Safeguarding Privacy in the Fight Against Terrorism

Report of the Technology and Privacy Advisory Committee

March 2004

SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM

The Report of the Technology and Privacy Advisory Committee

MARCH 2004

DEPARTMENT OF DEFENSE
TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE
3330 Defense Pentagon, Room 3E1045
Washington, DC 20301-3330

March 1, 2004

The Hon. Donald H. Rumsfeld
Secretary of Defense
Department of Defense
1000 Defense Pentagon 3E880
Washington, DC 20301-1000

Dear Secretary Rumsfeld:

In February 2003, you appointed the Technology and Privacy Advisory Committee to examine the Terrorism Information Awareness program and to develop safeguards "to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy." We are pleased to provide you with our final report.

TIA was only one of the programs within DOD and elsewhere in the government involved, or with the potential for being involved, in data mining concerning U.S. persons. The committee believes that data mining plays a critical role in the fight against terrorism, but that it should be used—and can be effectively—only in ways that do not compromise the privacy of U.S. persons. That is the goal of our recommendations. We believe our recommendations both protect privacy and facilitate the appropriate, effective, and efficient use of data mining tools to fight terrorism.

While we have focused on DOD, we do not believe that all of the necessary safeguards are within the power of the Secretary of Defense. Some of our recommendations therefore encourage you to recommend to the President and Congress actions we believe are necessary to ensure meaningful privacy protection not only in DOD, but throughout the government. These recommendations are designed to create a consistent, government-wide standard to facilitate the sharing of information among agencies that is critical to fighting terrorism.

The committee's deliberations have been substantive, wide-ranging, and collegial. The committee is unanimous in most of its recommendations. A separate statement from William T. Coleman, Jr., reflecting his opposition to some of the committee's conclusions, is appended to our report. A separate statement from Floyd Abrams, which highlights why the committee disagrees with many of the views expressed in Mr. Coleman's statement, is also appended. Those statements and the seriousness of our discussions reflect the importance and difficulty of these issues.

The committee's work was greatly aided by the testimony of 60 witnesses from DOD, other government agencies, private industry, academia, and advocacy groups, and by extensive briefings for individual committee members and staff from many other individuals. These people are acknowledged individually in our report, but we wish to take this opportunity to thank them once again for their dedicated and selfless public service. Finally, I express my gratitude for the commitment, cooperation, and tireless work of the committee members; Lisa Davis, the committee's Executive Director and Designated Federal Official; and Professor Fred H. Cate, the committee's Reporter.

Yours sincerely,

Newton N. Minow

Newton N. Minow
Chairman

Technology and Privacy Advisory Committee

Newton N. Minow
Chairman

Floyd Abrams
Zoë Baird
Griffin Bell
Gerhard Casper
William T. Coleman, Jr.
Lloyd N. Cutler
John O. Marsh, Jr.

Lisa A. Davis
Executive Director and Designated Federal Official

Fred H. Cate
Reporter

CONTENTS

EXECUTIVE SUMMARY

TAPAC'S CREATION AND CHARGE

The United States faces, in the words of British Prime Minister Tony Blair, "a new and deadly virus."[1] That virus is "terrorism, whose intent to inflict destruction is unconstrained by human feeling and whose capacity to inflict it is enlarged by technology."[2]

As the murderous attacks of September 11 painfully demonstrated, this new threat is unlike anything the nation has faced before. The combination of coordinated, well-financed terrorists, willing to sacrifice their lives, potentially armed with weapons of mass destruction, capable of operating within our own borders poses extraordinary risks to our security, as well as to our constitutional freedoms, which could all too easily be compromised in the fight against this new and deadly terrorist threat.

To help guard against this, Secretary of Defense Donald Rumsfeld appointed the Technology and Privacy Advisory Committee ("TAPAC") in February 2003 to examine the use of "advanced information technologies to identify terrorists before they act."[3] Secretary Rumsfeld charged the committee with developing safeguards "to ensure that the application of this or any like technology developed within [the Department of Defense] DOD is carried out in accordance with U.S. law and American values related to privacy."[4*]

The decision to create TAPAC was prompted by the escalating debate over the Terrorism Information Awareness ("TIA") program.† TIA had been created by the Defense Advanced Research Projects Agency ("DARPA") in 2002 as a tool to "become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options."[5]

TIA sparked controversy in Congress and the press, due in large part to the threat it was perceived as posing to informational privacy. On September 25, 2003, Congress terminated funding for the program with the exception of "processing, analysis, and collaboration tools for counterterrorism foreign intelligence," specified in a classified annex to the Act. These tools may be used only in connection with "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or

* U.S. laws apply to surveillance, searches, and seizures of personally identifiable information conducted or authorized by government officials within the United States. Those laws apply outside of the United States only if the surveillance, search, or seizure involves a U.S. citizen (although not necessarily a permanent resident alien).

This report focuses exclusively on the privacy issues posed by U.S. government data mining programs under U.S. law to U.S. persons, which are defined under U.S. law as U.S. citizens and permanent resident aliens. It does not address data mining concerning federal government employees in connection with their employment.

† When first announced, the program was entitled "Total Information Awareness." The title was changed to "Terrorism Information Awareness" in May 2003.

wholly against non-United States citizens."[6] This language makes clear that TIA-like activities may be continuing.

The Scope of government Data Mining

TIA was not unique in its potential for data mining.* TAPAC is aware of many other programs in use or under development both within DOD and elsewhere in the government that make similar uses of personal information concerning U.S. persons to detect and deter terrorist activities, including:

- DOD programs to determine whether data mining can be used to identify individuals who pose a threat to U.S. forces abroad
- the intelligence community's Advanced Research and Development Activity center, based in the National Security Agency, to conduct "advanced research and development related to extracting intelligence from, and providing security for, information transmitted or manipulated by electronic means"[7]
- the Computer-Assisted Passenger Prescreening System in the Department of Homeland Security ("DHS")
- the Treasury Department's Financial Crimes Enforcement Network
- federally mandated "Know Your Customer" rules
- the "MATRIX" (Multistate Anti-Terrorism Information Exchange) system to link law enforcement records with other government and private-sector databases in eight states and DHS
- Congress' mandate in the Homeland Security Act that DHS "establish and utilize . . . a secure communications and information technology infrastructure, including data mining and other advanced analytical tools," to "access, receive, and analyze data detect and identify threats of terrorism against the United States"[8]

TAPAC'S CONCLUSIONS

After many public hearings, numerous background briefings, and extensive research, TAPAC has reached four broad conclusions:

TIA was a flawed effort to achieve worthwhile ends. It was flawed by its perceived insensitivity to critical privacy issues, the manner in which it was presented to the public, and the lack of clarity and consistency with which it was described. DARPA stumbled badly in its handling of TIA, for which the agency has paid a significant price in terms of its credibility in Congress and with the public. This comes at a time when DARPA's historically creative and ambitious research capacity is more necessary than ever. By maintaining its focus on imaginative, far-sighted research, at the same time that it takes account of informational privacy concerns, DARPA should rapidly regain its bearings. It is in the best interests of the nation for it to do so.

Data mining is a vital tool in the fight against terrorism, but when used in connection with personal data concerning U.S. persons, data mining can present significant privacy issues. Data mining tools, like most technologies, are inherently neutral: they can be used for good or ill. However, when those tools are used by the government to scrutinize personally identifiable data concerning U.S. persons who have done nothing to warrant suspicion, if they are conducted without an adequate predicate they run the risk of becoming the 21st-century equivalent of general searches, which the authors of the Bill of Rights were so concerned to protect against.

To be certain, data mining has many valuable and lawful uses in both the private and public sectors. In many settings it may prove less intrusive to privacy than other techniques for guarding against terrorist threats. Moreover, the same technologies that make data mining feasible can be used to reduce the amount of personally identifiable data necessary, facilitate data mining

* We define "data mining" to mean: searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

Clear, uniform laws and standards governing data mining are necessary to empower DOD and other government agencies to use data mining tools effectively and aggressively in the fight against terrorism.

with anonymized data, and create immutable audit trails and other protections against misuse.

However, when data mining involves the government accessing personally identifiable information about U.S. persons, it also raises privacy issues. The magnitude of those issues varies depending upon many factors, including: the sensitivity of the data being mined, the expectation of privacy reasonably associated with the data, the consequences of an individual being identified by an inquiry, and the number (or percentage) of U.S. persons identified in response to an inquiry who have not otherwise done anything to warrant government suspicion.

In developing and using data mining tools the government can and must protect privacy. This has never been more starkly presented than following the September 11 terrorist attacks, which vividly demonstrated the need to deploy the tools necessary to protect and defend the nation without violating our constitutional values in the process.

Striking a balance between security and privacy is no easy task. Alexander Hamilton wrote in Federalist Paper 8 in 1787 that "[s]afety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates." "To be more safe," he concluded, nations "at length become willing to run the risk of being less free."[9] The Supreme Court wrote in 1963 that it is "under the pressing exigencies of crisis, that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action."[10]

This is precisely the challenge our nation faces today, a challenge made immediate and critical by the magnitude of the terrorist threat, its sustained nature, and the fact that it comes not from an identified enemy abroad but from a largely invisible enemy that may be operating within our borders.

Existing legal requirements applicable to the government's many data mining programs are numerous, but disjointed and often outdated, and as a result may compromise the protection of privacy, public confidence, and the nation's ability to craft effective and lawful responses to terrorism. This is especially true in the setting on which TAPAC focused—analyzing personally identifiable data to protect against terrorist threats.

The legal protections that have historically applied in this context recognize distinctions between U.S. persons and non-U.S. persons, between law enforcement and national security, and between activities that take place in the United States as opposed to those that take place beyond our borders. This "line at the border" approach to privacy law and to national security is now increasingly inadequate because of the new threat from terrorists who may be operating within our borders, and advances in digital technologies, including the Internet, that have exponentially increased the volume of data available about individuals and greatly reduced the financial and other obstacles to retaining, sharing, and transferring those data across borders. These developments highlight the need for new regulatory boundaries to help protect civil liberties and national security at the same time. It is time to update the law to respond to new challenges.

The stakes could not be higher. Clear, uniform laws and standards governing data mining are necessary to empower DOD and other government agencies to use data mining tools effectively and aggressively in the fight against terrorism. Those laws and standards are also necessary to protect informational privacy, which is both important in its own right and is often critical to a range of fundamental civil liberties, including our rights to speak, protest, associate, worship, and participate in the political process free from government intrusion or intimidation.

Recommendations Concerning DOD Data Mining

We believe it is possible to use information technologies to protect national security without compromising the privacy of U.S. persons. The answer lies in clear rules and policy guidance, adopted through an open and credible political process, supplemented with educational and technological tools, developed as an integral part of the technologies that threaten privacy, and enforced through appropriate managerial, political, and judicial oversight.

Recommendation 1

DOD should safeguard the privacy of U.S. persons when using data mining to fight terrorism.

Recommendation 2

The Secretary should establish a regulatory framework applicable to all data mining conducted by, or under the authority of, DOD, known or reasonably likely to involve personally identifiable information concerning U.S. persons.

The essential elements of that framework include a written finding by agency heads authorizing data mining; minimum technical requirements for data mining systems (including data minimization, data anonymization, creation of an audit trail, security and access controls, and training for personnel involved in data mining); special protections for data mining involving databases from other government agencies or from private industry; authorization from the Foreign Intelligence Surveillance Court before engaging in data mining with personally identifiable information concerning U.S. persons or reidentifying previously anonymized information concerning U.S. persons; and regular audits to ensure compliance.

We recommend *excluding* from these requirements data mining that is limited to foreign intelligence that does not involve U.S. persons; data mining concerning federal government employees in connection with their employment; and data mining that is based on particularized suspicion, including searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship passenger manifests or other lists of names or other nonsensitive information about U.S. persons.

In addition, we recommend that data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be subject to only the requirements that it be conducted pursuant to the written authorization of the agency head (as specified in Recommendation 2.1) and auditing for compliance (as specified in Recommendation 2.5).

Recommendation 3

DOD should, to the extent permitted by law, support research into means for improving the accuracy and effectiveness of data mining systems and technologies, technological and other tools for enhancing privacy protection, and the broader legal, ethical, social, and practical issues in connection with data mining concerning U.S. persons.

Recommendation 4

The Secretary should create a policy-level privacy officer.

Recommendation 5

The Secretary should create a panel of external advisors to advise the Secretary, the privacy officer, and other DOD officials on identifying and resolving informational privacy issues, and on the development and implementation of appropriate privacy protection mechanisms.

Recommendation 6

The Secretary should create and ensure the effective operation of meaningful oversight mechanisms.

Recommendation 7

The Secretary should work to ensure a culture of sensitivity to, and knowledge about, privacy issues involving U.S. persons throughout DOD and all of its research, acquisition, and operational activities.

Recommendations Concerning Government Data Mining

While TAPAC focused on TIA and related DARPA programs, it is counterproductive to the protection of both privacy and national security to address only these, while ignoring the many other government programs that use personal information on U.S. persons. Moreover, the privacy issues presented by data mining cannot be resolved by DOD alone. Action by Congress, the President, and the courts is necessary as well. Finally, because DOD is the only federal department to have an external advisory committee to examine the privacy implications of its programs, TAPAC occupies a unique position. We therefore direct our recommendations to the broad range of government data mining activities.

Recommendation 8

The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities. A government-wide approach is desirable to address the significant privacy issues raised by the many programs under development, or already in operation, that involve the use of personally identifiable information concerning U.S. persons for national security and law enforcement purposes.

We therefore believe that the provisions of Recommendation 2, which concern DOD's programs that involve data mining, should also be implemented across the federal government and made applicable to all government departments and agencies that develop, acquire, or use data mining tools in connection with U.S. persons for national security or law enforcement purposes.

We do not suggest that the resolution of informational privacy issues will be the same in every setting. Clearly, some modifications will be necessary. We believe, however, that government efforts to protect national security and fight crime and to protect privacy will be enhanced by the articulation of government-wide principles and a consistent system of laws and processes. National standards will also help provide clear models for state and local government efforts as well.

Recommendation 9

The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

Recommendation 10

The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

[These recommendations] . . . are designed to help break down the barriers to information-sharing among agencies that have previously hampered national security efforts, to provide sufficient clarity concerning access to and use of personal information . . . appropriately, and to ensure that scarce national security resources are deployed strategically and effectively.

Recommendation 11

The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process. This includes adopting new, consistent protections, along the lines of these recommendations, for information privacy in the law enforcement and national security contexts. In addition, we believe Congress and the President should work together to enact the legislation necessary to authorize the Foreign Intelligence Surveillance Court to receive requests for orders under Recommendations 2 and 8 and to grant or deny such orders.

There is also a critical need for Congress to exercise appropriate oversight, especially given the fact that many data mining programs may involve classified information which would prevent immediate public disclosure. We believe that each house of Congress should identify a single committee to exercise oversight of data mining activities, and that each agency's privacy officer and agency head should report jointly to those committees at least annually.

Recommendation 12

The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons.

Conclusion

Our goal in these recommendations is to articulate a framework of law and technology to enable the government simultaneously to combat terrorism and safeguard privacy. We believe rapid action is necessary to address the host of government programs that involve data mining concerning U.S. persons and to provide clear direction to the people responsible for developing, procuring, implementing, and overseeing those programs.

While these recommendations impose additional burdens on government officials before they employ some data mining tools, we believe that in the long-run they will enhance not only informational privacy, but national security as well. They are designed to help break down the barriers to information-sharing among agencies that have previously hampered national security efforts, to provide sufficient clarity concerning access to and use of personal information concerning U.S. persons so that DOD and other government officials can use such information appropriately, and to ensure that scarce national security resources are deployed strategically and effectively.

This broader, more comprehensive approach is essential if our nation is to achieve its goal of combating terrorism *and* safeguarding the privacy of U.S. persons. We must not sacrifice liberty for security, because as Benjamin Franklin warned more than two centuries ago, "they that can give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety."[11] Franklin might well have added that those who trade liberty for safety all too often achieve neither.

Summary of TAPAC Recommendations

Recommendations Concerning DOD Data Mining

RECOMMENDATION 1

DOD should safeguard the privacy of U.S. persons when using data mining to fight terrorism. "Data mining" is defined to mean: searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

RECOMMENDATION 2

The Secretary should establish a regulatory framework applicable to all data mining conducted by, or under the authority of, DOD, known or reasonably likely to involve personally identifiable information concerning U.S. persons. The requirements of this section apply to all DOD programs involving data mining concerning U.S. persons, with three exceptions: data mining (1) based on particularized suspicion, including searches of passenger manifests and similar lists; (2) that is limited to foreign intelligence that does not involve U.S. persons; or (3) that concerns federal government employees in connection with their employment. Data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be conditioned only on the written authorization described in Recommendation 2.1 and the compliance audits described in Recommendation 2.5. All other data mining concerning U.S. persons should comply with all of the following requirements:

RECOMMENDATION 2.1

Written finding by agency head authorizing data mining. Before an agency can employ data mining known or reasonably likely to involve data concerning U.S. persons, the agency head should first make a written finding that complies with the requirements of this recommendation authorizing the data mining.

An agency head may make the written finding described above either for programs that include data mining as one element, and data mining concerning U.S. persons may occur, or for specific applications of data mining where the use of information known or likely to concern U.S. persons is clearly anticipated.

RECOMMENDATION 2.2

Technical requirements for data mining. Data mining of databases known or reasonably likely to include personally identifiable information about U.S. persons should employ or be subject to the requirements of this recommendation (i.e., data minimization, data anonymization, audit trail, security and access, and training).

RECOMMENDATION 2.3

Third-party databases. Data mining involving databases from other government agencies or from private industry may present special risks. Such data mining involving, or reasonably likely to involve, U.S. persons, should adhere to the principles set forth in this recommendation.

