed that the question merited further consideration.

Legislative Answers

The issue of legislation in the area of privacy was then considered. General consensus was that it was inappropriate for legislation to discuss specific technologies. Rather, legislation should address general principles, such as whether and in what circumstances government agencies would be allowed access to personal information. It was argued that technology-specific legislation is a mistake, simply because technology changes so fast that it will bypass and invalidate the effect of even the most far-sighted legislation.

The challenge of educating Congress was also addressed. It was suggested that the recommendations of the 9/11 Commission and the reauthorization of the Patriot Act ensure that intelligence and privacy issues will be prominent in 2005. It was generally agreed that the best way to accomplish the necessary education was by working with members of Congress individually or in small groups. There was general agreement that outreach of some kind would be worthwhile and necessary.

Chapter Six:
Technology as a Tool to Protect Civil Liberties

Limits on Technology: A Historical Perspective

The Privacy Act of 1974 was passed in response to revelations about the collection of data on the political activities of American citizens by the military intelligence services, the excesses of Watergate, and the growing perception that the computer posed special threats to liberty. In passing the act, Congress sought to promote respect for the personal privacy of citizens in the collection, computerization and use of personal data; to prevent the creation of secret data banks containing information about citizens; to prevent illegal and overly broad investigation and surveillance of citizens; and to promote accountability, legislative oversight and open government in the use of computers.

To accomplish those objectives, Congress directed that: information about how a citizen exercises his or her First Amendment rights should not be collected or maintained without a strict review process; any information collected about citizens should be accurate, timely and relevant; interagency exchanges of personal data should be limited; data should be held securely and records kept of all disclosures and uses of personal data; agency personnel and contractors should be trained in accordance with Privacy Act requirements; and no new data banks or personal information systems should be created without the express authorization of Congress. The act has been modified, but its fundamental objectives remain unchanged.

The intrusion of the military into civilian affairs has been infrequent in U.S. history with, perhaps, the worst example occurring in the 1960s. During those years the army collected personal data on about 100,000 citizens in an effort to closely watch anti-Vietnam war demonstrations and protestors. Military agencies have been specifically precluded from domestic security activities since then, but recent changes in technology have afforded military intelligence the opportunity to return to those areas. Executive Order 12333 does not specifically prohibit the military from collecting information online and neither does the Privacy Act. The military can also collect and share personal information about citizens through its work with the Department of Homeland Security and the Terrorist Threat Integration Center.

Some expressed concern about military intelligence playing any role in homeland security beyond the support of military operations. The issue of whether the military can make a valuable contribution to domestic security agencies was raised and, with it, the question: What limits should be placed on those activities?

The use of new technology always brings the risk of unintended consequences. Data mining is no exception. It was observed that, even though the data mining technology under discussion is intended for defensive purposes, it can be used offensively. It will not be possible to keep the technology secret, so we must be prepared for the day when it could be used against us.

It will not be possible to keep the technology secret, so we must be prepared for the day when it could be used against us.

A Successful Strategy for Using Technology-based Surveillance

Technology-based surveillance systems do exist and are successfully managed. The large volume of information flowing through these systems requires the capability to sort, filter and distribute the data. At the same time, the data must also be certified and evaluated, at least at the preliminary level. These are significant challenges for both the technol-

ogy and the managers of the system.

Technical characteristics of a successful information management and surveillance system include:

- Automation. Everything that can be reliably done automatically should be done automatically. That includes audit trails, which can now be done automatically with a high degree of reliability.
- Audits. To the extent possible, auditing functions should be made part of the operations function. This would allow audits to be conducted regularly, without disrupting operations. There will be exceptions to this, but exceptions requiring human intervention should be documented in a way that clearly establishes lines of accountability.
- Access. Access to databases should be restricted to those who must have it in order to perform their analytical tasks. All rights of access should be frequently and automatically reviewed.

These characteristics should be written into the system before the system is built.