RECOMMENDATION 2.4

Personally identifiable information. It is not always possible to engage in data mining using anonymized data. Moreover, even searches involving anonymized data will ultimately result in matches which must be reidentified using personally identifiable information. The use of personally identifiable information known or reasonably likely to concern U.S. persons in data mining should adhere to the following provisions:

An agency within DOD may engage in data mining using personally identifiable information known or reasonably likely to concern U.S. persons on the condition that, prior to the commencement of the search, DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the search based on the existence of specific and articulable facts that meet the requirements of this recommendation.

DOD may seek the approval from the Foreign Intelligence Surveillance Court either for programs that include data mining as one element, and data mining of personally identifiable information known or likely to include information on U.S. persons may arise, or for specific applications of data mining where the use of personally identifiable information known or likely to include information on U.S. persons is clearly anticipated.

An agency may reidentify previously anonymized data known or reasonably likely to concern a U.S. person on the condition that DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the reidentification based on the existence of specific and articulable facts that meet the requirements of this recommendation.

Without obtaining a court order, the government may, in exigent circumstances, search personally identifiable information or reidentify anonymized information obtained through data mining if it meets the requirements of this recommendation.

RECOMMENDATION 2.5
Auditing for compliance. Any program or activity that involves data mining known or reasonably likely to include personally identifiable information about U.S. persons should be audited not less than annually to ensure compliance with the provisions of this recommendation and other applicable laws and regulations.

RECOMMENDATION 3
DOD should, to the extent permitted by law, support research into means for improving the accuracy and effectiveness of data mining systems and technologies, technological and other tools for enhancing privacy protection, and the broader legal, ethical, social, and practical issues in connection with data mining concerning U.S. persons.

RECOMMENDATION 4
The Secretary should create a policy-level privacy officer.

RECOMMENDATION 5
The Secretary should create a panel of external advisors to advise the Secretary, the privacy officer, and other DOD officials on identifying and resolving informational privacy issues, and on the development and implementation of appropriate privacy protection mechanisms.

RECOMMENDATION 6
The Secretary should create and ensure the effective operation of meaningful oversight mechanisms.

RECOMMENDATION 7
The Secretary should work to develop a culture of sensitivity to, and knowledge about, privacy issues involving U.S. persons throughout DOD's research, acquisition, and operational activities.

Recommendations Concerning Government Data Mining

RECOMMENDATION 8
The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities.

RECOMMENDATION 9
The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

RECOMMENDATION 10
The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

RECOMMENDATION 11
The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process. Specifically, Congress and the President should authorize the Foreign Intelligence Surveillance Court to receive requests for orders under Recommendations 2.4 and 8 and to grant or deny such orders, and each house of Congress should identify a single committee to receive all of the agencies' reports concerning data mining.

RECOMMENDATION 12
The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons.

ACKNOWLEDGMENTS

TAPAC acknowledges the responsiveness and dedication of the many DOD officials who have appeared before the committee and provided background information for individual members of TAPAC and its staff on both substantive and procedural matters. These people include: the Hon. E.C. Aldridge; the Hon. Michael W. Wynne; the Hon. Paul McHale; the Hon. William J. Haynes II; George B. Lotz, II; Sue Payton; Dr. Thomas H. Killion; Carol Haave; Dr. Anthony J. Tether; Lieutenant General Keith B. Alexander; Major General Paul D. Nielsen; Dr. Robert Popp; Robert L. Deitz; Brigadier General George R. Fay; Vito Potenza; Captain David C. Taylor; Vahan Moushegian; Stewart Aly; Jeff Green; Jim Smyser; and Lieutenant Colonel Ronald K. Miller.

We benefited significantly from presentations by officials from government agencies outside of DOD. We acknowledge the willingness of these public servants to advise us, even though our mandate did not include their agencies. They include: Maureen Baginski (Federal Bureau of Investigation); John Brennan (Terrorist Threat Integration Center); Nuala O'Connor Kelly and Steve Thayer (Department of Homeland Security); Michael R. Ramage (Florida Department of Law Enforcement); and Allan Wade (Central Intelligence Agency).

We appreciate the guidance and support of the Hon. Senator Ron Wyden (D-Ore.), the Hon. Representative Jerrold Nadler (D-N.Y.), and the Hon. Governor James S. Gilmore, III, who graciously appeared before the committee, and of the Hon. Senator Pat Roberts (R-Kan.), who hosted the committee's Capitol Hill hearings.

TAPAC gratefully acknowledges the contributions of all of the experts who have appeared before it. Their willingness to share their expertise and experience is in the finest tradition of public service. They include: Stewart Baker; Jennifer Barrett; Jerry Berman; Scott Charney; Gary Clayton; William Crowell; Michael de Janes; Jim Dempsey; Viet Dinh; Dr. Usama Fayyad; Dr. Edward W. Felten; Dan Gallington; Jamie Gorelick; Dr. David Jensen; Jeff Jonas; Dr. Takeo Kanade; Teresa Lunt; Judith Miller; Dr. Gregory Piatetsky-Shapiro; Thomas M. Regan; Martha Rogers; Paul Rosenzweig; Dr. Nils R. Sandell, Jr.; Brian Sharkey; Jeffrey Smith; David Sobel; James B. Steinberg; Dr. Latanya Sweeney; Jay Stanley; Michael Vatis; and Lee M. Zeichner. Appendix B contains a complete listing of witnesses and their affiliations.

TAPAC has benefited from the behind-the-scenes assistance of many individuals and organizations who have provided information and insights to committee members and staff. These include: David Apatoff; Jerry Berman; the Brookings Institution; the Center for Democracy and Technology; the Century Fund; Ernie Cooper; Jim Dempsey; David Dickinson; Lisa Gagnon; Philip Heymann; Craig L. LaMay; Martha Minow; Mary Minow; Nell Minow; the Markle Foundation Task Force on National Security in the Information Age; Kate Martin; R. Eden Martin; Patrice McDermott; Joseph Onek; Paul Rosenzweig; Paul Schwartz; David Sobel; Dan Strunk; Peter Swire; K.A. Taipale; Howard Trienens; Michael Vatis; Brian Weiss; and Lee M. Zeichner.

The day-to-day work of TAPAC has been managed by Lisa A. Davis, Executive Director and Designated Federal Official for TAPAC. Her professionalism and skill have been invaluable. We gratefully acknowledge her dedicated assistance and that of her staff.

Fred H. Cate, Distinguished Professor and Director of the Center for Applied Cybersecurity Research at Indiana University, assisted the committee in its deliberations and in the drafting of this report. We are grateful for the extensive knowledge and exceptional commitment he brought to these tasks.

Introduction

TAPAC's Creation and Charge

In early 2002, the Defense Advanced Research Projects Agency ("DARPA") announced that it was developing advanced information technologies which could access personally identifiable information in the fight against terrorism. The project—called "Terrorism Information Awareness" ("TIA")*—responded to the terrorist attacks of September 11, 2001, and the demonstrated need for technological tools to make better use of existing data to identify and stop terrorist threats. TIA soon prompted serious public and Congressional criticism. This criticism centered on the possible use by government of personal information on U.S. citizens and permanent resident aliens ("U.S. persons"†) that had been lawfully collected by public or private entities, without their knowledge or consent.

To address these and other concerns about TIA, Secretary of Defense Donald Rumsfeld appointed two committees in February 2003. One is an internal oversight board to establish "policies and procedures for use within [the Department of Defense] DOD of TIA-developed tools" and "protocols for transferring these capabilities to entities outside DOD. . . . in accordance with existing privacy protection laws and policies."[12]

The other committee is the Technology and Privacy Advisory Committee ("TAPAC"), the members of which are private citizens, independent from the government and "selected on the basis of their preeminence in the fields of constitutional law and public policy relating to communication and information management."[13] TAPAC is charged with examining "the use of advanced information technologies to help identify terrorists before they act."[14] From TAPAC, Secretary Rumsfeld sought answers to four questions:

1. Should the goal of developing technologies that may help identify terrorists before they act be pursued?
2. What safeguards should be developed to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy?
3. Which public policy goals are implicated by TIA and what steps should be taken to ensure that TIA does not frustrate those goals?
4. How should the government ensure that the application of these technologies to global databases respects international and foreign domestic law and policy?[15]

* When first announced, the program was entitled "Total Information Awareness." The title was changed to "Terrorism Information Awareness" in May 2003.

† A "U.S. person" is defined by Executive Order 12333 as an individual who is a U.S. citizen or permanent resident alien, a group or organization that is an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States (except if directed and controlled by a foreign government or governments). TAPAC is concerned only with the privacy interests of individuals and so uses the term to refer only to a U.S. citizen or permanent resident alien.

We believe the decision to create TAPAC has proved both timely and correct. Privacy issues should be considered contemporaneously with the development of technologies that might create them so that appropriate protections can be built into new systems.

This report presents TAPAC's answers to these and related questions about the impact of advanced information technologies on the privacy of personally identifiable information about U.S. persons ("informational privacy"), and the steps necessary to ensure that such privacy is protected when those technologies are used to fight terrorism. Our specific answers appear under the heading "Conclusions and Recommendations," below.

We believe the decision to create TAPAC has proved both timely and correct. Too often, technologies race ahead of public policy. Privacy issues should be considered contemporaneously with the development of technologies that might create them so that appropriate protections can be built into new systems.

Moreover, privacy is often critical to the exercise of other civil liberties, including our rights to think, speak, protest, associate, worship, and participate in the political process free from inappropriate governmental intrusion. As a result, while we have focused on "privacy," we understand that the protection of informational privacy is related to the protection of many civil liberties; threats to privacy often endanger a broader range of civil liberties as well. Therefore, it is essential not only to our privacy but to our freedom that our laws keep pace with advancing technologies. By appointing TAPAC when he did, the Secretary of Defense has helped to ensure that privacy issues are considered along with new technological capabilities.

To reach the conclusions set forth in this report, TAPAC has held one organizational and four public committee meetings; heard from 60 witnesses from government, private industry, academia, and advocacy groups; and consulted hundreds of documents. In addition, there have been numerous subcommittee meetings, and individual committee members and staff have received extensive briefings from more than two dozen other officials and experts. The committee has had access to a wide range of information, both classified and unclassified. The committee welcomed participation by the public and all interested parties, and sought to inform and motivate that participation through a website (www.sainc.com/tapac) containing information from its meetings, related background materials, and this report. The committee's thinking about these difficult issues has been greatly aided by the prior and parallel work of other individuals and organizations.

Government Data Mining

On September 25, 2003, Congress passed the Department of Defense Appropriations Act, 2004.[16] Section 8131 of the Act terminated TIA, but explicitly permitted funding for "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence,"[17] specified in a classified, and therefore non-public, annex to the Act. Under the Act, those tools may only be used in connection with "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens."[18] In its report accompanying the Act, the Conference Committee directed that the Information Awareness Office ("IAO")—the home of TIA—be terminated immediately, but permitted continuing research on four IAO projects.[19]

As a result, while the program known as TIA has been eliminated, the reference to "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence" in the classified annex makes clear that TIA-like activities could continue to be pursued outside of the public's view. Moreover, we were informed about a variety of other activities in DOD and elsewhere that raise similar privacy issues. Some of these have been described to us as a result of a request we made to the General Counsel to "mak[e] sure that we are made aware of all existing and planned programs within the Department that involve 'the application of pattern queries/data correlation technology to counter-terrorism and counter-intelligence missions,' as well as other DOD programs that may use data about U.S. citizens or permanent residents."[20]

In addition, there are a number of government programs in place or under development outside of DOD that rely on broad searches of

DOD Data Mining Activities

- The Army provided $250,000 through an existing defense contractor for Torch Concepts, with the assistance of DOD and TSA, to obtain five million passenger records from JetBlue Airways in September 2002. The records were used for a study demonstrating how data profiling can be used to identify high-risk passengers, with the ultimate intended goal of determining whether profiling could be used to identify people who pose a threat to U.S. forces abroad. For approximately 40 percent of the passengers Torch Concepts was able to buy from a commercial supplier of data products and services demographic information including data on gender, occupation, income, Social Security Number, home ownership, years at current residence, number of children and adults in the household, and vehicles. After a public outcry, the Army abandoned further work on this project; the Inspector General of the Army is currently investigating.[22]

- The Intelligence Community operates an Advanced Research and Development Activity ("ARDA") center, based in DOD in the National Security Agency ("NSA"), to conduct "high risk, high payoff research designed to produce new technology to address some of the most important and challenging IT [information technology] problems faced by the intelligence community." Begun in May 1998, ARDA was designed to conduct "advanced research and development related to extracting intelligence from, and providing security for, information transmitted or manipulated by electronic means."[23] One of ARDA's current projects—Novel Intelligence from Massive Data—appears to address some of the same issues as TIA, including how to focus "analytic attention on the most critical information found within massive data." One of ARDA's goals for this project is to examine large quantities of data to "[r]eveal new indicators, issues, and/or threats that would not otherwise have been found due to the massiveness of the data."[24]

- In 2001, DOD began an Advanced Concept Technology Demonstration, "Counter Bomb, Counter Bomber," to explore technologies for preventing suicide and other human-carried bomb attacks against U.S. military forces abroad. The project identified 120 technologies that could be used not only to protect U.S. military installations, but to use personally identifiable information about non-U.S. persons to identify potential bombers as they were recruited, trained, and transported to their targets, and potential bomb material as it was acquired and transported. Further work on the project is on hold pending TAPAC's report on how to resolve informational privacy issues.

- DOD's Joint Protection Enterprise Network is designed to share information across military commands to enhance decision-making and collaboration regarding efforts to protect U.S. military forces. One project—Threat Alerts and Locally Observed Notices ("TALON")—allows military installations to share information about threats, suspicious activity, or other anomalous behavior via a Web-based system. Information about people—including U.S. persons—who are denied access to, or who are observed behaving suspiciously around, one military installation can be instantly shared with others and aggregated with other data about those people.

Other Government Data Mining Activities

- The Transportation Security Administration ("TSA") in DHS has announced that it is in the process of deploying the second generation of the Computer-Assisted Passenger Prescreening System ("CAPPS II") which compares airline passenger names with private- and public-sector databases to assess the level of risk a passenger might pose.[25] TSA substantially revamped its plans for CAPPS II during the summer of 2003 in response to public concerns about privacy.
- Section 201 of the Homeland Security Act, signed into law in November 2002, requires DHS to "establish and utilize . . . a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools," to "access, receive, and analyze data detect and identify threats of terrorism against the United States."[26]
- Section 314 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act"),[27] adopted in the aftermath of the September 11, 2001 terrorist attacks, expands the power of the Treasury Department's Financial Crimes Enforcement Network—FinCEN—to require financial institutions to report suspected money laundering or terrorist activities by their customers.[28]
- Section 326 of the USA PATRIOT Act requires new "Know Your Customer" rules which require financial institutions to (1) verify the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintain records of the information used to verify the person's identity and; (3) determine whether the person appears on any list of known or suspected terrorists or terrorist organizations.[29]
- Section 365 of the USA PATRIOT Act expands the requirements of the Bank Secrecy Act to require not only financial institutions, but all commercial entities to file currency transaction reports for cash or coin transactions of $10,000 or more.[30]
- Florida police have created a new database—called "MATRIX" (Multistate Anti-Terrorism Information Exchange)—to link law enforcement records with other government and private-sector databases. The new system is designed to "find patterns and links among people and events faster than ever before."[31] Eight states and DHS are now participating in MATRIX. The program is funded by a $4 million grant from the Justice Department and an $8 million from DHS.[32]

personal information concerning U.S. persons to detect and deter terrorist and other criminal activities. Many of these have been the subject of Congressional testimony and press reports. It is therefore clear that TIA was not unique in its potential to use personal data about U.S. persons.

For example, Congress adopted the Homeland Security Act in November 2002, in which it required the Department of Homeland Security ("DHS")—a department concerned with domestic security—to "establish and utilize . . . a secure communications and information technology infrastructure, including data mining and other advanced analytical tools," to "access, receive, and analyze data detect and identify threats of terrorism against the United States."[21] New programs, facilitated by rapid advances in technology, emerged regularly while the committee was meeting.

The common feature of all of these programs is that they involve sifting through data about identifiable individuals, even though those individuals have done nothing to warrant government suspicion, in search of useful information. This is what we understand to be "data mining." As we discuss below, we believe it to be a broad concept, encompassing searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.*[33]

The lists of programs within DOD and other government agencies highlight the types of data mining activities other than TIA currently in use or under development. They are illustrative—not exhaustive—and the variety of uses of personal data they represent suggests that TIA was not the tip of the iceberg, but rather one small specimen in a sea of icebergs. Like TIA, these and similar programs allow real-time searches of databases, often without regard for physical location. They therefore increase the store of personally identifiable information to which the government has access and reduce the need to aggregate data physically to be able to use them.

Data mining has many valuable and lawful uses in both the private and public sectors. It has been employed for years to identify and apprehend criminals, deliver customized services, and improve efficiency. It can help protect public safety and national security, while also reducing the need for potentially more intrusive government activities, such as physical searches of luggage, vehicles, and people. Moreover, the same technologies that make data mining feasible can be used to reduce the amount of personally identifiable data necessary, facilitate data mining with anonymized data, and create immutable audit trails and other protections against misuse. In short, when systems are well constructed and used subject to proper procedures and with appropriate authorization, data mining is a valuable tool in the fight against terrorism.

New Challenges to an Outdated Regulatory Structure

government data mining presents risks to informational privacy, however, and today those risks are exacerbated by the fact that the laws applicable to data mining are disjointed. As a result, programs thought to pose similar risks to informational privacy are subject to a variety of often inconsistent legal requirements. This reflects the historical divide in the United States between laws applicable to law enforcement and those applicable to foreign intelligence and national security activities, as well as the different departments, contexts, and times in which those programs were developed.

It was only three months after Congress required DHS to engage in data mining that it prohibited DOD—a department concerned with security outside of the United States—from deploying data mining tools within the United States, collecting or using data about U.S. persons, or developing other elements of TIA (including translation software, networks to link the intelligence community, and other tools that had few if any privacy implications).[34] This inconsistent treatment of similar technologies based on the department that developed them runs the risk of compromising the protection of both national security and informational privacy.

Laws regulating the collection and use of information about U.S. persons are often not merely disjointed, but outdated. Many date from the

* We recognize that the term "data mining" has been criticized as potentially misleading, to the extent it suggests that data are being depleted (in the way that gold mining depletes the store of gold), or bearing an inherently negative connotation (as in "strip mining"). We use the term in the belief that it is more intuitively understandable to non-experts than "knowledge discovery" or other more recent terms.

While we define "data mining" broadly, we do not recommend that all activities within this definition be subject to new regulation. For example, we recommend no new regulation of data mining based on particularized suspicion, or that is limited to lawfully collected foreign intelligence, or that concerns federal government employees and is conducted solely in connection with their employment. We recommend that data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be subject only to two new requirements (namely, that it be conducted pursuant to the written authorization of the agency head and be subject to compliance audits.) See the discussion under "Conclusions and Recommendations" below.

1970s, and therefore fail to address extraordinary developments in digital technologies, including the Internet. As noted, the government has always used personally identifiable data about individual U.S. persons as part of its law enforcement and national security efforts, subject to legal protections for privacy. Dramatic advances in information technology, however, have greatly increased the government's ability to access data from diverse sources, including commercial and transactional databases. Those technologies have exponentially increased the volume of data available about individuals and greatly reduced the financial and other obstacles to retaining, sharing, and using those data in both the public and private sector.

The ubiquity of information networks and digital data has created new opportunities for tracking terrorists and preventing attacks. It was to respond to these challenges that DARPA created the IAO and began developing TIA. But technological advances also raise important privacy issues and create the need for legal advances as well. New technologies allow the government to engage in data mining with a far greater volume and variety of data concerning U.S. persons, about whom the government has no suspicions, in the quest for information about potential terrorists or other criminals. Current laws are often inadequate to address the new and difficult challenges presented by dramatic developments in information technologies. And that inadequacy will only become more acute as the store of digital data and the ability to search it continue to expand dramatically in the future.

This is especially true in the setting on which we are focused—analyzing personally identifiable data to protect against terrorist threats. The legal protections that have historically applied in this context recognize distinctions between U.S. persons and non-U.S. persons, between law enforcement and national security, and between activities that take place in the United States as opposed to those that take place beyond our borders. This "line at the border" approach to privacy law and to national security is now increasingly outdated because of new technologies and new threats. Information flows ignore national borders and greatly reduce the relevance of geography and nationality.

Similarly, as the terrorist attacks of September 11, 2001, made clear, the threat to national security is both at home and abroad. The threat of attacks from terrorists who may be operating within our borders contribute to making traditional "line at the border" distinctions less adequate. Moreover, we have been reminded repeatedly since September 11 that our response must be far better coordinated—linking intelligence gathered for law enforcement, border security, and national security, in the United States and around the world.

These developments highlight the need for new regulatory boundaries to help protect civil liberties and national security, and to help empower those responsible for defending our nation to use advanced information technologies—including data mining appropriately and effectively. It is time to update the law to respond to new challenges.

TAPAC has approached its charge with both a broad and narrow focus, and with both long- and short-term perspectives. We developed our initial analysis in the context of TIA and related DARPA programs. However, we believe it is counterproductive to the protection of both informational privacy and national security to address only TIA and other DARPA programs, while ignoring the many other government programs that use personal information on U.S. persons.

More importantly, because of the urgent need to enhance information sharing among agencies concerned with intelligence gathering, national security, and law enforcement, we believe a uniform system of laws and technological measures to facilitate data mining and information sharing without compromising the privacy of U.S. persons is essential. Neither national security nor informational privacy are served by subjecting different agencies' data mining activities to different legal regimes. Moreover, the steps that we believe are necessary to protect privacy cannot be accomplished within any one agency or department alone.

We conclude that advanced information technology–including data mining–is a vital tool in the fight against terrorism, but in developing and using that tool the government must–and can–protect privacy.

Finally, because DOD is the only federal department to have an external advisory committee to examine the privacy implications of its programs, TAPAC occupies a unique position. We have benefited from presentations by officials from other departments and by the spirit of cooperation those officials have demonstrated. We have noted that many of the technologies and systems being used for data mining are similar and can raise similar privacy issues. We therefore believe our recommendations could serve as a useful model for other government agencies with programs involving data mining and the use of private sector databases for anti-terrorism or law enforcement purposes.

Security and Liberty

We conclude that advanced information technology—including data mining—is a vital tool in the fight against terrorism, but in developing and using that tool the government must—and can—protect privacy and fundamental civil liberties.

Without question, the fundamental obligation of government is to protect and defend the nation and its people whether from attacks from without or within. The challenge that leaders throughout our nation's history have recognized is how to meet this core obligation without violating our constitutional values.

This is not an easy task. When the nation's security is threatened, the government's constitutional duty to provide for the national defense often leads to constitutionally protected liberties being challenged. The people's inherent concern for ensuring our country's safety makes us willing to compromise in our defense of those liberties. As the Supreme Court wrote in 1963: it is "under the pressing exigencies of crisis, that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action."[35]

Four years later the Court returned to this theme: "It would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which makes the defense of the Nation worthwhile."[36]

On this fundamental point we part company with the views expressed by our colleague William T. Coleman, Jr., in his separate statement.[37] Our nation's history teaches that in times of war and other crises, the need for security inevitably threatens our commitment to liberty. The tension between security and liberty is not new. In 1787 George Washington warned in his letter to the Continental Congress transmitting the new draft Constitution of the need for individuals to "give up a share of liberty to preserve the rest": "It is at all times difficult to draw with precision the line between those rights which must be surrendered, and those which may be reserved."[38]

Later that same year, Alexander Hamilton wrote in Federalist Paper 8, exhorting the people of New York to ratify the Constitution:

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

We believe it is possible to use information technologies . . . without compromising the privacy of U.S. persons. The answer lies in clear rules and policy guidance, . . . supplemented with education and technological tools, developed as an integral part of the technologies that threaten privacy, and enforced through appropriate managerial, political, and judicial oversight.

> will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free.[39]

This is the challenge our nation faces today, a challenge made more acute by the magnitude of the threat, its sustained and well-organized nature, its technological armaments, and the fact that it comes not from an identified enemy abroad but from a largely invisible enemy that may be operating within our borders.

That challenge is not eliminated by the commitment of our leaders or our confidence in their good intentions. The "Bill of Rights," Floyd Abrams writes in his separate statement, "is rooted in distrust of government and the judgment that government must be limited in its powers to assure that the public retains its liberties."[40] We agree.

The presence of known and suspected terrorists within the United States not only makes the war on terrorism more difficult, but also intensifies the risk to privacy. As Governor James Gilmore, Chair of the Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, testified before TAPAC, because the September 11 terrorists exploited this nation's protections for privacy and anonymity, there is a natural impulse to cut back on those protections. But such a move "ignores the historical relationship between the American people and the government of the United States."[41]

Advanced information technologies are essential to fighting terrorism, as stressed by the Congressional *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001*.[42] The Joint Inquiry found that the U.S. intelligence community failed to "bring together and fully appreciate a range of information that could have greatly enhanced its chances of uncovering and preventing Usama [sic] Bin Ladin's plan to attack these United States on September 11, 2001";[43] to translate "the volumes of foreign language counterterrorism intelligence it collected,"[44] and to "adequately share relevant counterterrorism information, prior to September 11,"[45] resulting in an overall "breakdown in communications."[46] When applied to personally identifiable information, however, information technologies can raise significant privacy issues.

We believe it is possible to use information technologies to protect security without compromising the privacy of U.S. persons. The answer lies in clear rules and policy guidance, adopted through an open and credible political process, supplemented with education and technological tools, developed as an integral part of the technologies that threaten privacy, and enforced through appropriate managerial, political, and judicial oversight.

The stakes on both sides—guarding against terrorist attacks and protecting privacy—could not be higher. We must not sacrifice one for the other, because, as Benjamin Franklin warned more than two centuries ago: "they that can give up essential liberty to purchase a little temporary safety deserve

neither liberty nor safety."[47] This is not merely a theoretical issue. Franklin might well have added that those who would trade liberty for safety all too often achieve neither. In the words of President Bush: "stability cannot be purchased at the expense of liberty."[48]

Security and liberty are inextricably linked. If the rule of law is compromised by threats from abroad or from within the nation, the legal guarantees for civil liberties are compromised as well. John Locke wrote almost four centuries ago: "In all states of created beings, capable of law, where there is no law, there is no freedom. For liberty is to be free from the restraint and violence from others; which cannot be where there is no law."[49] The Framers of the Constitution reflected this same view when they linked their commitment to "establish Justice, insure domestic Tranquility, [and] provide for the common defense" with their desire to "secure the Blessings of Liberty."[50]

Our goal in this report is to articulate a framework of legal protections that make it possible, in the words of Senator Ron Wyden (D-Ore.), to "fight terrorism ferociously" without undermining privacy.[51] The magnitude and nature of the new terrorist threat argue for heightening, not compromising, our vigilance concerning privacy. We agree fully with the recent conclusion of the Gilmore Commission in its fifth and final report on combating terrorism: "Rather than the traditional portrayal of security and civil liberties as competing values that must be weighed on opposite ends of a balance, those values should be recognized as mutually reinforcing."[52] That is the goal of our recommendations. As the Markle Foundation Task Force on National Security in the Information Age wisely put it: we need to "mobilize" information in the war against terrorism, while working to "embed respect for essential values into the very fabric" of all government agencies.[53]

We address our recommendations to the Secretary of Defense, but we believe the basic framework should be promulgated more widely because of the need for rapid action to address not only TIA, but the host of other government programs collecting or using data about U.S. persons in the fight against terrorism. This broader, more comprehensive approach is essential if our nation is to achieve its goal of combating terrorism *and* safeguarding the privacy of U.S. persons.

The New Terrorist Threat

The United States faces, in the words of British Prime Minister Tony Blair, "a new and deadly virus."[54] That virus is "terrorism, whose intent to inflict destruction is unconstrained by human feeling and whose capacity to inflict it is enlarged by technology."[55]

This new threat is different in at least four ways from anything the nation has faced before, as the murderous attacks of September 11 painfully demonstrated.

The Threat from Within

First is the power of terrorists to strike from within. In the war on terrorism, the United States is now part of the battlefield. This is a substantial change in the American experience, as Assistant Secretary of Defense for Homeland Security Paul McHale reminded the committee. With the creation of the U.S. Northern Command following the September 11 terrorist attacks, a general officer once again has command responsibility for the continental United States, hearkening back 225 years to when General George Washington commanded the revolutionary army.[56]

The fact that terrorists threaten from within our borders means we have little if any notice of an attack, as William T. Coleman, Jr., observes in his separate statement: Attacks like those of September 11 "had never happened before in the United States, seldom elsewhere in the western world. When nation-states plan to attack another nation-state, usually there is some advance notice. We see armies, navies building up, equipment and uniformed human beings being moved."[57]

The threat from within our borders therefore heightens the importance of detecting terrorists' plans, while making that task all the more difficult. "[T]he difficulty," Mr. Coleman notes, "is caused by the fact that the information relevant to the terrorist is in the same data as that of other persons who are perfectly innocent. In other words, the few possible terrorists' names are interwoven with the overwhelming number of innocent persons. For, in this war, the nation's enemies often are attempting to carry out attacks within the United States and often conceal themselves among the innocent civilian population, [and] use civilian facilities in order to do so. . . ."[58]

The Suicidal Threat

Second, the new threat is marked by the willingness of terrorists to sacrifice their own lives in the relentless pursuit of the devastation of our nation. This suicidal commitment marks a new and dangerous development that significantly undermines traditional defensive strategies. It is substantially more difficult to defend against attacks by people so bent on destruction that they are willing to die.

The Threat of Weapons of Mass Destruction

Third, terrorists have already demonstrated their ability to turn technologies into weapons than can cause mass destruction. Even ordinary airplanes we have seen transformed into deadly missiles capable of unimagined devastation. The risks posed by other technological advances—nuclear, biological,

The combination of coordinated, well-financed terrorists, willing to sacrifice their lives, . . . operating from within the United States . . . poses extraordinary risks to our safety and our way of life.

and chemical—are difficult to comprehend and impossible to overstate. Weapons of mass destruction are now within the grasp of not only nation-states, but individual terrorist organizations. The scope of annihilation threatened by technologies in the hands of terrorists is unprecedented.

The Terrorist Infrastructure

Finally, terrorists are increasingly well organized, using advanced information technologies to communicate with each other and transfer funds around the world instantly, anonymously, and often undetectably. The September 11 attacks demonstrated the terrorists' remarkable ability to launch highly coordinated, well-financed, and painstakingly rehearsed attacks against the United States. This increases the magnitude of risk threatened by terrorist attacks and heightens the difficulty of identifying and apprehending would-be perpetrators.

The New Threat

The combination of coordinated, well-financed terrorists, willing to sacrifice their lives, potentially armed with weapons of mass destruction, capable of operating from within the United States is like nothing else this nation has faced. It poses extraordinary risks to our safety and our way of life, while challenging our ability to defend ourselves.

In the words of our colleague Floyd Abrams:

> The threat of nuclear, biological, or chemical attacks within the United States by terrorists who are, at one and the same time, technologically skilled and suicidally oriented, may well pose the greatest threat to our people that we have ever faced before. The threat is not only real; it is long-term in nature, with no end in sight and, quite possibly, with no end at all. It may be the fate of our children and grandchildren always to be at risk.
>
> Given the level of this threat, it is not only understandable but necessary that our government seek out new and creative ways to prevent acts of terrorism.[59]

It is against this background—of a new, different, and deadly threat—that we have approached Secretary Rumsfeld's charge to our committee: to determine whether "the goal of developing technologies that may help identify terrorists before they act [should] be pursued" and, if so, to "ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy."[60]

Empowering Our Nation's Defenders

Finally, the nature and magnitude of this new threat makes us more aware than ever of the many men and women who fight against terrorism and defend our country. Floyd Abrams is most assuredly correct when he writes that "[m]any dedicated and selfless public servants, both in and out of uniform, who testified before our committee are engaged in that effort and they deserve the nation's thanks for their contributions."[61] We have been fortunate to work with many of them during the preparation of this report, and we are both impressed by, and deeply grateful for, their dedication, skill, and courage.

Far more than gratitude, however, we owe these individuals clear, practical guidance so that they can fight terrorism with maximum effectiveness, but without creating unnecessary risks for themselves or for the laws and values they have pledged their lives to defend.

William T. Coleman, Jr., writes:

> Today the United States has over 150,000 U.S. military persons fighting in Afghanistan and Iraq, plus significant air force, marine, and naval forces around the same area, in addition naval personnel are at seas and oceans throughout the world intercepting ships carrying illegal items, some of which will yield cash to supply terrorists, others carrying items which can be used in assembly of weapons of mass destruction. In addition, there are CIA and other civilian U.S. personnel risking their lives each day to corner terrorists and prevent attacks on the United States, or U.S. facilities abroad, or on its allies. . . . Everyone agrees that obtaining accurate, quick, live intelligence in real-time, informative ways is often as invaluable as actual combat with the terrorists.[62]

We agree. That is what this report is about, with one significant addition: we deal not only with using information to fight terrorism aggressively and effectively, but doing so without compromising the laws and values reflected in our Constitution. Ultimately, as Prime Minister Blair stressed before Congress, "[o]ur ultimate weapon is not our guns, but our beliefs."[63] Amongst those beliefs is a commitment to preserve civil liberties, including privacy, at the same time as we defend ourselves against our enemies.

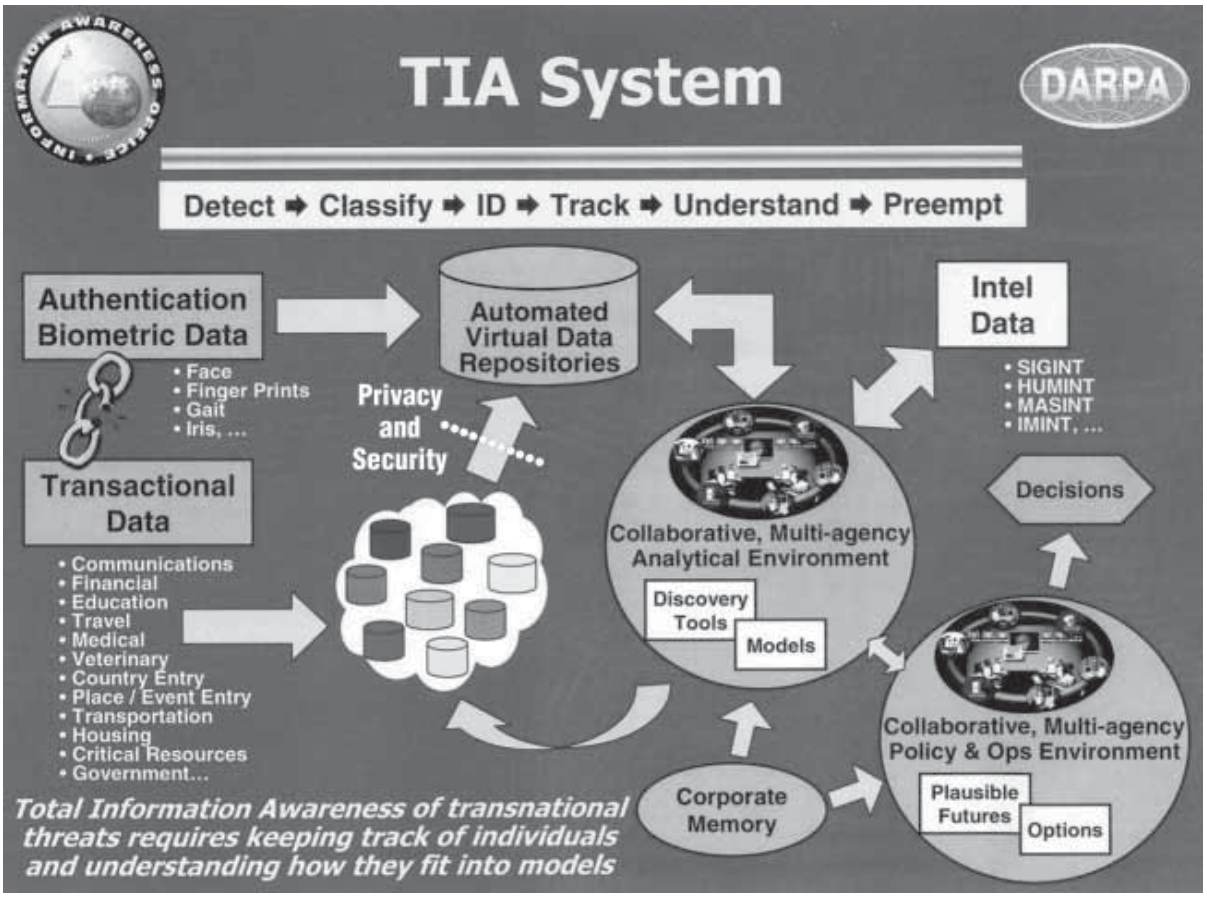
We are profoundly aware of the magnitude of the new terrorist threat, its sustained and well-organized nature, its technological armaments, and the fact that it comes not from an identified enemy abroad but from a largely invisible enemy that may be operating within our borders. As President Bush and others have observed, these distinctive features threaten more than our safety: they threaten our freedom. It would be a poor defense indeed of we gave up the latter in an attempt to secure the former.