The human characteristics required for the successful information management and surveillance system include:

- Compliance with rules. A culture of compliance is essential to successful operation of a surveillance system. Acknowledgement of the importance of compliance must begin at the top and be fostered throughout the organization. The compliance function should be forced down through the levels of management, so that responsibility for compliance is dispersed to all levels of the organization. Compliance must become an aspect of daily operations and not be reserved to the oversight function.
- Training. Every function in the system is regulated, and to ensure compliance with regulatory procedures, training must be an integral part of operations. Such training should be rigorous, continuous and mandatory for all employees.
- Oversight. An essential function that should be separate from other operational functions. Oversight must be consistent and thorough, always with the understanding that too much oversight can create

undue caution and unacceptably slow decision making.

Architecture-A Place to Connect Policy and Technology

The starting point for analyzing the impact of technology on civil liberties is to recognize that technology is a tool and does not provide total security or privacy. Technology is a tool that is part of a technical system, which is itself a value-driven construction. The policy that establishes the technical system also establishes the values that will be used to manage that system. Technology is neutral, and because its use is value driven, the correct values, including privacy and respect for civil liberties, should be incorporated into the policy that guides the system at the onset.

TIA was offered as an example of the wrong way to develop policy and technology. It was argued that the termination of TIA was a serious setback for security and only a Pyrrhic victory for civil liberties. TIA was made up of seven programs. When terminated, six of those programs were classified, and the seventh, the privacy-protection program, was abandoned. This decision had two results, neither of which advanced the cause of protecting civil liberties. The first was that a public, visible program was ended along with an important opportunity to debate the subject. However, the technology development that was at the core of TIA was not terminated. It was moved into classified programs beyond the reach of public scrutiny. The second result was that the technology research being done under TIA was transferred from the Defense Advanced Research Projects Agency (DARPA), where the customers (i.e., government agencies) were in charge, to vendor companies trying to sell the same government agencies their product. That shift in the control of technology development may sell products, but it was argued that it would not provide the government with the right solutions, which are products that will promote security while protecting privacy.

TIA challenged the notion that privacy is protected by the government's inability to analyze available data efficiently. In the new environment, data is always available and the analysis and storage of data becomes less expensive every day. In the new economics of information technology, it is less expensive to retain data than it is to reduce and man-

age its volume through selective editing. The ability to search large databases now drives data management, and there is less emphasis on editing as a strategy to retain only the data that supports a given function.

The availability of all this data means that the privacy of any individual is vulnerable, so the question of selective attention by government agencies to an individual is more significant.

The availability of all this data means that the privacy of any individual is vulnerable, so the question of selective attention by government agencies to an individual is more significant. The policy guiding these choices must balance government and societal needs for information against an individual's need for privacy and freedom from surveillance. To have selective attention and still protect individual rights, it was argued that the policy must be supported by a technical system that includes due process protections. The technical features required for such systems include distributed architecture, rule-based processing, selective revelation and authentication and auditing capabilities.

The architecture is a framework based on policy and procedures that are designed to manage the technical system. The goal is a system that incorporates a distributed architecture based on web services that supports both privacy and the government's need to share information among its agencies.

Discussion then focused on the following issues:

Privacy and Policy-Together from the Beginning

Numerous views were expressed on the issue of when to integrate privacy principles into the development of technical systems. One participant argued that it was critical to include privacy considerations, along with security needs and compliance issues as fundamental system requirements, into the design of the system from the beginning. It was said that layering a privacy policy onto an already developed technical system was certain to leave gaps in privacy protection that were preventable. Another noted that government agencies were now in the

market for technical systems and that systems offered by vendors had little or no privacy protections built in. In these cases, the privacy policy will have to be added onto the technology after purchase, resulting in predictable gaps in privacy protection.