Our goal in this report, therefore, is to provide the guidance necessary to empower our nation's defenders to use advanced information technology tools to protect our safety *and* our freedom.

TIA

Early Descriptions of TIA

TIA was first cited publicly in April 2002 by the Director of DARPA, in testimony before the Senate Armed Services Committee.[64] In May, the newly created DARPA IAO described TIA on its website. The program first attracted significant public notice after an August 2002 speech by the then-Director of IAO. Speaking at the DARPA-Tech 2002 Conference, he described the need to "become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options."[65] To accomplish these purposes, he articulated the need for a "much more systematic approach."[66] "Total Information Awareness—a prototype system—is our answer."[67]



Early DARPA TIA Slide

The IAO Director went on to identify "one of the significant new data sources that needs to be mined to discover and track terrorists"—the "transaction space."[68] "If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space."[69] He then showed a slide of transaction data that included "Communications, Financial, Education, Travel, Medical, Veterinary, Country Entry, Place/Event Entry, Transportation, Housing, Critical Resources, and government" records.

Early Public and Congressional Reaction to TIA

The IAO Director mentioned the importance of protecting privacy in his speech, and six months earlier, in March 2002, IAO had begun funding research on privacy-enhancing technologies. Nevertheless, the seeds had been sown for serious concerns about privacy. On November 24, 2002, at the height of the debate over enactment of the Homeland Security Act, William Safire wrote a column in the *New York Times* critical of TIA. Safire wrote:

> Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."
>
> To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you—passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance—and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen.[70]

Although DARPA officials and others argued that Safire misstated facts about TIA, his criticism sparked a nationwide reaction. In the seven months between the initial disclosure of TIA and Safire's column, only 12 press reports had appeared about the program. In the next 30 days, the press carried 285 stories, and by the time TAPAC was created, that figure had risen to 508.

In December 2002, the Assistant to the Secretary of Defense for Intelligence Oversight, who is responsible for ensuring DOD compliance with the laws and regulations governing the collection and use of intelligence information, conducted an internal review of TIA and related programs. The review included not just DARPA, but other units within DOD and the armed services, and The Rand Corporation, a DARPA contractor.

The review found that neither DARPA nor IAO are "intelligence organizations," because they develop but do not use technological tools for information gathering. Nevertheless, the review noted that the same legal constraints that regulate intelligence activities involving data on U.S. persons would apply to the use of TIA by any part of the Defense Intelligence Community to "collect, retain, or disseminate information" on U.S. persons. The review concluded that no legal obligations or "rights of United States persons" had been violated.[71]

The review did determine that some DARPA officials, because they were not involved in intelligence activities, had only a "limited understanding of Intelligence Oversight regulations." As a result of the review, DARPA "quickly took Intelligence Oversight concerns into account" and "institutionalized training and awareness of Intelligence Oversight for its personnel."[72] The review remains open and the Assistant to the Secretary of Defense for Intelligence Oversight has committed to engage in "ongoing monitoring" so long as DARPA is involved in developing tools for intelligence gathering.

Opposition to TIA, however, continued to mount. In late 2002 Senators Charles E. Grassley (R-Iowa), Chuck Hagel (R-Neb.), and Bill Nelson (D-Fla.) wrote separately to the DOD Inspector General asking him to review TIA. On January 10, 2003, the Inspector General announced an audit of TIA, including "an examination of safeguards regarding the protection of privacy and civil liberties."[73] As discussed below,* the audit concluded that "[a]lthough the DARPA development of TIA-type technologies could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility for governmental abuse of power and to help ensure the successful transition of the technology into an operational environment."[74]

On January 23, 2003, the Senate adopted an amendment to the Omnibus Appropriations Act proposed by Senator Ron Wyden (D-Ore.) prohibiting the expenditure of funds on TIA unless the Secretary of Defense, the Director of the CIA, and the Attorney General jointly reported to Congress within 90 days of the enactment of the law about the development of TIA, its likely efficacy, the laws applicable to it, and its likely impact on civil liberties. The amendment also prohibited deployment of TIA in connection with data about U.S. persons without specific Congressional authorization.[75] Congress adopted the amendment as part of the Consolidated Appropriations Resolution on February 13 and the President signed it into law on February 24.[76]

MAY 20, 2003 DARPA REPORT

The report specified by the Wyden Amendment was delivered to Congress on May 20, 2003.[77] It divided DARPA's IAO programs into three categories—TIA, High-Interest TIA-Related Programs, and Other IAO Programs—and described the latter two categories in far greater detail than TIA itself. The report described TIA as:

> a research and development program that will integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies into an experimental prototype network focused on combating terrorism through better analysis and decision making.[78]

In addition, the report described eight other "High-Interest TIA-related Programs" being developed by the IAO in connection with TIA, and ten "Other IAO Programs" that "may provide technology as possible components of TIA prototype but are considered of secondary interest within the context of this report."[79]

With regard to the privacy issues posed by TIA and related programs, the report provided:

> The Department of Defense's TIA research and development efforts address both privacy and civil liberties in the following ways:
>
> - The Department of Defense must fully comply with the laws and regulations governing intelligence activities and all other laws that protect the privacy and constitutional rights of U.S. persons.
> - As an integral part of its research, TIA program itself is seeking to develop new technologies that will safeguard the privacy of U.S. persons.
> - TIA's research and testing activities are conducted using either real intelligence information that the federal government has already legally obtained, or artificial synthetic information that, *ipso facto*, does not implicate the privacy interests of U.S. persons.[80]

* See the discussion under "Inspector General's Report" below.

Congressional Response

On September 25, 2003, Congress passed the Department of Defense Appropriations Act, 2004.[81] Section 8131 of the Act terminated funding for TIA, with the exception of "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence"[82] specified in a classified annex to the Act. Under the Act, those tools may be used only in connection with "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens."[83]

In its report accompanying the Act, the Conference Committee directed that the IAO itself be terminated immediately, but permitted continuing research on four IAO projects: Bio-Advanced Leading Indicator Recognition, Rapid Analytic Wargaming, Wargaming the Asymmetric Environment, and Automated Speech and Text Exploitation in Multiple Languages."[84] The Act thus terminated the IAO and further research on privacy enhancing technologies, while keeping open the possibility of "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence" being developed outside of DARPA in secret. The President signed the Act on September 30, 2003.

Inspector General's Report

On December 12, 2003, the DOD Inspector General released the results of an audit of TIA announced in January in response to Congressional inquiries. The audit concluded that "[a]lthough the DARPA development of TIA-type technologies could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility for governmental abuse of power and to help ensure the successful transition of the technology into an operational environment."[85]

With specific regard to privacy, the audit found that DARPA failed to perform any form of privacy impact assessment, did not involve appropriate privacy and legal experts, and "focused on development of new technology rather than on the policies, procedures, and legal implications associated with the operational use of technology."[86] The report acknowledged that DARPA was sponsoring "research of privacy safeguards and options that would balance security and privacy issues," but found that such measures "were not as comprehensive as a privacy impact assessment would have been in scrutinizing TIA technology."[87]

"As a result," the audit concluded, "DOD risk[ed] spending funds to develop systems that may not be either deployable or used to their fullest potential without costly revision."[88] The report noted that this was particularly true with regard to the potential deployment of TIA for law enforcement: "DARPA need[ed] to consider how TIA will be used in terms of law enforcement to ensure that privacy is built into the developmental process."[89]

Understanding the TIA Controversy

Many factors have contributed to the controversy over TIA. One of the most important was DARPA's inability—or unwillingness—to describe TIA, its objectives, and the data to which it would apply clearly, consistently, and coherently. For example, DARPA's May 2003 report described TIA in these words:

> TIA research and development efforts seek to integrate technologies developed by DARPA (and elsewhere, as appropriate) into a series of increasingly powerful prototype configurations that can be stress-tested in operationally relevant environments using real-time feedback to refine concepts of operation and performance requirements down to the technology component level.[90]

The changing and inconsistent descriptions of TIA have been well documented.[91] In August 2002, DARPA's descriptions of TIA focused on "significant new data sources that [need] to be

mined to discover and track terrorists" and "transactional data" found in "Communications, Financial, Education, Travel, Medical, Veterinary, Country Entry, Place/Event Entry, Transportation, Housing, Critical Resources, and government" records. By 2003, all such references had been removed from TIA materials, the diagram depicting them had been removed from TIA's website, and in DARPA's May 2003 report to Congress, data mining was not even mentioned.

Similarly, when the IAO Director presented TIA to the DARPATech conference in August 2002, he told his audience that "[t]he relevant information extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task."[92] The diagram accompanying his presentation and available on TIA's website until early 2003, referred to "Automated Virtual Data Depositories" and depicted "Transactional Data" flowing into those depositories. The phrase "virtual, centralized grand database" has been widely quoted from DARPA documents. But in its May 2003 report to Congress, DARPA wrote that "the TIA Program is not attempting to create or access a centralized database that will store information gathered from various publicly or privately held databases."[93]

In that same report, DARPA described "How TIA Would Work" in terms of "Red Teams"

> imagin[ing] the types of terrorist attacks that might be carried out against the United States at home or abroad. They would develop scenarios for these attacks and determine what kind of planning and preparation activities would have to be carried out in order to conduct these attacks. . . . The red team would determine the types of transactions that would have to be carried out to perform these activities. . . . These transactions would form a pattern that may be discernable in certain databases to which the U.S. government would have lawful access.[94]

The government would then identify those specific patterns that "are related to potential terrorist planning." Rather than trying to prevent terrorist attacks by searching databases for "unusual patterns," intelligence agencies would "instead [search] for patterns that are related to predicted terrorist activities." This explanation is the sole description of how the TIA program would work in DARPA's May 20, 2003 report to Congress.

Clearly, the objectives of programs may change or one official may describe a program differently than another, but DARPA's failure to acknowledge or explain significant inconsistencies contributed to undermining public and Congressional confidence in the agency. DARPA exacerbated the controversy over TIA in other ways as well.

For example, the TIA logo on the IAO website, depicting an all-seeing eye atop a pyramid, surrounded by the Latin motto "*Scientia Est Potentia*"—Knowledge Is Power—suggested George Orwell's all-knowing "Big Brother" government in his classic novel *1984*. Changing the name from "Total" to "Terrorism" Information Awareness after the controversy erupted, as if the title rather than the potential substance of TIA was the problem, did not help.

Controversy over other IAO projects, such as the planned FutureMAP program, helped to fuel Congressional skepticism. FutureMAP involved the creation of an Internet-based futures market in which traders could bet on the occurrence and timing of events such as terrorist attacks, assassinations, and the like. Although similar markets are used in commercial settings today for purposes as diverse as predicting the weather affecting Florida orange crops and estimating the success of a forthcoming Hollywood movie, the subject matter of FutureMAP and the perception that it was both ill considered and unseemly caused an outcry so great that DoD terminated further consideration of the program and the director of IAO ultimately resigned.

Other factors beyond DARPA's control contributed as well. As a research agency charged with developing, but not implementing, technological tools, DARPA was unprepared to answer critics' questions about the privacy implications of how TIA might be used. Historically, DARPA had engaged in high-risk, high-pay-off research for the DOD, conducted out of the limelight. Much of its research has resulted in spectacular advances, with benefits far beyond the defense establishment—for example, DARPA created ARPANet, the precursor to the Internet, as a technological tool for linking defense researchers—but never before had the agency been required to account for the potential impact on privacy of future uses of a tool it was in the process of developing.

This led to sustained miscommunication between DARPA and its critics. DARPA answered questions about privacy by repeatedly assuring the public that *it* was not aggregating personally identifiable information on U.S. persons or using TIA to access any such information, and that any such activities in the future would be by *other agencies* which would bear responsibility for complying with the laws and regulations applicable to *them*. Some observers found these responses evasive especially in the light of DARPA's public rhetoric promoting TIA. Although the Assistant to the Secretary of Defense for Intelligence Oversight found no evidence that TIA was at any time using personally identifiable information on U.S. persons, DARPA's assurances failed to resolve critics' concerns.

The timing of revelations about TIA also contributed to the controversy surrounding the program. Many Americans were growing increasingly uneasy about government actions, in the aftermath of the September 11, 2001 terrorist attacks, that appeared to threaten civil liberties: the detention of non-U.S. persons without charge or access to counsel, monitoring of inmate telephone calls with their attorneys, passage of the USA PATRIOT Act with the new powers it conferred on the government to conduct—in some cases secret—searches and seizures, physical searches of airline passengers and their luggage, and the Attorney General's Operation TIPS program (later abandoned) under which delivery, repair, and other workers who entered people's homes would report to the government on what they saw there. Moreover, news of TIA was breaking during the fall of 2002, just as Congress was debating the Homeland Security Act, with the goal of centralizing many of the government's surveillance programs within a new Cabinet-level department. All of this coalesced to heighten concerns among legislators and members of the public to the potential threat of government use of personal data.

Another significant contributor to the controversy was DARPA's failure to build protections for privacy into TIA technologies as they were being developed. We recognize that DARPA had underway separate initiatives to develop privacy-protecting technologies, but these were not part of the TIA tools that DARPA was demonstrating in 2002 and 2003. As the Inspector General noted, these research projects "were not as comprehensive as a privacy impact assessment would have been in scrutinizing TIA technology."[95]

Informational privacy is respected and meaningful policy oversight guaranteed only when they are made a central part of the technology development process and when the tools necessary to ensure them are developed as an integral part of writing software and building systems. DARPA failed, in the words of the Inspector General's report, "to ensure that privacy is built into the developmental process."[96] DARPA was by no means unique, but that failure ultimately contributed to the elimination of TIA. Ironically, it also contributed to Congress withdrawing funding for the privacy enhancing technologies that DARPA was developing.

Informational Privacy and Its Protection from Intrusion by the Government

The Meaning of "Privacy"

There is a surprising lack of clarity about what "privacy" means and the role the government should play in protecting it. This is due in part to the fact that the word "privacy" is used to convey many meanings. The Supreme Court alone has used the term to describe an individual's constitutional right to be free from unreasonable searches and seizures by the government;[97] the right to make decisions about contraception,[98] abortion,[99] and other "fundamental" issues such as marriage, procreation, child rearing, and education;[100] the right not to disclose certain information to the government;[101] the right to associate free from government intrusion;[102] and the right to enjoy one's own home free from intrusion by the government,[103] sexually explicit mail[104] or radio broadcasts,[105] or other intrusions.[106]

In addition to its breadth, the term is also inherently subjective. What threatens one individual's sense of privacy may not concern another person.[107] Moreover, most people regard their own privacy as deserving of as much protection as possible, but are far less solicitous about the privacy of others, particularly if privacy interferes with apprehending criminals, locating missing persons, protecting the safety of children and pets, or ensuring the fitness of childcare workers or airline pilots.

The broad and subjective nature of privacy does not undermine its significance, but it does increase the difficulty—and heighten the importance—of determining precisely what privacy interests warrant protection. TAPAC has devoted considerable attention to this issue and to reviewing the U.S. legal system's treatment of privacy. We are concerned primarily with U.S. laws protecting the privacy of personal information from intrusion by the government. We address non-U.S. laws and laws applicable to private sector use of personal information only as necessary to illustrate the range of data on which the government may draw and to identify the legal limits on the government accessing that information.*

Constitutional Protections

Privacy is not explicitly protected in the Constitution. The Supreme Court, however, has repeatedly interpreted many of the amendments constituting the Bill of Rights to provide protection to a variety of elements of individual privacy against government activities. The Court has found protections for privacy in the First Amendment provisions for freedom of expression and association, the Third Amendment restriction on quartering soldiers in private homes, the Fourth Amendment prohibition on unreasonable searches and seizures, the due process clause and guarantee against self-incrimination in the Fifth Amendment, the Ninth and Tenth Amendment reservations of

* As we have noted, this report focuses exclusively on the privacy issues posed by U.S. government data mining programs under U.S. law to U.S. persons. The U.S. laws discussed in this section apply to surveillance, searches, and seizures of personally identifiable information conducted or authorized by government officials within the territory of the United States. Those laws apply outside of the United States only if the surveillance, search, or seizure involves a U.S. citizen (although not necessarily a permanent resident alien).

power in the people and the States, and the equal protection and due process clauses of the Fourteenth Amendment.[108]

We examine the two constitutionally based privacy protections most applicable to informational privacy, and a third provision that limits the ways in which the government may use information.