The question of whether existing policymaking structures were equipped to manage the development of privacy policy was raised. It was generally agreed that the judiciary was not a good choice (and would not want the responsibility in any case); the executive was not sufficiently trusted by people that were opposed to the use of the technology; and Congress was not particularly competent for the task and would be, in the best of circumstances, cumbersome to deal with. There was also agreement that, in the absence of a generally accepted method for making policy, government agencies would proceed on their own, most likely through the rule-making process, and that the results should be expected to be irregular and haphazard. But the policymaking process would be further complicated by security classification rules, which would prevent the transparent sharing of information, creating another reason for public skepticism.

Another conferee suggested that the problem was more difficult since there was no centralized project, such as TIA, around which a national debate could take place. Government agencies and departments would try to find a way to resolve the privacy-technology debate for themselves, but the larger issue of developing a framework to address these questions across all government agencies and departments would be an unreachable goal for the time being.

Errors and Exceptions

After acknowledging that technology guided by good policy could help protect civil liberties, a participant inquired how, if such a system were fully automated, the victims of misidentification and faulty inference would have an effective way of redressing such grievances. It was argued that a centralized process for redress, supervised by people with appropriate training, should be a part of such a system and general consensus was that any acceptable system would have to provide a process

for the correction of such errors quickly and effectively.

The question of when it would be appropriate to allow for exceptions was then raised. It was suggested that rules are rational and only apply to situations anticipated by them, but that exceptions are different because they arise from new and unanticipated circumstances. That being the case, it was argued that the search for a fully automated rules-based system is a search for the unattainable. Because a rules-based system is inherently incomplete, there would always be a need for human intervention to authorize exceptions to the rule.

The critical question then becomes who makes the decision granting an exception and what standards will be used. It was argued that, because impartiality is essential, the judiciary is the best place for this power to reside. Other participants acknowledged the need but suggested that, because such decisions would be frequent and would need to be made quickly, this was not the best place. It was suggested that a new type of judiciary, with real-time access and secure networks could be an answer to the need for rapid response. It was also suggested that an Office of Inspector General in an agency like the Department of Homeland Security could satisfy that need.

To represent victims of such mistakes, the creation of a new responsibility for the federal public defender system was also urged.

To represent victims of such mistakes, the creation of a new responsibility for the federal public defender system was also urged. A specialized group of attorneys, familiar with technology systems and having security clearances, could help victims redress their grievances and, at the same time, build public support for the technical systems.

How Much Transparency Is Enough?

It was acknowledged that the demise of TIA demonstrated that transparency of process is critical to winning public trust and support for these programs. Concerns were expressed about how much transparency was needed. It was suggested that it may be necessary to conceal some

of the databases searched/processes being used, at least in terrorism investigations, and it was questioned whether this would be tolerated by the public. It was also noted that, if too much information is revealed, people can counterprogram their data, or otherwise change their behavior to avoid detection. The issue raised was whether it makes sense to build a valid, predictive system for use against terrorists and then, by revealing the nature of the system to satisfy privacy advocates, give enough information to terrorists that would allow them to mask their behavior and thereby render the system less effective.

It was argued that announcing what databases would be investigated, or deciding that some databases would be off limits in advance, would undermine the successful use of the technology. To be effective, that pattern analysis must be able to scan large databases in search of unanticipated data anomalies, the location of which cannot be predicted. It was suggested that the government should not be dedicated to protecting personal secrecy but should focus on protecting anonymity for First Amendment rights and personal autonomy through the exercise of due process rights. But it was noted that the public thinks more categorically and would want assurances that certain types of information (e.g., medical or library records) are simply off limits. While this issue was acknowledged, it was generally agreed that designating particular data as being unusable or unavailable for particular investigations would seriously undermine any technical system.

It was suggested that the government should not be dedicated to protecting personal secrecy but should focus on protecting anonymity for First Amendment rights and personal autonomy through the exercise of due process rights.

Chapter Seven: Wrap and Discussion

Next Steps: Forging a Consensus

The issue of how best to build on conference discussions and develop momentum leading to consensus on these issues was then raised. The importance of reaching out to Congress was acknowledged, and it was noted that, because Congress responds to its constituents, broadening the discussion to reach a larger, nontechnical audience could stimulate public reaction and help move Congress to action.