The Fourth Amendment

One of the colonists' most potent grievances against the British government was its use of general searches. The hostility to general searches found powerful expression in the U.S. Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[109]

As interpreted by the Supreme Court, this provision prohibits "unreasonable" searches and seizures, requires that most searches be conducted only with a warrant issued by a court,[110] conditions the issuing of warrants on the government showing "probable cause" that a crime has been or is likely to be committed and that the information sought is germane to that crime, and generally requires that the government provide the subject of a search with contemporaneous notice of the search.[111] Stanford Law School Dean Kathleen Sullivan has written that "[b]y permitting searches and seizures only if reasonable, and interposing the courts between the privacy of citizens and the potential excesses of executive zeal," these constitutional protections help to protect against "dragnets, or general searches, which were anathema to the colonists who rebelled against the British crown."[112]

The protection afforded by the Fourth Amendment, while considerable, is not absolute. The Supreme Court has determined, for example, that warrants are not required to search or seize items in the "plain view" of a law enforcement officer,[113] for searches that are conducted incidental to valid arrests,[114] and for searches involving national security. Jeffrey H. Smith and Elizabeth L. Howe have written that "[t]he national security exception has been narrowly drawn to apply only in instances of immediate and grave peril to the nation and must be invoked by special authorization of the Attorney General or the President. The national security exception is available only in cases of foreign security, not domestic security, and the contours of the exception are more specifically outlined by statute."[115]

In the areas where the Fourth Amendment does apply, what makes a search or seizure "unreasonable"? In his 1967 concurrence in *Katz v. United States*, Justice Harlan wrote that reasonableness was defined by the individual's "actual," subjective expectation of privacy and the extent to which that expectation was "one that society was prepared to recognize as 'reasonable.'"[116] The Court adopted that test for determining what was "private" within the meaning of the Fourth Amendment in 1968 and continues to apply it today, with somewhat uneven results. The Court has found "reasonable" expectations of privacy in homes,[117] businesses,[118] sealed luggage and packages,[119] and even drums of chemicals,[120] but no "reasonable" expectations of privacy in voice or writing samples,[121] phone numbers,[122] conversations recorded by concealed microphones,[123] and automobile passenger compartments,[124] trunks,[125] and glove boxes.[126]

Most pertinent to TIA and other government projects that could involve accessing data about U.S. persons from commercial databases, the Supreme Court held in 1976 in *United States v. Miller*[127] that there can be no reasonable expectation of privacy in objects or information held by a third party. The case involved bank records, to which, the Court noted, "respondent can assert neither ownership nor possession."[128] Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business,"[129] and therefore the Court found that the Fourth

Amendment is not implicated when the government sought access to them:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government. This Court has held repeatedly that *the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.*[130]

Professor Daniel Solove has summarized the Court's logic: "since information maintained by third parties is exposed to others, it is not private, and therefore not protected by the Fourth Amendment."[131] Congress reacted to the decision by enacting a statutory right of privacy in bank records,[132] but this logic has served as the basis for another important exclusion from the protection of the Fourth Amendment: information about (as opposed to the content of) telephone calls. The Supreme Court has found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, when the call was placed, the duration of the call, etc.), because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call. "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[133]

As a result, under the Fourth Amendment, the use of "pen registers" (to record out-going call information) and "trap and trace" devices (to record in-coming call information) do not require a warrant because they don't collect the content of a call, but only information about the call that is necessarily disclosed to others.

Because virtually all transactions and communications, especially if they have any electronic component, require disclosing information to a third party, the scope of Fourth Amendment protection is dramatically reduced. This is especially apparent in the context of the Internet, both because anonymous cash transactions are technologically difficult and even the most secure, encrypted communications require the disclosure of significant communications attributes. Professor Paul Schwartz has written that those attributes can include "records of session times and durations"; "any temporarily assigned network address"; "any credit card or bank account number" used for payment; and "dialing, routing, addressing and signaling information" that is in transmission.[134] As with information disclosed to a third party, Congress reacted to the Supreme Court's decision by creating a statutory warrant requirement for pen registers.[135]

The exclusion from Fourth Amendment protection of information disclosed to (or possessed by) a third party raises significant issues when applied to government mining of commercial databases and other government efforts to aggregate personally identifiable information held in the private sector. Such information, by definition, will be held by third parties, so government use of those data, under the Supreme Court's current interpretations, is unlikely to be limited by the Fourth Amendment, no matter how great the intrusion into informational privacy.

This raises significant privacy concerns, especially since such information increasingly substitutes for direct surveillance and its aggregation can create detailed and highly personal profiles of individual behavior. *Miller* and its progeny clearly conflict with American values concerning privacy—as suggested by Congress' speedy enactment of statutory privacy rights in material disclosed to third persons and in communications attributes. These actions also highlight the critical role that Congress plays in protecting privacy.

Mr. Coleman suggests that information disclosed to third parties does not warrant protection,

because he characterizes such disclosures as voluntary.[136] This ignores the fact that often such disclosures are not voluntary. We unavoidably disclose information about ourselves everyday, often without knowledge, and increasingly without choice. To fly, open a bank account, or obtain employment, for example, one is required to provide a name (and, in the latter two cases, Social Security Number) and an acceptable form of identification. Such disclosures are hardly "voluntary."

Moreover, even when disclosures are voluntary, they are often made pursuant to explicit promises as to how the information will be used. As the language of *Miller* makes clear, however, the Court does not—or did not in 1976—care about the terms under which the disclosures were made—"even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[137] If a business promises confidentiality to a customer, and subject to that promise obtains access to his or her personal information, we cannot agree with the characterization of that business' subsequent disclosure of that information to the government, even if motivated by the best of reasons, as "voluntary."

Finally, Mr. Coleman ignores the fact that *Miller* denies constitutional protection to information even when the government *seizes* it from an unwilling third party. Again, we believe that to characterize access to information under those terms as "voluntary" is plainly contrary to American values concerning privacy.

Freedom from unreasonable searches and seizures by the government is the core meaning of a constitutional right to informational privacy. Like most constitutional rights, the right to be free from unreasonable searches and seizures applies only against the government. This highlights the conclusion in our recommendations, with which Mr. Coleman disagrees,[138] that data mining by the government presents privacy issues different from—and often greater than—data mining by private entities, and therefore warrants special scrutiny.

This focus on government activity reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance. Only the government collects and uses information free from market competition and consumer preferences. When dealing with the government, individuals have no opportunity to express their expectations of privacy by choosing to do business elsewhere or by not engaging in transactions at all. We, like the framers of our Constitution, recognize that in the government context, the law alone provides—or should provide—protection for those expectations.

The Fourth Amendment applies to searches and surveillance conducted for domestic law enforcement purposes within the United States, and those conducted outside of the United States if they involve U.S. citizens (although not necessarily permanent resident aliens). The Fourth Amendment also applies to searches and surveillance conducted for national security and intelligence purposes within the United States, if they involve U.S. persons who do not have a connection to a foreign power.[139] The Supreme Court has not yet addressed whether the Fourth Amendment applies to searches and surveillance for national security and intelligence purposes, if they involve U.S. persons who are connected to a foreign power or are conducted wholly outside of the United States.[140] Appellate courts have found, however, that there is an exception to the Fourth Amendment's warrant requirement for searches conducted for intelligence purposes within the United States that involve only non-U.S. persons or agents of foreign powers.[141] Statutory protections, discussed below, fill some of the gaps in the Fourth Amendment's scope and impose additional restrictions on government searches and seizures.

Protection Against Government Disclosure of Personal Matters

The Supreme Court has extended the protection of privacy from government intrusion beyond the Fourth Amendment to a more general constitutional right against government-compelled "disclosure of personal matters."[142] In 1977, the Supreme Court decided *Whalen v. Roe*, a case involving a challenge to a New York statute requiring that copies of prescriptions for certain drugs be provided to the state, on the basis that the requirement would infringe patients' privacy rights. In his opinion for the unanimous Court, Justice Stevens wrote that the constitutionally protected "zone of privacy" included "the individual interest in avoiding disclosure of personal matters . . . ."[143] Nevertheless, having found this new privacy interest in nondisclosure of personal information, the Court did not apply strict scrutiny—which it typically reserves for cases involving "fundamental" interests. Instead, applying a lower level of scrutiny, the Court found that the statute did not infringe the individuals' interest in nondisclosure.[144] The Court also explicitly rejected the application of the Fourth Amendment right of privacy, writing that Fourth Amendment cases "involve affirmative, unannounced, narrowly focused intrusions."[145]

The Supreme Court has never decided a case in which it found that a government regulation or action violated the constitutional privacy right recognized in *Whalen*. Lower courts have, with courts in the District of Columbia, Second, Third, Fifth, and Ninth Circuits using *Whalen* to strike down government actions on the basis that they violated individuals' right in nondisclosure.[146] Courts in the Fourth and Sixth Circuits have severely limited the scope of the *Whalen* nondisclosure privacy right.[147] Even those courts that have relied on the right of nondisclosure, however, have applied only intermediate scrutiny, instead of the strict scrutiny typically used to protect fundamental constitutional rights.[148]

Protection Against Unlawful Discrimination

While the Fourth Amendment provides the most direct restraint on the power of the government to search and seize personally identifiable information, the Equal Protection Clause of the Fourteenth Amendment and implicit in the Fifth Amendment limit the government's use of information in ways that might deny persons "the equal protection of the laws."[149]

The Supreme Court's Equal Protection jurisprudence is complex, but it generally requires that if the government acts based on individuals' race, national origin, ethnicity, or religion, the government will have to demonstrate that its action meets strict scrutiny—that the action was necessary to serve a compelling state interest. This standard is difficult to meet. Classifications based on sex or illegitimacy must meet only intermediate scrutiny.[150]

As a practical matter, this means that formal data mining criteria that focus on race, national origin, ethnicity, or religion will be subject to significant judicial scrutiny. Formal criteria that include sex or illegitimacy, and informal, unwritten criteria of all forms, are more likely to be able to involve a suspect category if it is not the sole basis for selecting people for further investigation.[151] And criteria that relate to, but are not identical with, suspect categories are generally permitted so long as the government does not intend to impose disproportionate burdens based on race, national origin, ethnicity, or religion.[152]

Other Protections for Informational Privacy in the Public Sector

Most of the provisions that protect informational privacy from intrusion by the government are statutory, rather than constitutional, in origin.

The Privacy Act of 1974

Congress has enacted a variety of statutory provisions limiting the power of the government

to compel the disclosure of personal information and protecting against misuse of personal information possessed by the government. The broadest of these is the Privacy Act of 1974.[153] That Act requires federal agencies to store only relevant and necessary personal information and only for purposes required to be accomplished by statute or Executive Order; collect information to the extent possible from the data subject; maintain records that are accurate, complete, timely, and relevant; and establish administrative, physical, and technical safeguards to protect the security of records.[154] The Privacy Act also prohibits disclosure, even to other government agencies, of personally identifiable information in any record contained in a "system of records," except pursuant to a written request by or with the written consent of the data subject, or pursuant to a specific exception.[155] Agencies must log disclosures of records and, in some cases, inform the subjects of such disclosures when they occur. Under the Act, data subjects must be able to access and copy their records, each agency must establish a procedure for amendment of records, and refusals by agencies to amend their records are subject to judicial review. Agencies must publish a notice of the existence, character, and accessibility of their record systems.[156] Finally, individuals may seek legal redress if an agency denies them access to their records.

Markle Task Force researcher Sean Fogarty and University of Virginia law professor Daniel Ortiz write that the Privacy Act is less protective of privacy than may first appear, because of numerous broad exceptions.[157] Twelve of these are expressly provided for in the Act itself. These include:

- An agency can disclose its records to officers and employees within the agency itself, the Bureau of the Census, the National Archives, Congress, the Comptroller General, and consumer reporting agencies.[158]
- Information contained in an agency's records can be disclosed for "civil or criminal law enforcement activity if the activity is authorized by law."[159]
- Under the "routine use" exemption,[160] federal agencies are permitted to disclose personal information so long as the nature and scope of the routine use was previously published in the *Federal Register* and the disclosure of data was "for a purpose which is compatible with the purpose for which it was collected." According to the Office of Management and Budget ("OMB"), "compatibility" covers uses that are either (1) functionally equivalent or (2) necessary and proper.[161]

In addition, the Privacy Act has been subject to judicial interpretations which have created new exceptions. For example, courts have found that the following special entities do not constitute an "agency": a federally chartered production credit association, an individual government employee,[162] state and local government agencies,[163] the White House Office and those components of the Executive Office of the President whose sole function is to advise and assist the President,[164] grand juries,[165]and national banks.[166]

Moreover, the Privacy Act applies only to information maintained in a "system of records."[167] The Act defines "system of records" as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[168] As a result, the D.C. Circuit Court held that "retrieval capability is not sufficient to create a system of records. . . . 'To be in a system of records, a record must . . . in practice [be] retrieved by an individual's name or other personal identifier.'"[169] Fogarty and Ortiz have noted that "[a] number of courts have held that private notes written by government agents are not considered a 'system of records' when kept in personal files and are consequently exempt from the Act."[170]

Sectoral Protections

In addition to the Privacy Act and the privacy exceptions to the Freedom of Information Act,[171] there are also many more focused privacy laws applicable to specific sectors of the government

or types of government activities. Many of these apply to information, people, or settings left unprotected by the Supreme Court's interpretation of the Fourth Amendment. For example, the Right to Financial Privacy Act, enacted in response to the Supreme Court's decision in *United States v. Miller*,[172] restricts the government's access to bank records.[173]

Federal statutes prohibit the Department of Health and Human Services from disclosing Social Security records except as "otherwise provided by Federal law" or regulation.[174] Similarly, federal law prohibits the Internal Revenue Service from disclosing information on income tax returns[175] and the Census Bureau from disclosing certain categories of census data.[176]

Some statutes protecting privacy in commercial sectors also impose limits on government access to personal information.[177] For example, the Cable Act of 1984 prohibits cable companies from providing the government with personally identifiable information about their customers, unless the government presents a court order.[178] Stewart Baker writes that such an order can "only be obtained upon 'clear and convincing evidence' that the customer was suspected of engaging in a crime and if the order afforded the customer an opportunity to contest the government's claim."[179] The USA PATRIOT Act amended this provision to apply only to records about cable television service and not other services—such as Internet or telephone—that a cable operator might provide.[180] The Video Privacy Protection Act prohibits video rental companies from disclosing personally identifiable information about their customers unless the government presents a search warrant, court order, or grand jury subpoena.[181] The Family Education Rights and Privacy Act of 1974 contains a similar provision applicable to educational records.[182]

Electronic Surveillance

Perhaps the most significant sectoral protections for informational privacy apply to electronic surveillance and other searches. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, sets forth statutory guidelines for obtaining a warrant to conduct surveillance for domestic law enforcement purposes.[183] These requirements go beyond the protections provided by the Fourth Amendment. James Dempsey writes that the additional protections include:

> permitting the use of wiretaps only for investigations of a short list of very serious crimes; requiring high-level Justice Department approval before court authorization can be sought; requiring law enforcement agencies to exhaust other, less intrusive techniques before turning to eavesdropping; directing them to minimize the interception of innocent conversations; providing for periodic judicial oversight of the progress of a wiretap; establishing a statutory suppression rule; and requiring detailed annual reports to be published on the number and nature of wiretaps.[184]

The USA PATRIOT Act subsequently weakened some of these protections. Even prior to that, however, courts rarely refused the government a wiretap order. Between 1968 and 2002, courts approved a total of 29,250 wiretap orders (9,928 federal and 19,322 state). Those figures have increased fairly steadily since 1980. Over the past 35 years, courts have only refused 32 wiretap orders sought by the government.[185]

The Electronic Communications Privacy Act of 1986 ("ECPA") applies to both government and private-sector surveillance, and provides some—albeit weaker—protection to help fill the gap left by Supreme Court decisions holding that the Fourth Amendment does not apply to communications information disclosed to third parties.[186] The Act sets forth procedures that the government must follow to engage in electronic surveillance.[187] In the case of basic identifying information about calls, the government must merely certify that the "information likely to be obtained is relevant to an ongoing 'criminal investigation.'"[188] The USA PATRIOT Act extended these provisions to "addressing and routing"

information about Internet communications.[189] To obtain more detailed information about communications, such as where a particular cell phone is located, the government must obtain either a search warrant or a special court order—known as a "section 2703(d) order." To obtain a section 2703(d) order, the government must present "specific and articulable facts" that the information sought is relevant to an ongoing criminal investigation.[190]

To obtain access to e-mail stored by a service provider (to which the Fourth Amendment does not apply because the information is in the hands of a third party), ECPA requires that the government obtain a warrant if the e-mail has been stored for 180 days or less.[191] If the e-mail has been stored for more than 180 days, the government need only present a subpoena,[192] which the FBI, the Internal Revenue Service, and grand juries are empowered to issue themselves.[193]

Intelligence Gathering

While the above statutes apply when the government seeks information for law enforcement purposes, the Foreign Intelligence Surveillance Act of 1978 ("FISA") governs surveillance and, since being amended in 1994, physical searches conducted within the United States for the purpose of gathering foreign intelligence.[194] As amended by the USA PATRIOT Act, FISA creates a special eleven-judge court—the Foreign Intelligence Surveillance Court.

FISA regulates certain electronic surveillance and physical searches in the U.S. against foreign powers and agents of foreign powers, including U.S. persons where a significant purpose of the surveillance or search is to obtain foreign intelligence information. An application approved by the Attorney General is submitted to the Court for authorization setting out the facts to support a finding by the judge that there is probable cause to believe that the proposed target is a foreign power or an agent of a foreign power and describing the premises or property to be the subject of the search or surveillance. Each application includes "minimization procedures" as the term is defined in the Act, setting out the procedures to be employed to minimize the acquisition, retention and dissemination of U.S. person information. Surveillance and searches are authorized for periods of 90 days (to target a U.S. person agent of a foreign power) up to a year (to target a foreign government). In certain limited circumstances, the Attorney General may authorize electronic surveillance or physical searches without Court authorization when the means of communication or premises are used exclusively by certain foreign powers as defined in the Act (e.g., a foreign government).

Between 1979 and 2002, FISA judges have approved 15,247 FISA warrants—all but one that the Attorney General has sought.[195] Despite (or perhaps as one contributor to) this high approval rate, the requirements for obtaining a warrant help to impose a discipline and careful internal process for assembling and reviewing FISA warrant applications.

Executive Order 12333, issued by President Ronald Reagan in 1981, establishes the basic framework under which U.S. intelligence activities are conducted today.[196] The Executive Order explicitly recognizes that "[t]imely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the security of the United States," but that intelligence gathering activities must be carried out in a "responsible manner that is consistent with the Constitution and applicable law."[197] The Executive Order restricts government surveillance of U.S. persons outside of the United States, even for foreign intelligence purposes, unless the persons involved are agents of a foreign power or the surveillance is necessary to acquire "significant information that cannot reasonably be acquired by other means."[198]

The Executive Order is implemented within each agency by procedures that require the approval of the agency head and of the Attorney General. DOD adopted its "Procedures Governing the

Activities of DOD Intelligence Components that Affect United States Persons" in December 1982 with the approval of Attorney General William French Smith and Secretary of Defense Caspar W. Weinberger.[199] These procedures address in detail the collection, retention, and dissemination of information about U.S. persons, and provide extensive guidance as to when and how DOD officials may engage in collection techniques such as electronic surveillance and nonconsensual physical searches, but they provide little direct guidance concerning data mining.

The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations ("General Crimes Guidelines"), first adopted in 1976 by Attorney General Edward Levi and most recently revised by Attorney General John Ashcroft in May 2002, provide guidance to FBI officials concerning surveillance and other searches, including concerning the terms under which the FBI may use publicly available sources of information. According to the Guidelines, the FBI:

> may draw on and retain pertinent information from any source permitted by law, including information derived from past or ongoing investigative activities; other information collected or provided by governmental entities, such as foreign intelligence information and lookout list information; publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such information; and information voluntarily provided by private entities.[200]

The Guidelines specifically authorize the FBI to carry out "general topical research, including conducting online searches and accessing online sites and forums as part of such research on the same terms and conditions as members of the public generally," but requires that such research not include searches by "individuals' names or other individual identifiers."[201] The Guidelines authorize "online search activity" and "access [to] online sites and forums on the same terms and conditions as members of the public generally," without any restriction as to subject-based searches, "[f]or the purpose of detecting or preventing terrorism or other criminal activities."[202] Finally, the Guidelines provide that "[f]or the purpose of detecting or preventing terrorist activities," the FBI may "visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally."[203]

The General Crimes Guidelines are supplemented by the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection that Attorney General John Ashcroft revised in October 2003.[204] These more recent Guidelines, large portions of which are classified, focus on guiding the activities of the FBI in "preventing, preempting, and disrupting terrorist threats to the United States."[205] The Guidelines authorize widespread sharing of information necessary to achieve this purpose. The sections concerning how this information may be collected are classified, but given the subject of these Guidelines, it is reasonable to assume that they are no more restrictive than the General Crimes Guidelines.

The number and variety of statutes applicable to government collection and use of personal information highlight the special sensitivity in the United States of government use of personal information, but also suggest the complexity of laws in this area. Moreover, in every case the protection for informational privacy is subject to significant exemptions to accommodate other public interests.[206]

Government Privacy Policies

The most recently adopted privacy protection in the public sector, reflecting an earlier development in the private sector, is the reliance on privacy policies posted on government websites. Beginning in the mid-1990s, the FTC and states attorneys general had encouraged U.S. operators of commercial websites to adopt and publish online privacy policies. Adoption of such policies was

voluntary, compliance with them was not. The Commission interprets section five of the Federal Trade Commission Act, which empowers the FTC to prosecute "unfair and deceptive" trade practices, to include violations of posted privacy policies.[207]

According to the FTC, a privacy policy provides an adequate substantive level of privacy protection only if it contained five elements:

- *Notice*—data collectors must disclose their information practices before collecting personal information from consumers;
- *Choice*—consumers must be given a choice as to whether and how personal information collected from them may be used;
- *Access*—consumers should be able to view and contest the accuracy and completeness of data collected about them;
- *Security*—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use; and
- *Enforcement*—there must be a reliable mechanism in place to impose sanctions for noncompliance with these fair information practices.[208]

The campaign proved successful, with the percentage of commercial websites that posted some form of privacy disclosure rising from 14 percent in 1988 to 88 percent in 2000. Of the "most popular" commercial websites surveyed by the FTC, the numbers went from 73 percent having a privacy disclosure in 1998 to 100 percent in 2000.[209]

In June 1999, OMB Director Jack Lew issued a memorandum to federal agencies instructing them to post privacy policies providing users with basic information about the nature of personally identifiable information collected on the website and the uses to which that information might be put. [210] A year later, the General Accounting Office reported that 85 percent of federal government agency websites posted a privacy policy.[211] By comparison, a 2000 Brown University study of 1,700 state and local government websites found that only 7 percent posted a privacy policy.[212]

In 2002, Congress enacted the E-government Act of 2002 requiring that federal government agencies post privacy policies on their websites.[213] Those policies must disclose:

- what information is to be collected;
- why the information is being collected;
- the intended use of the agency of the information;
- with whom the information will be shared;
- what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- how the information will be secured; and
- the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the "Privacy Act"), and other laws relevant to the protection of the privacy of an individual.[214]

The Act also requires that agencies conduct and, where feasible, publicize privacy impact assessments before developing or procuring new information technologies or instituting new information collections programs.[215] In September 2003, OMB released a memo to heads of executive departments and agencies providing guidance on application of the new law.[216] Information technologies used for national security are exempt from the privacy impact assessment requirement.[217] Because of this exemption, while it remains to be seen what impact this law will have, it is unlikely to play much of a role with regard to data mining for national security and anti-terrorist purposes.[218]

Non-U.S. Privacy Protections and Principles

While the concept of a legal right to privacy first evolved in the United States, and this country is home to some of the strongest protections against government invasions of privacy, many other nations have developed privacy laws. Unlike the U.S. legal system, many of these other nations' laws apply across all sectors and create equal or greater protection for privacy against intrusions by the private sector as by the government, although they often exclude—or apply less protection to—information collection and use relating to national security and foreign intelligence. The first national omnibus privacy law was adopted in Sweden in 1973.[219] The European Union adopted a broad data protection directive in 1995[220] and today all European nations have omnibus laws.

The *Wall Street Journal* reports that these laws are so restrictive that they prohibit a business from making its corporate telephone directory accessible from non-European countries, if it contains office telephone numbers of individual employees.[221] As this example suggests, the protection for informational privacy is both much greater in Europe than in the United States and also conflicts with other values, such as the First Amendment's protection of expression.

There are significant differences among other nations' privacy laws, but they all typically embody a set of "Fair Information Practice" principles. These principles are based on the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines") issued by the Committee of Ministers of the Organization for Economic Cooperation and Development ("OECD").[222] The OECD Guidelines, which are based on a 1973 report by a U.S. Department of Health, Education, and Welfare advisory committee,[223] identify eight principles. While broad and sometimes vague, those principles serve as the basis for many privacy laws, including the U.S. Privacy Act of 1974:

- *Collection limitation principle*—data should be obtained lawfully and fairly;
- *Data quality principle*—data should be relevant to their purposes, accurate, complete and up-to-date;
- *Purpose specification principle*—the identification of the purposes for which data will be used and destruction of the data if no longer necessary to serve that purpose;
- *Use limitation principle*—use for purposes other than those specified is authorized only with consent of the data subject or by authority of law;
- *Security safeguards principle*—procedures to guard against loss, corruption, destruction or misuse of data should be established;
- *Openness principle*—it should be possible to acquire information about the collection, storage and use of personal data systems;
- *Individual participation principle*—the data subject normally has a right of access and to challenge data relating to her; and
- *Accountability principle*—a data controller should be designed and accountable for complying with the measures to give effect to the principles.[224]

The European Union's data protection directive and many more recent privacy laws reflect three additional principles:

- *Special protection for sensitive data principle*—there should be greater restrictions on data collection and processing that involves "sensitive data." U.S. law tends to regard data about children,[225] finances,[226] and health[227] as sensitive. Under the EU data protection directive, information is sensitive if it involves "racial

Even where it is at its strongest, the legal protection for informational privacy is not absolute. It is always in tension with other values and goals.

or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] health or sexual life."[228]

- *Data transfers principle*—this principle explicitly restricts authorized users of personal information from transferring that information to third parties without the permission of the data subject.[229]
- *Independent oversight principle*—entities that process personal data should not only be accountable, but should also be subject to independent oversight. In the case of the government, this requires oversight by an office or department that is separate and independent from the unit engaged in the data processing. Under the data protection directive, the independent overseer must have the authority to audit data processing systems, investigate complaints brought by individuals, and enforce sanctions for noncompliance.[230]

These principles admit of wide interpretation, but they are emerging as an aspirational multinational norm for privacy protection.

SUMMARY

The Supreme Court has interpreted the Fourth Amendment, as well as other constitutional provisions, to provide varying degrees of protection to informational privacy when the government engages in surveillance or searches or seizes personally identifiable information. This protection has been substantially weakened by Supreme Court interpretations excluding information that has been disclosed to a third party, and by the Court's decision in *Whalen v. Roe* to apply only intermediate scrutiny to general disclosure requirements.

Constitutional protection has been bolstered by a variety of common law interpretations, statutes, regulations, and other legal protections. Congress has played a particularly important role by enacting laws to protect privacy. Because of its many sources and the ways in which it has evolved in response to specific issues, the protection is uneven, inconsistent, and in some places incomplete.

Even where it is at its strongest, the legal protection for informational privacy is not absolute. It is always in tension with other values and goals. This is certainly true in the war on terrorism. TAPAC's goal is to minimize that tension in the context of government data mining by identifying the risks to informational privacy that data mining presents and recommending measures to guard against those risks, so that this valuable tool can be used to protect national security without compromising informational privacy.

Privacy Risks Presented by Government Data Mining

Digital Information and the Privacy Debate

Government data mining concerning U.S. persons presents risks to informational privacy which are not adequately addressed by existing law. Those risks are plainly influenced by a larger on-going debate about the privacy of personal information generally. This reflects not only the government's expanding use of personal information in the aftermath of the September 2001 terrorist attacks, but also concerns that predate those attacks. For example, the debate reflects the proliferation of digital technologies and networks, such as the World Wide Web, that make personal information easy and inexpensive to collect, store, share, and use. It is also prompted by the growing role of information technologies in daily life—GPS technology, smart passes, caller id, cell phones, miniature cameras, and computer chips in cars and appliances.

According to the *New York Times*, the types of information that businesses and other private sector entities routinely collect about individuals include:

- Your health history; your credit history; your marital history; your educational history; your employment history.
- The times and telephone numbers of every call you make and receive.
- The magazines you subscribe to and the books you borrow from the library.
- Your travel history. . . .
- The trail of your cash withdrawals.
- All your purchases by credit card or check. In the not-so-distant future, when electronic cash becomes the rule, even the purchases you still make by bills and coins could be logged.
- What you eat. No sooner had supermarket scanners gone on line . . . than data began to be tracked for marketing purposes. . . .
- Your electronic mail and your telephone messages. . . .
- Where you go, what you see on the World Wide Web.[231]

This information may serve valuable private-sector purposes, such as delivering customized service or rewarding frequent travelers or shoppers. Moreover, for legal and proprietary reasons, not all of this information is readily available to anyone who asks, but much of it can be easily purchased. Data about individuals from public records (e.g., property tax records, court documents, hunting and fishing licenses, business and professional licenses), credit reports, warranty and sweepstake entry cards, frequent traveler and shopper programs, magazine subscriptions, Internet "cookies" and other browsing records, and many other sources are widely available. Thanks to powerful information technologies, these data may be inexpensively stored and linked together or with other demographic or proprietary data to build sophisticated portraits of individual behavior.

Informational privacy is critical to participation in democracy and in society.

Businesses, charities, and political parties use databases of personal information everyday for marketing, product and service customization, and fund-raising.

As a result of these and other factors, public and political sensitivity to privacy issues in some quarters is greatly heightened. The consistent results of dozens of surveys over the past decade indicate that most people are worried about privacy, believe they have lost some control of information about themselves, and favor legal steps to protect privacy.[232] This does not mean that they value privacy above all else. In fact, according to Alan Westin, the majority of people are "privacy pragmatists," who recognize the valuable uses of personal information and are willing to permit information about them to be used if they perceive a clear benefit and if the subsequent use is subject to their control or clear legal safeguards.[233]

This pragmatic sensitivity demonstrates that many people regard privacy as of crucial importance in a free society, but as only one value that must be balanced with others. We share this view. Informational privacy is critical to participation in democracy and in society. On this point we disagree with the views to the contrary expressed by our colleague William T. Coleman, Jr.[234] But we do not suggest that privacy is the only important interest. There are other interests that must be taken into account: the ability of the government to combat the risks of terrorism with which our nation is faced is one. The First Amendment-rooted interest in public access to information is another. But the reality of these other interests does not diminish the importance of privacy in a democratic society.

As we discuss in the following sections, awareness that the government may, without individual consent or judicial authorization, obtain access to myriad, distributed stores of information about an individual may have a chilling effect on commercial, social, and political activity. Informational privacy is, therefore, linked to other civil liberties, including freedom of expression, association, and religion.

Data mining is not inherently bad. It has been used for decades for many positive purposes. Data mining by the government of personally identifiable information concerning U.S. persons, however, often does pose privacy risks. The nature and extent of those risks varies widely and will turn on many factors, including the ways in which those systems are used, the data to which they are applied, and the sanctions that flow from that use. Moreover, even if data mining intrudes to some degree on privacy, it may be less intrusive than other government activities to protect public safety and national security, such as physical searches of luggage, vehicles, and people.

Nevertheless, it is possible to generalize meaningfully as to the types of risks that may be posed by data mining technologies when applied to U.S. person data. It is important to do so in order

Informational privacy is . . . linked to other civil liberties, including freedom of expression, association, and religion.

The greatest risk of government data mining is that access to individually identifiable data chills individual behavior.

to craft technological and other safeguards that can protect against those risks so that the government can engage in appropriate data mining to fight terrorism without compromising the privacy interests of U.S. persons.

We believe the privacy risks that government data mining projects may pose can be divided into six broad categories: (1) chilling effect and other surveillance risks; (2) data aggregation; (3) data inaccuracy; (4) data misuse; (5) false positives; and (6) risks associated with data processing.

Chilling Effect and Other Surveillance Risks

The greatest risk of government data mining is that access to individually identifiable data chills individual behavior. As the original TIA motto "*Scientia Est Potentia*" provided: Knowledge Is Power. This conclusion is true not only as to actual knowledge, but also concerning potential knowledge. *Potential* knowledge can equal *present* power. This helps explain the constitutional hostility to general searches—to government surveillance without individualized suspicion—by the government. Awareness that the government may, without probable cause or other specific authorization, obtain access to myriad, distributed stores of information about an individual may alter his or her behavior. People are likely to act differently if they know their conduct *could be* observed.

It is this principle that was at the heart of Jeremy Bentham's concept of the Panopticon—a model prison consisting of a central tower surrounded by a ring of prison cells. One-way windows would allow a person in the tower to see into the prison cells, but prevent the prisoners from seeing into the tower. Bentham posited that a single inspector in the tower could control the behavior of all of the prisoners through "the illusion of constant surveillance."[235] According to philosopher and historian Michel Foucault, "modern society increasingly functions like a super Panopticon," in which government constrains individual behavior by the threat of surveillance.[236]

This is not always a bad outcome. For example, surveillance cameras in stores can deter shoplifting. But surveillance can also impede innocuous, everyday activities. Few Americans would want cameras in their bathrooms or bedrooms or tape recorders in their offices or attached to their phones. Knowledge that the government is observing data we generate through thousands of ordinary activities can alter the way we live our lives and interact with others. Knowledge of that power can cause people to change their behavior to be more consistent with a perceived social norm, to mask their behavior, and/or to reduce their activities or participation in society to avoid the surveillance. Vice President Hubert Humphrey observed almost 40 years ago: "we act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change."[237]

The risk is not only that commercial and social activities are chilled, but that protected rights of expression, protest, association, and political participation are affected as well. In the context of government data monitoring in a democracy, we are especially sensitive to the risk of the government surveillance changing the legal behavior of U.S. persons, encouraging conformance with a

perceived norm, discouraging political dissent, or otherwise altering participation in political life.[238] Professor and former Deputy Attorney General Philip Heymann has written: "No matter how honest the government was in restricting its uses of the data, many citizens would become more cautious in their activities, including being less outspoken in their dissent to government policies. For two hundred years Americans have proudly distrusted their government."[239] The risk, therefore, of the power to access data from disparate sources is not merely to informational privacy, but to civil liberties including freedom of expression, association, and religion.

To diminish these risks, it is critical that government data mining activities be as transparent as possible and subject to both clearly defined limits and effective oversight.

Data Aggregation Risks

The risk of chilling individuals' behavior is especially great when the government is aggregating data from across our lives. As noted, advances in information technologies and networks have resulted in individuals generating hundreds of transactional records everyday as we make purchases, browse the Internet, travel, commute, make phone calls, send e-mail, go to school, punch time clocks, use electronic keys, watch television, or engage in thousands of other ordinary activities. Added to these transactional records are many other records about our behavior, whether consciously constructed (such as employment records) or the product of surveillance cameras in public places and the workplace, audio monitoring at point of sale in retail stores and restaurants, or telephone conversations with merchants recorded for training or security purposes.

The same technologies that make it easy and inexpensive to generate these records, also make it possible and practical to store, share, and combine them. Commercial data aggregators do this every day. Their activities and the impact of those activities on informational privacy are beyond the scope of TAPAC's charge, but their existence demonstrates that the aggregation of disparate information about specific individuals is already a reality. They also provide a convenient one-stop source for the government to obtain some, although certainly not all, of the records we generate every day.

Advanced data mining tools pose additional risks to informational privacy by giving the government the capacity to make simultaneous inquiries of separate databases irrespective of where those databases are located. This raises the possibility that individuals will be profiled and given advantages or denied rights or benefits based on aggregated information that may be outdated, inaccurate, misattributed, or simply inappropriate in a democratic society for the government to access. For example, commercial online retailers today often recommend purchases to a browser based on the aggregated interests of recent users of the browser's computer. As anyone who shares their home computer with children knows, this often results in unusual recommendations when the parent finally gets his or her time online. In the case of recommendations for retail purchases this imprecision is usually merely an inconvenience (or a source of humor or parental concern about what the children are doing online). If the government, however, uses this information to deny boarding of an aircraft or to determine whom to subject to FBI surveillance, the consequences are much more significant.