The difficulty of resolving the question of the meaning of privacy in America was also acknowledged and it was suggested that, if notions of privacy are as dynamic as they seem to be currently, then systems built to protect privacy must be flexible and adaptable to these changing notions.

The difficulty of resolving the question of the meaning of privacy in America was also acknowledged and it was suggested that, if notions of privacy are as dynamic as they seem to be currently, then systems built to protect privacy must be flexible and adaptable to these changing notions. It was argued that the voluntary surrender of privacy in return for convenience was a case in point and, as such exchanges become more pervasive, the underlying concepts of privacy also evolve. It was noted that there may also be issues for people who choose not to make such exchanges, because they may be treated

differently and unfairly if they choose not to surrender their privacy.

Finally, it was observed that Americans are more comfortable sharing personal information with the private sector than with the government and, within the government, are more comfortable with some agencies than others. In this respect, American opinions are quite different and opposite the views expressed by Europeans. Europeans appear to be more comfortable exchanging personal information with their governments than with their private sector, especially if they think they are receiving enhanced personal security in return.

Starting Over: Context and Perspective

It was suggested that the context of these discussions should be reexamined. Once the context is agreed on, definitions and baseline assumptions become clearer and the role of individuals and organizations becomes more apparent. It was suggested that a new way of thinking about these issues is needed, a way of expanding the reach of our analysis to better match the constantly changing realities. It was noted that most people dealing with these issues have spent their careers learning to specialize, narrowing their focus to concentrate on an area of specialty. As specialists, people tend to rely on certain basic assumptions that have served them in the past, even though the changing world calls for regular reassessment of those assumptions.

It was suggested that a new way of thinking about these issues is needed, a way of expanding the reach of our analysis to better match the constantly changing realities.

It was suggested that technology will continue to change the way people live and alter their relationships with the rest of the world. These changes, in turn, demand that old assumptions be regularly challenged and that we be prepared for the possibility that the old assumptions may be invalid. Understanding that advances in technology come more quickly than advances in law or policy, it was argued that Americans must now look past old assumptions and methods to a new world of managing uncertainty, managing risk and manipulating systems with a goal

of anticipating future events such as terrorist attacks.

This changing environment requires a disciplined, forward-looking process designed to analyze information in a way that allows for the understanding of future uncertainties and management of risk. The process will be difficult to construct, because it will require thinking and analysis to be done in reverse, beginning from a point in the future to assess risks and uncertainties being faced now.

As a starting point, a management approach called scenario building was proposed for consideration. Scenario building is a method of analyzing complex problems in order to reach decisions about priorities and resource allocation. Elements of scenario building include:

- Identifying the decisions to be made.
- Challenging underlying assumptions to ensure their validity.
- Identifying key factors in the decision environment affecting the decision.
- Setting priorities by ranking the factors according to the importance of their uncertainties.
- Selecting the appropriate logical or analytical tool for the scenario being analyzed.
- Identifying probable implications.
- Recognizing that beliefs, hopes and fears influence behavior as much as numbers and facts.
- Assessing the probability of each scenario to allow decision makers to allocate limited resources more effectively.
- Identifying and selecting leading indicators to decide which, if any, of the scenarios is actually occurring.

Finally, it was suggested that policy must always encourage the continuing development of technology.

It was emphasized that this is only one method of analysis, but was argued that only through the use of such a system can targets of opportunity that may be available to terrorist adversaries be identified. It was further argued that better scenario analysis, including risk identification and assessment, will support decisions on where to allocate resources so as to have the best chance of

achieving critical objectives.

Finally, it was suggested that policy must always encourage the continuing development of technology. In the current environment and for the foreseeable future, it was argued that the best chance to deter terrorist attack is through the aggressive use of technology. Technology is neutral and only in its application do ethical dilemmas regarding the abuse of technology arise. It was argued that success in managing these technologies will only come through the development of a clear process and the discipline to follow it.

Technology is neutral and only in its application do ethical dilemmas regarding the abuse of technology arise.

Perceptions Matter

Decisions about how to address the terrorist challenge are pressing and critically important. The stakes are high and it was put forth that if a way is not found to address the problem constructively, decisions will be postponed and then, under the threat of a terrorist attack, expedient decisions will be made, after which much energy will be expended to correct those decisions.

It was argued that the response to this challenge is a matter of national survival, if only because of the threat attacks pose to the economy and our system of government. A free market economy relies on the confidence of those participating in it, and the threat of a dirty bomb, another anthrax attack or a cyber attack on financial or power systems could have a catastrophic impact. It was suggested that the world is too interconnected and nation states too dependent on each other for there to be any alternative to solving this problem.

The perception that the overall effort will do more to help security than it will harm civil liberties is crucial to success, and it was argued that a way must be found to shape the perception of the American public in support of that effort.

It was agreed that an open process, similar to processes employed by the medical system, offered an example that should be

seriously explored. In the interim the issue is how to build a consensus for the expanded use of advanced technology to penetrate terrorist cells in an environment of public suspicion. The perception that the overall effort will do more to help security than it will harm civil liberties is crucial to success, and it was argued that a way must be found to shape the perception of the American public in support of that effort.

Operating in the New Environment

The current environment has a number of characteristics that form the privacy versus technology debate in the war on terror:

- In the environment where the debate over privacy versus technology is taking place, the velocity of change is accelerating.
- There are more actors with more capabilities engaged in this environment, which means that strategic calculations are much more complex than before and the prospect of miscalculation by any of the actors is far greater.
- There is an interactive quality to developments that makes unambiguous solutions unlikely and this raises special challenges. In this rapidly changing landscape, change will be sudden and often move in unanticipated directions.
- It will be difficult for traditional analytic filters and disciplines to understand this world. For example, why should the definition of privacy be crafted solely by lawyers when it is clear that the definition is under constant pressure from other dynamics?

In the debate over data mining, it was argued that undue restrictions on searches would handicap the effectiveness of technology in important ways. While data mining does help to determine patterns of behavior that government agencies may wish to track, the patterns themselves do not provide the insights that can occur when analysts discover anomalies related to the patterns. These anomalies highlight unexpected behaviors that can lead to unique insights, and it is these insights that are put at risk when a search is too narrowly constrained.

It was suggested that U.S. terrorist adversaries would be inter-

ested in the conference discussion, particularly as it provided insight into opportunities to exploit American concerns about privacy. It was argued that terrorists will try to exploit our concerns about privacy and that, at some point government agencies should develop strategies to counter the efforts of those who do not share our values and seek to use them against us.

The final point concerned the implications of a legal regime that consistently lags behind the surge of new technology. Noting that the same technology is or will soon be available to terrorist adversaries, the question was raised whether the determination to protect privacy relegates the U.S. to a permanent and perhaps growing competitive disadvantage in the use of the most advanced technology. There was some agreement that the country is at risk of becoming competitively disadvantaged, and the more constraints we place on ourselves, the more rapidly that disadvantage will grow.

Basis for Citizen Resistance

Another conferee suggested that citizen resistance was rooted in the belief that America is a law-abiding society. It was argued that violating the law is uncommon and that the fear of exposure for embarrassing matters that do not rise to the level of law breaking is the real explanation for citizen resistance. Given that situation, it should be expected that active resistance to the idea that government should be given enhanced access to personal information will continue. On the other hand, it was noted that America is faced with a serious terrorist threat and that sacrifices should be expected, from citizens and the law enforcement community. To make progress on the enhanced use of technology issue, it was argued that law enforcement must be prepared to sacrifice its claim to use information collected and analyzed in terrorism investigations against citizens who are not terrorists, but who may have broken other laws. Unless law enforcement is willing to make this concession, it was contended that resistance to the employment of advanced technologies should be expected to continue.