The practical issues surrounding data aggregation are addressed in the following section. Here we highlight the substantive risks even accurate data mining presents to individual privacy and civil rights. Data aggregation creates the risk that the resulting profile provides the government with substitutes for information it is otherwise not allowed to access or act upon. Similarly, the ability to aggregate records held by third parties may provide the government with precisely the same information it previously would have been required to obtain a warrant to access. In this way,

aggregated data may allow for existing privacy laws to be circumvented inadvertently or may make those laws less relevant.

Data mining can also diminish informational privacy by eliminating the practical obscurity that currently results from data being difficult to locate and access. This is not undesirable in every instance, but knowledge that the government can collect the data trails that we unknowingly leave behind us every day is as, or more, likely to chill individual behavior as direct, real-time government surveillance. As a result, such data mining should be subject to authorization and other procedural requirements and to oversight appropriate to this form of government surveillance.

Data Inaccuracy Risks

Many of the risks associated with the government accessing data about the transactions and experiences of U.S. persons concern the inevitability that some of those data will be inaccurate. Inaccuracy typically occurs in three ways: the data may have been wrong when collected, the data may have been associated or linked to the wrong person, or the government when acting on the data may target the wrong person. All three types of risks are important to guard against.

Data Errors

Some government data mining programs countenance accessing data from private industry or public records not maintained for national security or law enforcement purposes. The accuracy of these records raises important practical concerns about the value of national security analyses performed on potentially bad data, as well as privacy issues. Many records contain errors, especially records maintained for uses where accuracy is not a paramount concern or the subject of significant resources. Transposed letters or numbers, transposed first and last names, missing address components (e.g., apartment number), and other errors can cause significant errors in records. As noted in *Computerworld* magazine in 2003: "A single piece of dirty data might seem like a trivial problem, but if you multiply that 'trivial' problem by thousands or millions of pieces of erroneous, duplicated or inconsistent data, it becomes a prescription for chaos."[240]

Data Integration

Integrating and analyzing a large volume of data such as credit card transactions or airline ticket bookings raise many practical issues, even before considering the potential privacy threat. One of the most significant of these issues concerns the significant difficulties of integrating data accurately. Business and government have long struggled with how to ensure that information about one person is correctly attributed to that individual and only to that individual. Many factors contribute to the difficulty of integrating data accurately:

- Names may be recorded in a variety of different ways in different records (e.g., J. Smith, J.Q. Smith, John Q. Smith).
- Individuals change their names; this is especially likely for women. There are approximately 2.3 million marriages and 1.1 million divorces every year in the United States, often resulting in changed last names (and also changed addresses).[241]
- Many people share names. There are tens of thousands of John Smiths in the United States alone. This is true even of less common names. The information about each of those John Smiths must be kept separate.
- Many individuals have more than one address (e.g., home, office, vacation home, post office box), and are likely to change addresses. As of 1998 there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses. And, according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year.[242] 2.6 million businesses file change-of-address forms every year.

- Inclusion of Social Security Numbers ("SSNs") improves the likelihood of a correct match to the accountholder, but is no guarantee. Even when accounts include SSNs, identification may be difficult because accounts for the same household may reflect different primary SSNs (e.g., husband, wife, minor beneficiary) and because of the presence of transcription errors in recording strings of numbers. Most records do not include SSNs.
- Different companies, or different divisions within the same company, may record or rely on different pieces of information. For example, a retailer may organize its store records by customer name; its catalog sales unit may use residential telephone number; and its e-commerce division may rely on e-mail address.
- Institutions maintain records in a wide variety of formats and on many different technological platforms.

According to the General Accounting Office, the government already suffers significant financial losses from its inability to integrate its own data accurately.[243] Integrating 12 different watch lists maintained by nine federal agencies has proved extremely difficult.[244] The task of integrating data accurately is especially difficult in the counterterrorism arena, which often involves matching data from disparate systems over which the intelligence community has no control, from intercepts and other sources where little or no identifying information is provided, and in ways that prevent seeking or verifying additional identifying information. Any data mining program or computer matching program that requires integrating data from disparate sources poses the risk of targeting one individual because of actions committed by another.

Individual Identification

Another persistent problem is how to verify the identity of people. Fraudulent drivers licenses have proved easy to obtain from state motor vehicles bureaus and fake drivers licenses are widely and inexpensively available. The September 11 hijackers had such documents, and little appears to have changed in the intervening two years. Moreover, photographs on drivers licenses and passports, which are issued for terms of between four and ten years, often provide poor verification of identity. Biometric identifiers are not widely used today, and pose significant issues about their cost, reliability, and impact on privacy. The use of transactional information (e.g., what was the amount of your most recent deposit?) also raises significant privacy and practical issues, especially in the hands of the government. Most Americans do not want the government verifying identity by asking questions about their recent banking transactions.

The risk of an individual being targeted for some consequence because the government has confused him or her with another person is significant. The problems associated with misidentifying people on the current "do not fly" lists are well documented. Consider this report from *USA Today*:

> On all eight flights Greg Yasinitsky booked last year, airline agents stopped him when he tried to get a boarding pass. Each time, the Pullman, Wash., music professor had to endure intensive luggage searches and pat-downs before being cleared to board. The reason: His name was "similar to somebody's name" on the government's terror watch list. Agents "would get a horrified look on their face," he says.
>
> Yasinitsky, 49, is one of scores of travelers who say they've done nothing wrong, but who face repeated harassment at airports because computers flag them as being on a terror watch list. Larry Musarra, a retired Coast Guard commander from Juneau, Alaska, two sons and an uncle have been delayed from boarding 21 flights combined in the past year. A retired English teacher has also encountered delays, as have two San Francisco peace activists and various fliers named David Nelson.[245]

Even in a system designed for security purposes, problems of misidentification are not uncommon.

For example, during a 2002–2003 investigation, the General Accounting Office found that U.S. border guards failed 100 percent of the time to spot counterfeit identity documents that GAO agents were using to enter the country illegally.[246] Similar results were found when GAO agents tried to gain unauthorized access to federal buildings, airports, and military bases prior to the September 11 attacks.[247] This heightens public concerns about the risk of misidentification U.S. persons might face under some elements of government data mining programs, depending upon the use made of them by counter-intelligence and law enforcement officials.

The problems of data inaccuracy are only intensified by government actions such as that of the Justice Department in March 2003, exempting the FBI's National Crime Information Center from the Privacy Act's requirements that data be "accurate, relevant, timely and complete,"[248] or that of DHS in August 2003, exempting the TSA's passenger screening database from the Privacy Act's requirements that government records include only "relevant and necessary" personal information.[249] Inaccuracies may be unavoidable, but the risks they pose for privacy are not insurmountable. Rather than avoiding accuracy obligations, a better approach—for both privacy and national security purposes—is to seek to reduce accuracy risks through careful consideration of the types and sources of data to be used, the use of sophisticated data matching algorithms, protocols for testing and monitoring the accuracy of data and matches, and systems for correcting or discarding bad data.

False Positives

Another significant risk of any data-based system concerns false positives (e.g., people identified as possible terrorists who are not) not because of bad information or misidentification, but because of the inability of the system to distinguish between innocent and suspicious behavior or through reliance on incomplete data. According to Paul Rosenzweig, Senior Legal Research Fellow at The Heritage Foundation, "[t]he only certainty is that there will be false positives."[250] False positives impose many costs: in economic terms, to informational privacy, to national security (which is undermined when scarce resources are spent investigating non-threats), and in public annoyance and undercutting public support for counter-terrorism efforts. Given the inevitability of false positives, government data mining efforts must evaluate the number and percentage of false positives that any system generates and the consequences of a false positive result. Those efforts must also provide some system, consonant with the purpose of the data mining, for detecting and correcting or otherwise responding to false positives. False negatives (e.g., people not identified as possible terrorists who are) can also pose significant risks, although these are not concerned with informational privacy.

Mission Creep

Another privacy risk posed by government access to U.S. person data is caused by the fact that data collected for one purpose are being used for another. For example, an airline passenger requests a special meal for the purpose of ensuring that he or she has something appropriate to eat when in the air. The government, however, may wish to access that information to determine the religious affiliation of the traveler. Data disclosed voluntarily for one purpose are now being used for another wholly different purpose. This threat is especially acute if the subsequent use compromises civil rights, for example, targeting an individual solely on the basis of religion or expression, or using information in a way that would violate the constitutional guarantee against self-incrimination.

Even data accessed or used under an explicit guarantee that they are intended only for one purpose are likely to be used for others later. This is a particularly acute risk when the use of personal data about U.S. persons is justified by an extraordinary need such as protecting against terrorist threats. Once the systems to access and use personal data are in place, there is an understandable interest in using those systems for other worthwhile purposes (e.g., preventing

and prosecuting violent crimes). The consistent experience with data protection suggests that, over time, there is always pressure to use data collected for one purpose for other purposes. The expansive uses to which Social Security Numbers have been put are a practical example.

The danger is not only to privacy expectations, but also to ensuring the appropriateness of the data and the manner in which they are maintained. For example, if a consumer does not have a discount card when shopping at a given store, the cashier may supply one of his or her own so that the customer gets the discounted price. If the government, however, accesses the record of purchases made with a given discount card, the information will not be accurate for the purpose of determining who made the purchase. Similarly, businesses are understandably reluctant to invest significant resources in ensuring the accuracy and protecting the integrity of information that is not particularly sensitive and does not involve a high level of economic value. government data mining, however, may read great significance into that same information, without regard for the fact that little effort was expended to ensure that it was accurate when collected and unchanged while stored.

Reuse of data may be appropriate and efficient when the subsequent uses are sufficiently important or consistent with the initial use to warrant the extension. However, it is important that there be an appropriate process for determining acceptable subsequent uses, an explicit evaluation of the usefulness of the data for new uses, and political and legal oversight.

Data Processing Risks

Disclosure

Whenever data are accessed or stored the risk of disclosure always increases. The disclosure may be by an authorized user who determines there is some public value in disclosure, by an authorized user who simply fails to protect the data's confidentiality, by an authorized user who engages in unauthorized access (discussed above), or through a security breach (discussed below).

Data Misuse

There is also the risk of data misuse. Even the best of information systems suffer some degree of data misuse by people with authorized access. Sometimes the misuse is targeted, such as the use of tax records as a source of information on political opponents. Sometimes the misuse is more akin to curiosity, as in the case of thousands of Internal Revenue Service agents disciplined for browsing through the records of famous taxpayers.[251]

The disclosure and data misuse risks presented by government data mining can be reduced through training, technological tools that limit access to data and maintain an immutable audit trail of who has accessed data, and effective oversight.

Data Transfer

The risks associated with data are always increased when the data are transferred. Information, unlike physical objects, is almost always transferred by being duplicated. A single transfer of data doubles the risks of accidental disclosure, misuse, or alteration. Moreover, when data are transferred, it is virtually impossible for the original custodian to retain meaningful control. In addition, data transfer greatly diminishes the ability to correct erroneous data. This issue has received considerable attention in the context of credit reporting, where consumers object to credit bureaus about inaccurate data supplied by businesses with whom the consumers interact. The bureaus cannot independently verify the accuracy of the data, because the data relate to transactions between the consumer and a third-party business. Moreover, if the bureau does correct the data, but the reporting third-party does not, the latter is likely to report the inaccurate data in the following month's reporting cycle.

This is a serious issue that data mining programs pose, whether or not they involve the government retaining the data. If a business reports inaccurate data into a government data mining system, the

government is ill-placed to know of the data's inaccuracy. However, even if the government discovered the inaccuracy and chose not to rely on the faulty data, if the business does not correct its records, the system would collect the same inaccurate data if it accesses the business' records again in the future. U.S. persons are understandably concerned about being trapped in a cycle of bad data, for which no one takes responsibility, and which are difficult to correct.

The data transfer risks presented by government data mining can be reduced through many of the same tools applicable to other data processing risks, as well as by designing systems to leave data in place whenever possible.

Data Retention

If data are retained by industry for government's use or by government itself, this raises concerns about the inability to move beyond one's own past or to overcome the effects of erroneous data. Many U.S. laws impose a limit on how long certain types of data may be retained or used. For example, the Fair Credit Reporting Act prohibits the dissemination of certain types of obsolete information, such as bankruptcy adjudications more than ten years prior to the report, suits and judgments older than seven years, paid tax liens older than seven years, and any other adverse information older than seven years.[252] State expungement laws allow for certain criminal offenses to be removed from one's record.

The Supreme Court highlighted the risks associated with not only retention, but also transfer and aggregation of personal data, in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, a 1989 case involving FBI rap sheets. Because the rap sheets included only arrest and conviction information that had previously been made public by local law enforcement agencies, the Reporters Committee for Freedom of the Press argued that the rap sheets did not implicate any privacy interest. The Court wrote: "We reject respondents' cramped notion of personal privacy. . . . In an organized society, there are few facts that are not at one time or another divulged to another."[253]

The Court noted that just because information had been made public in disparate places for other purposes, did not mean that no privacy interest applied to it. "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[254] The Court cited to a "web of federal statutory and regulatory provisions" that restricted disclosure of personal information. "[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public."[255]

The Court then cited to its 1977 opinion in *Whalen v. Roe*:

> "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[256]

The passage of time can heighten the privacy interest in information, especially when that information has been aggregated from diverse sources.

The risks associated with data retention can be diminished by clearly specifying the purposes of data mining, carefully evaluating the fitness and relevance of data for the intended purpose, leaving the data in place whenever possible, and implementing systems for updating or discarding

outdated information. As with most mechanisms designed to protect informational privacy, these will also improve the accuracy and efficiency of the data mining as well.

Security

government access to or use of personal data always poses security risks that the data will be intercepted or misappropriated, whether by the unauthorized acts of employees or contractors or third-party "hacking." Hundreds of reported incidents of business and government websites and databases being compromised give a real sense of urgency to this concern. Moreover, it is further exacerbated by the fact that many of the types of personal data that might be most useful for anti-terrorist data mining programs to access are also most useful for identity theft, one of the nation's fastest-growing crimes. Financial records, credit card receipts, airline and rental car transactions, and the like contain precisely the type of information necessary to impersonate another.

Security is enhanced by strong technological protections (such as encryption, firewalls, passwords, and audit trails), but it is also a product of training, personnel screening, oversight, and enforcement as well.

SUMMARY

government data mining can pose a variety of risks to informational privacy. Even technologies presenting no direct threat to privacy may indirectly create privacy risks by making personally identifiable information more readily accessible or understandable to the government. This does not mean that the government should not employ data mining tools, nor does it diminish the threat presented by terrorism. Rather, TAPAC believes that the privacy risks presented by government data mining should lead the government to explicitly take those risks into account when determining whether and how to use data mining tools, use those tools only in ways that contribute meaningfully to the fight against terrorism, and enact appropriate legal, technological, and managerial safeguards to minimize those risks and protect against misuse.

This is especially important because the privacy risks associated with government data mining are only likely to increase as information technologies develop. Microsoft Chief Trustworthy Computing Strategist Scott Charney testified before TAPAC that technological innovation is leading to less expensive storage capacity for digital data, cheaper and more advanced tracking technologies, steady advances in computer processing power, and increased standardization in data formats. Taken together, these developments mean that more personally identifiable data will be created and stored, they will be easier to access, and it will be increasingly possible to aggregate and match them quickly, reliably, and affordably.

Data mining is only in its infancy, and as it expands, so too will the issues it presents for informational privacy. As Representative Jerrold Nadler (D-N.Y.) testified before TAPAC, "[t]he question isn't whether technology will be developed, but rather whether it will be used wisely."[257] That is the goal of this report and of the recommendations that follow: to ensure that government data mining is used wisely in the fight against terrorism.

Conclusions and Recommendations

Based on the forgoing analysis, TAPAC makes three sets of conclusions and recommendations:

1. conclusions concerning TIA and answers to Secretary Rumsfeld's questions to the committee;
2. recommendations concerning data mining within DOD; and
3. recommendations concerning government data mining more broadly.

Our recommendations are rooted in existing law and guided by the principles articulated by the Supreme Court and Congress, but our recommendations also reach beyond the requirements of existing judicial interpretations, laws, and regulations. Serious privacy concerns may well be implicated in circumstances not yet fully recognized by the law.

In fact, legitimate privacy concerns may exist which DOD should take account of but which may never be recognized as legally cognizable rights. TAPAC's charge was to take account of "U.S. law *and American values* relating to privacy,"[258] and the following conclusions and recommendations seek to do so.

TIA and the Secretary's Questions to TAPAC

TIA was a flawed effort to achieve worthwhile ends. It was flawed by its perceived insensitivity to critical privacy issues, the manner in which it was presented, and the lack of clarity and consistency with which it was described. DARPA stumbled badly in its handling of TIA, for which the agency has paid a significant price in terms of its credibility in Congress and with the public. This comes at a time when DARPA's historically creative and ambitious research capacity is more necessary than ever. By maintaining its focus on imaginative, far-sighted research, at the same time that it takes account of informational privacy concerns, DARPA should rapidly regain its bearings. It is in the best interests of the nation for it to do so.

Secretary Rumsfeld posed four questions to TAPAC which we address directly before providing specific recommendations concerning data mining within DOD and elsewhere in the government.

TIA was a flawed effort to achieve worthwhile ends. It was flawed by its perceived insensitivity to critical privacy issues, the manner in which it was presented, and the lack of clarity and consistency with which it was described.

DARPA's historically creative and ambitious research capacity is more necessary than ever. . . . DARPA should rapidly regain its bearings.

1 *Should the goal of developing technologies that may help identify terrorists before they act be pursued?*

Yes, subject to the safeguards outlined in our recommendations below.