It was also argued that the resistance of citizens to the enhanced

use of technology by government agencies was the result of repeated overreaching by the law enforcement community. Skepticism about government motives comes from many sources but that overreaching was a common thread. As an example, the Patriot Act was cited because it was passed as an antiterrorism measure but contained several provisions that expanded law enforcement powers in the domestic area. Similarly, the CAPS II program was cited because it was sold as a way to look for foreign terrorists, but its authority soon expanded to include persons who had committed ordinary domestic crimes. The participant argued that sacrifice was necessary to be successful in the war on terror, but that constitutional principles, including the principles of particular suspicion and probable cause, must remain paramount.

Skepticism about government motives comes from many sources but that overreaching was a common thread.

Building Public Support

It was put forth that the TIA program was terminated because, even though the public understood that this is a fight for survival, it did not understand how the technology would help win the battle. It was argued that a means of explaining the benefits of these technologies to the public was crucial to the success of any effort. There was agreement on that point, but concerns were raised about the slippery slope argument. This argument accepts that the first step to regulation or control, no matter how justified, inevitably leads to further steps that cannot be as easily justified. This argument is particularly compelling in the area of privacy because, while people may have difficulty digesting the technological issues, they are aware that any assurances against aggressive government behavior given when establishing such a system may be easily revoked, especially in times of crisis. It was argued that the critical first step would be the giving of real assurances that constraints put into any system to protect privacy will be preserved and second, that a method for preserving those constraints will be established.

There was general consensus that building public support would lead to Congressional support and that, even though the issue of pro-

viding binding assurances would be difficult, the need to generate public support required the effort. It was also suggested that, if real protections against abuse are built into technical systems at the front end, the decision to override such protections would be more apparent and therefore risky for the bureaucrat contemplating the decision. Increasing the consequences for government employees considering the violation of public assurances, it was argued, makes the decision to go down the slippery slope more difficult and may be, in the end, the best deterrent to agency abuse that the political system can offer.

The politicization of the war on terror and the counterterrorism effort, in general, have been very destructive, and Congress has a role to play in developing these initiatives. It was suggested that Congress has a constructive role to play in stimulating the national debate and the encouragement of policies that would protect security and privacy in mutually reinforcing ways. It was agreed that Congress should not be the rule-making authority on these initiatives, but it was argued that it can do its part by creating institutions inside the executive branch and requiring those institutions to conduct their operations transparently, which will encourage public confidence.

The politicization of the war on terror and the counterterrorism effort, in general, have been very destructive, and Congress has a role to play in developing these initiatives.

Strategies for Going Forward-Issues and Ideas

Any strategy for going forward must focus on both the need for effective communications and the substance of what is to be communicated. Substantively, it was argued that public support would be available for a program containing the following elements:

- Clear legal limits on the uses of data mining and related technologies.
- Clear and understandable oversight mechanisms.
- An open process allowing for the participation of interest groups.
- Mechanisms for the redress of grievances by those who may have

been adversely affected by the application of the technology.

It was also suggested that the following elements would be critical to an effective communications strategy:

- Positive explanations of technological proposals to the public and the press.
- Restraint in public statements (i.e., using care in communications and restraining the urge to over promise).

Another participant agreed with the notion of educating the press. It was observed that journalists routinely reach large audiences and that, while favorable coverage is good, unfavorable coverage can be fatal to a program. It was also suggested that members of the press should be educated about the subject matter and cultivated, because it may be necessary to contact them to respond to inaccurate stories or supplement coverage. It was particularly noted that care should be taken in presenting information to the press to ensure more accurate and effective coverage. Finally, it was suggested that maintaining credibility with the press is crucial because, without credibility, no useful relationship can continue.

It was particularly noted that care should be taken in presenting information to the press to ensure more accurate and effective coverage.

It was also said that success will require more than better public relations skills. When it comes to data mining and other technologies, there is real resistance among citizens to the principle of government having the power to conduct such operations, and it may be better to advocate a narrower use of technology, which is an incremental advance beyond what is being done now. It was suggested that incremental advances are preferable to the current situation, in which government agencies are not taking advantage of technological efficiencies because of the concern that their actions would be misperceived as broad, intrusive use of technology.

The current environment is not receptive to the enhanced use of

technology, but another terrorist attack would not only do serious damage to the economy but would result in calls for action against groups and individuals that would make the concerns being expressed about civil liberties seem almost trivial. It was also suggested that the enhanced use of technology, and particularly pattern recognition derived from data mining, is an effective way of focusing law enforcement resources that would otherwise be inadequate to the terrorist challenge. One participant reluctantly concluded that, because of the complexity of the issues and the difficulty of communicating the issues to the public, the Presidential Commission model would be the most appropriate way to address the problem.

It was suggested that incremental advances are preferable to the current situation, in which government agencies are not taking advantage of technological efficiencies because of the concern that their actions would be misperceived as broad, intrusive use of technology.

Other views were offered, including a proposal to create an independent agency, outside of law enforcement, with the authority to search any database in the world using any method available to identify terrorists, but with the understanding that absolutely none of the information obtained would be used to identify individuals. At a certain point, most likely when enough information is accumulated to make a case for probable cause, further steps could be taken only with a court order.

It was argued that there is an urgent need for citizens to unite in the recognition that the Constitution is designed to protect civil liberties and national security and that the time for a leisurely debate of these issues may have passed.

A conferee agreed that the next steps should begin with the Constitution and not just Fourth Amendment protections of civil liberties but also the Article IV, Section 4 requirement that the federal government protect the nation against invasion. It was suggested that the country is not engaged in a law enforcement exercise but a national security challenge. It was argued that there is an urgent need for citizens to unite in the recognition that the Constitution is designed to protect civil lib-

erties and national security and that the time for a leisurely debate of these issues may have passed.

Appendix A: Conference Participants

Kenneth Bass
Sterne, Kessler, Goldstein & Fox

M.E. (Spike) Bowman
Senior Counsel, National Security Law
Federal Bureau of Investigation (FBI)

Joel Brenner
Inspector General
National Security Agency

Ted Bridis
Staff Writer
The Associated Press

Valerie Caproni
General Counsel
Federal Bureau of Investigation (FBI)

Fred H. Cate
Distinguished Professor and Director
Indiana University Center for Applied Cybersecurity Research

Robert D. Caudle
Associate General Counsel
Office of General Counsel
Central Intelligence Agency (CIA)

Angeline Chen
George Mason University Law School
International Launch Services

Michael Chertoff
Circuit Judge
United States Court of Appeals, Third Circuit

Thomas J. Connelly
Associate General Counsel
Information Analysis and Infrastructure Protection (IAIP)
US Department of Homeland Security

Jeffrey R. Cooper
Corporate Vice President for Technology
and Chief Scientist, SAIC Strategies
Science Applications International Corporation (SAIC)

Willie Curtis
Professor of International Politics
Department of Political Science
US Naval Academy

Stephen Dycus
Professor
Vermont Law School

Lara M. Flint
Staff Counsel
Center for Democracy and Technology

Richard E. Friedman
President/Chair
National Strategy Forum

Frank M. Gren
Managing Director
Galway Partners

John J. Hamre
President and CEO
Center for Strategic and International Studies (CSIS)

Michael A. Jacobs
Senior Vice President and General Counsel
LexisNexis

John R. Livingston, Jr.
Counsel
US Senate Select Committee on Intelligence

Heather MacDonald
John M. Olin Fellow for Policy Research
Manhattan Institute

Kate Martin
Executive Director
Center for National Security Studies

John Michael McConnell
Vice President
Booz Allen Hamilton

Holly McMahon
Staff Director
ABA Standing Committee on Law and National Security

Judith A. Miller
Williams & Connolly LLP

Newton Minow
Senior Counsel
Sidley Austin Brown & Wood LLP

Kevin M. O'Connell
Director of Intelligence Policy Center
National Security Research Division
RAND Corporation

Joseph Onek
Senior Counsel and Director
Liberty and Security Initiative
The Constitution Project

George A. B. Peirce
General Counsel
Defense Intelligence Agency

John M. Poindexter
JMP Consulting

Vito T. Potenza
Deputy General Counsel
National Security Agency

Jill D. Rhodes
Senior Advisor
SRA International, Inc.

Paul Rosenzweig
Senior Legal Research Fellow
The Heritage Foundation

David Schanzer
Minority Staff Director
Select Committee on Homeland Security

Stephen E. Schmidt
Chief Technology Officer
Office of the Director
Federal Bureau of Investigation (FBI)

Walter Gary Sharp, Sr.
Director of Legal Research for International, Comparative and Foreign Law
The Law Library of Congress

Suzanne Spaulding
Minority Staff Director
House Permanent Select Committee on Intelligence
Chair, ABA Standing Committee on Law and National Security

Barry Steinhardt
Director, Technology and liberty Program
American Civil Liberties Union (ACLU)

Kim Taipale
Executive Director
Center for Advanced Studies in Science and Technology Policy

Stuart S. Taylor, Jr.
Opinion Columnist
National Journal

Michael Vatis
Independent Consultant and Attorney

Eugene Volokh
Professor of Law
University of California at Los Angeles School of Law

S. Enders Wimbush
Director
Center for Future Security Strategies
Hudson Institute

Elizabeth Withnell
Counsel for FOIA and Privacy
US Department of Homeland Security, Privacy Office

Appendix B: Bibliography: List of the Conference Read-Ahead Materials

Block, Robert and Gary Fields. "Is Military Creeping Into Domestic Spying And Enforcement?" *The Wall Street Journal* (March 9, 2004): Page B1.

Bowman, M. E. "The Legacy of the Church Committee." *Intelligencer* V. 14, no. 1 (Winter/Spring 2004): Pages 27-34.

MacDonald, Heather. "Common Sense and Computer Analysis." *The Washington Post* (May 31, 2004): Page A23.

MacDonald, Heather. "What We Don't Know Can Hurt Us." City Journal V. 14, no. 2 (Spring 2004): http://www.city-journal.org/html/14_2_what_we_dont_know.html.

Minow, Newton. "Seven Clicks Away." *The Wall Street Journal* (June 3, 2004): Page A14.

"New Documents Obtained by ACLU Raise Troubling Questions About Matrix Program." ACLU Issue Brief #2 (May 20, 2004): http://www.aclu.org/Files/OpenFile.cfm?id=14253.

Report to Congress regarding the Terrorism Information Awareness Program, Executive Summary. *Defense Advanced Research Projects Agency (DARPA)* (May 20, 2003): http://www.globalsecurity.org/security/library/report/2003/tia-exec-summ_20may2003.pdf.

Rhodes, Jill D. "CAPPS II: Red Light, Green Light, or "Mother May I?" *Journal of Homeland Security* (March 2004): http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=107.

Singel, Ryan. "Data Scant for Watchlist Usage." *Wired Magazine* (May 17, 2004): http://www.wired.com/news/privacy/0,1848,63478,00.html.

Stanley, Jay and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." American Civil Liberties Union Technology and Liberty Program (January 2003): http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39#FileAttach.

Taipale, K.A.. "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data." Center for Advanced Studies in Science and Technology Policy. *Columbia Science & Technology Law Review* V.5, Issue 2 (December 2003): www.taipale.org/papers/DMDS-ExecSum.pdf.

"The Dawn of Micro Monitoring: Its Promise, And Its Challenges To Privacy And Security." *Remarks of Senator Patrick Leahy*. Conference On "Video Surveillance: Legal and Technological Challenges," Georgetown University Law Center, Washington, D.C. (March 23, 2004): http://leahy.senate.gov/press/200403/032304.html.

Zetter, Kim. "Getting Naked for Big Brother." *Wired Magazine* (May 17, 2004): http://www.wired.com/news/privacy/0,1848,63450,00.html?tw=wn_story_related