2 *What safeguards should be developed to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy?*

We propose a series of safeguards under our recommendations below, including written authorization to engage in data mining; technical standards for data mining operations; the requirement that most data mining involving personally identifiable data concerning U.S. persons be conducted only with the authorization of a court; the appointment of designated privacy officers; and oversight by appropriate administration officials, Congress, and the public.

3 *Which public policy goals are implicated by TIA and what steps should be taken to ensure that TIA does not frustrate those goals?*

TIA and other data mining systems implicate national security and privacy. We believe that the recommendations outlined below are appropriate to ensure that data mining tools are used to enhance national security without compromising privacy.

4 *How should the government ensure that the application of these technologies to global databases respects international and foreign domestic law and policy?*

TIA and other data mining systems may pose issues under the domestic laws of other countries when applied to their citizens. This was amply illustrated by the controversy in late 2003 over the acquisition of personally identifiable information about citizens of Latin American countries by a private U.S. information supplier, acting on behalf of DHS. The supplier and DHS had to delete information obtained from Mexican voter rolls, in violation of Mexican law, and investigations were pending by national authorities in Guatemala, Mexico, Nicaragua, and other countries.[259] Similarly, European officials delayed cooperating with DHS's plan to require airlines, including European airlines, to collect personal information about every passenger and share that information with U.S. officials in an effort to detect terrorists.[260]

The activities of foreign governments, as well as of corporations and other private sector entities, may also threaten the privacy of U.S. persons.

TAPAC has focused on informational privacy issues presented under U.S. law by U.S. government data mining involving U.S. persons. We have concluded that to address the legal requirements applicable to data mining in other nations or the impact of those nations' data mining on U.S. persons was impractical given the time and resources available to us. The privacy officer and panel of external advisors that we call for in Recommendations 3 and 4 below should assist in addressing the legal issues presented under other nations' laws by U.S. government data mining or under U.S. law by foreign government data mining.

The . . . recommendations are intended to help the Secretary of Defense establish the clear rules and policy guidance, educational and technological tools, and appropriate managerial oversight and advisory resources necessary to guide DOD's use of data mining to protect national security without compromising the privacy of U.S. persons.

Recommendations Concerning DOD Data Mining

The following recommendations are intended to help the Secretary of Defense establish the clear rules and policy guidance, educational and technological tools, and appropriate managerial oversight and advisory resources necessary to guide DOD's use of data mining to protect national security without compromising the privacy of U.S. persons.

Given the breadth of our definition of data mining—searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government—the specific actions necessary to protect privacy will differ depending upon the context.

For example, data mining includes "pattern-based" searches, such as those TIA-related technologies were designed to perform. These involve developing models of what terrorist behavior might look like and then examining databases for similar patterns. This is similar to commercial data mining techniques—businesses develop a pattern of attributes or behaviors that their good customers have in common, and then search databases to find people meeting those patterns—but potentially far more powerful given the range of data to which the government has access and the capacity of data mining to eliminate the need to aggregate data before searching them.

As we use the term, data mining may also include "subject-based" searches, which look for information about a specific individual or links to known terrorist suspects. This has long been a basic tool of criminal investigators everywhere: start with *known* suspects and, with proper authorization (in many cases, a warrant or a subpoena), look for information about them and the people with whom they interact. However, the power of data mining technology and the range of data to which the government has access have contributed to blurring the line between subject- and pattern-based searches. The broader the search criteria, and the more people other than actual terrorists who will be identified by those criteria, the more pattern-like these searches become.

Even when a subject-based search starts with a known suspect, it can be transformed into a pattern-based search as investigators target individuals for investigation solely because of their connection with the suspect. The more tenuous the connection, the more like a pattern-based search it becomes. Searches that lack specific focus on identified suspects do pose greater risks for U.S. persons and should be subject to greater scrutiny and accountability. That scrutiny will not only help protect informational privacy, but may also help investigators to hone their inquiries to make them more meaningful and more likely to produce useful results. Good privacy protection in the context of data mining is often consistent with more efficient investigation.

Good privacy protection in the context of data mining is often consistent with more efficient investigation.

Data mining inquiries, however categorized, can serve many useful purposes in the fight against terrorism and other crimes. Because they involve the government accessing personally identifiable information about U.S. persons, however, those inquiries also raise privacy issues. The magnitude of those issues varies depending upon many factors, including: the sensitivity of the data being mined, the expectation of privacy reasonably associated with the data, the consequences of an individual being identified by an inquiry, and the number (or percentage) of U.S. persons identified in response to an inquiry who have not otherwise done anything to warrant government suspicion.

Even significant privacy issues may be resolved—as they have been in related contexts for decades—through appropriate legal and technological protections, such as a requirement that the government establish a predicate and obtain a warrant or other authorization before seizing or searching certain nonpublic information.

This is the approach we follow in our recommendations: the government may engage in data mining concerning U.S. persons only after meeting certain legal and technological requirements that accommodate the likely privacy implications of the search. For analytical clarity, we divide data mining concerning U.S. persons into five categories:

Data Mining Based on Particularized Suspicion

If the data mining is limited to searches based on particularized suspicion about a specific individual, we believe existing law should govern. Because, by definition, there is enough evidence about such a person to warrant further investigation, and that investigation is clearly subject to the protections of the Fourth Amendment, supplemented by federal statutes, we rely on existing law. We understand this category of data mining to include searches seeking to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship passenger manifests or other lists of names or other nonsensitive information about U.S. persons.

The view of William T. Coleman, Jr., in his separate statement that TAPAC's recommendations would require recourse to the Foreign Intelligence Surveillance Court before the government could review an airline passenger manifest is incorrect. Mr. Coleman writes: "I find it hard to say that a person's privacy is invaded when a government agent, seeking to avoid a terrorist attack, sees many innocent persons' names on an aircraft's passenger list among others. . . ."[261] We agree and therefore explicitly recommend that the examination of passenger lists *not* be subject to any new regulatory requirements.

Moreover, to the extent the government wished to access additional information on U.S. person passengers that did require Foreign Intelligence Surveillance Court approval, that approval could be sought one time for an entire aviation security program. In no event would "a judge . . . have to first review each list, hear why the government wishes to look at it," or respond to "changes in such lists [that] occur until the last moment before many flights" as Mr. Coleman states.[262] In any event, even in those situations where we recommend recourse to the Court, we also recommend an exception for exigent circumstances.

Foreign Intelligence Data Mining

We recommend that data mining of personally identifiable data on U.S. persons be subject to the approval of the Foreign Intelligence Surveillance Court, and believe that present authorities allow the government to seek such approval for lawful foreign intelligence activities. To the extent this is not clear under present authorities, we recommend clarification. Our recommendations for FISA court approval do not apply to activities directed wholly against non-U.S. persons.

Federal Government Employees

We recommend no additional requirements applicable to data mining concerning federal government employees that is solely in connection with their employment. Background checks, security investigations, and monitoring of the use of government resources—including telephones and computers—are common features of government employment. They are critical to public accountability, and occur subject to both notice to employees and significant oversight. These activities are beyond the scope of our inquiry and already the subject of extensive regulation.

Publicly Available Data

government data mining that is limited to searches of information concerning U.S. persons that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—poses different privacy issues. While the threat to informational privacy may not be as great as if the searches involved non-public data, such data mining by the government nonetheless raises augmented privacy concerns than if conducted by the private sector.

We therefore believe that the administrative authorization and oversight required under Recommendation 2.1 below are appropriate and should be required. Before the government could engage in data mining of publicly available data concerning U.S. persons, Recommendation 2.1 would require a written finding by the agency head that the data mining is both necessary and appropriate for the lawful purpose for which the information is being sought. Administrative authorization may be granted either for entire programs that include data mining as one element or for specific applications of data mining known or likely to concern U.S. persons. In addition, we would require regular compliance audits, as set forth in Recommendation 2.5.

We are mindful that as more personally identifiable information becomes available via the Internet, and the extraordinary power of technology to aggregate and process that information continues to expand, our society may one day wish to subject government data mining of even publicly available information to greater scrutiny and legal process. For the present, however, we believe the requirements of Recommendations 2.1 and 2.5 below are sufficient to protect the informational privacy of U.S. persons in this setting.

Other Data Mining Involving U.S. Persons

For all other government data mining that involves personally identifiable information about U.S. persons, we recommend below that the government be required to first establish a predicate demonstrating the need for the data mining to prevent or respond to terrorism, and second, unless exigent circumstances are present, obtain authorization from the Foreign Intelligence Surveillance Court for its data mining activities. As we stress, that authorization may be sought either for programs that include data mining known or likely to include information on U.S. persons, or for specific applications of data mining where the use of personally identifiable information concerning U.S. persons is clearly anticipated. Legislation will be required for the Foreign Intelligence Surveillance Court to fulfill the role we recommend.

Our conclusion, therefore, that data mining concerning U.S. persons raises privacy issues, does not in any way suggest that the government should not have the power to engage in data mining, subject to appropriate legal and technological protections.

Our conclusion, therefore, that data mining concerning U.S. persons inevitably raises privacy issues, does not in any way suggest that the government should not have the power to engage in data mining, subject to appropriate legal and technological protections. Quite the contrary, we believe that those protections are essential *so that* the government can engage in appropriate data mining when necessary to fight terrorism and defend our nation. And we believe that those protections are needed to provide clear guidance to DOD personnel engaged in anti-terrorism activities.

Our recommendations are not based on any conclusion that the Supreme Court interprets the Fourth Amendment to *require* them, despite Mr. Coleman's statements to the contrary.[263] If they were, our recommendations would be superfluous, because the privacy protections we advocate would already be required by the Court. Instead, we recommend additional regulation of government data mining precisely because the Court has *not* yet interpreted the Fourth Amendment to require it, despite the dramatic technological changes in the 28 years since the Court decided *Miller*. Until the Court's interpretations catch up with what we believe American values require, our recommendations are intended to help fill the gap and provide much-needed clarity and predictability for both the American public and government officials.

We believe these recommendations should apply generally to the full spectrum of data mining activities throughout DOD that are known or reasonably likely to involve personally identifiable information about U.S. persons, except as specifically noted below. We believe these recommendations are prudent, necessary, and consistent with the leadership Secretary Rumsfeld demonstrated in appointing TAPAC.

Recommendation 1

DOD should safeguard the privacy of U.S. persons when using data mining to fight terrorism. We do not underestimate the difficulty of this challenge, especially in the face of dramatic changes in information technologies and terrorist threats. In the words of the first report of Markle Foundation Task Force on National Security in the Information Age: "Information analysis is the brain of homeland security."[264] There are more than 650 million intelligence intercepts alone every day. One of the most immediate challenges facing U.S. anti-terrorist activities is separating out the "signal" of useful information from the "noise" of all of those data.[265] More data are available than there are—or ever could be—analysts to analyze it.

Technological tools to help analyze data and focus human analysts' attention on critical relationships and patterns of conduct are clearly needed. Their use, however, necessarily raises significant informational privacy issues. We believe that the following recommendations will help assure that the privacy interests of U.S. persons are not compromised.

RECOMMENDATION 2

The Secretary should establish a regulatory framework applicable to all data mining conducted by, or under the authority of, DOD, known or reasonably likely to involve personally identifiable information concerning U.S. persons. Protecting privacy while defending the nation and enforcing its laws requires a broad-based set of tools, including law, technology, training, and oversight. All are necessary.

Government data mining presents special risks to informational privacy. If conducted without an adequate predicate, it has the potential to be a 21st-century equivalent of general searches, which the authors of the Bill of Rights were so concerned to protect against. It may be more or less invasive than a physical general search, but its key characteristic is that data mining involves scrutiny of personally identifiable information where the individuals involved have done nothing to warrant government suspicion.

Some would argue that because the private sector is permitted to engage in data mining, the government should too—that the government should have at least as much access to private sector information as companies and individuals do. This is the position advocated by the Attorney General in his recently amended Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations. Under those guidelines, the government faces little, if any, restriction on accessing personally identifiable information held by third parties.

We disagree. Because government access to personal data can threaten individual liberty and invade constitutionally protected informational privacy rights, such access poses greater and farther-reaching risks than commercial access. government access to personally identifiable information, wherever located, should be subject to clear rules and meaningful oversight to protect informational privacy.[266]

We recommend that the requirements of this section apply to all DOD programs involving data mining concerning U.S. persons, *with three exceptions*: data mining (1) based on particularized suspicion (including searches of passenger manifests and similar lists); (2) that is limited to foreign intelligence that does not involve U.S. persons; or (3) that concerns federal government employees in connection with their employment. As we have already noted, these three areas are already subject to extensive regulation, which we do not propose expanding.

In addition, we recommend that data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be conditioned only on the written authorization described in Recommendation 2.1 and the compliance audits described in Recommendation 2.5, but excluded from the requirements of Recommendations 2.2, 2.3, and 2.4.

All other data mining concerning U.S. persons should comply with all of the following requirements:

RECOMMENDATION 2.1

Written finding by agency head authorizing data mining.

a Before an agency can employ data mining known or reasonably likely to involve data concerning U.S. persons,* the agency head should first make a written finding authorizing the data mining and specifying:

   i the purposes for which the system may be used;

   ii the need for the data to accomplish that purpose;

   iii the specific uses to which the data will be put;

* "Data mining" is defined to mean: searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

iv that the data are appropriate for that use, taking into account the purpose(s) for which the data were collected, their age, and the conditions under which they have been stored and protected;

v that other equally effective but less intrusive means of achieving the same purpose are either not practically available or are already being used;

vi the effect(s) on individuals identified through the data mining (e.g., they will be the subject of further investigation for which a warrant will be sought, they will be subject to additional scrutiny before being allowed to board an aircraft, etc.)

vii that the system has been demonstrated to his or her satisfaction to be effective and appropriate for that purpose;

viii that the system complies with the other requirements of this recommendation as enacted by law, Executive Order, or other means;

ix that the system yields a rate of false positives that is acceptable in view of the purpose of the search, the severity of the effect of being identified, and the likelihood of further investigation; and

x that there is a system in place for dealing with false positives (e.g., reporting false positives to developers to improve the system, correcting incorrect information if possible, remedying the effects of false positives as quickly as practicable, etc.), including identifying the frequency and effects of false positives.

b An agency head may make the written finding described in paragraph (a) above either for programs that include data mining as one element, and data mining concerning U.S. persons may occur, or for specific applications of data mining where the use of information known or likely to concern U.S. persons is clearly anticipated.

RECOMMENDATION 2.2

Technical requirements for data mining. Data mining of databases known or reasonably likely to include personally identifiable information about U.S. persons should employ or be subject to the following requirements:

a *Data minimization*—the least data consistent with the purpose of the data mining should be accessed, disseminated, and retained.

b *Data anonymization*—whenever practicable data mining should be performed on databases from which information by which specific individuals can be commonly identified (e.g., name, address, telephone number, SSN, unique title, etc.) has been removed, encrypted, or otherwise obscured.[267] Where it is not practicable to use anonymized data, or access to identifying information is required, the agency should comply with Recommendation 2.4 below.

c *Audit trail*—data mining systems should be designed to create a permanent, tamper-resistant record of when data have been accessed and by whom.

d *Security and access*—data mining systems should be secured against accidental or deliberate unauthorized access, use, alteration, or destruction, and access to such systems should be restricted to persons with a legitimate need and protected by appropriate access controls taking into account the sensitivity of the data.

e *Training*—all persons engaged in developing or using data mining systems should be trained in their appropriate use and the laws and regulations applicable to their use.

RECOMMENDATION 2.3

Third-party databases. Data mining involving databases from other government agencies or from private industry may present special risks. Such data mining involving, or reasonably likely to involve, U.S. persons, should adhere to the following principles:

a The agency engaging in the data mining should take into account the purpose for which the data were collected, their age, and the conditions under which they have been stored and protected when determining whether the proposed data mining is likely to be effective.

b If data are to be used for purposes that are inconsistent with those for which the data were originally collected, the agency should specifically evaluate whether the inconsistent use is justified and whether the data are appropriate for such use.

c Data should be left in place whenever possible. If this is impossible, they should be returned or destroyed as soon as practicable.

d Government agencies should not encourage any person voluntarily to provide data in violation of the terms and conditions (usually reflected in a privacy policy) under which they were collected.

e Government agencies should seek data in the order provided by Executive Order 12333: from or with the consent of the data subject, from publicly available sources, from proprietary sources, through a method requiring authorization less than probable cause (e.g., a pen register or trap and trace device), through a method requiring a warrant, and finally through a method requiring a wiretap order.

f Private entities that provide data to the government upon request or subject to judicial process should be indemnified for any liability that results from the government's acquisition or use of the data.

g Private entities that provide data to the government upon request or subject to judicial process should be reasonably compensated for the costs they incur in complying with the government's request or order.

RECOMMENDATION 2.4

Personally identifiable information. It is not always possible to engage in data mining using anonymized data. Moreover, even searches involving anonymized data will ultimately result in matches which must be reidentified using personally identifiable information. The use of personally identifiable information known or reasonably likely to concern U.S. persons in data mining should adhere to the following provisions:

a An agency within DOD may engage in data mining using personally identifiable information known or reasonably likely to concern U.S. persons on the condition that, prior to the commencement of the search, DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the search based on the existence of specific and articulable facts that:

  i The search will be conducted in a manner that otherwise complies with the requirements of these recommendations however enacted;

  ii The use of personally identifiable information is reasonably related to identifying or apprehending terrorists, preventing terrorist attacks, or locating or preventing the use of weapons of mass destruction;

  iii The search is likely to yield information reasonably related to identifying or apprehending terrorists, preventing terrorist attacks, or locating or preventing the use of weapons of mass destruction; and

  iv The search is not practicable with anonymized data in light of all of the circumstances (e.g., the type of data, type of search, the need for the personally identifiable information, and other issues affecting the timing of the search).

b DOD may seek the approval from the Foreign Intelligence Surveillance Court described in paragraph (a) above either for programs that include data mining as one element, and data

mining of personally identifiable information known or likely to include information on U.S. persons may arise, or for specific applications of data mining where the use of personally identifiable information known or likely to include information on U.S. persons is clearly anticipated.

c An agency may reidentify previously anonymized data known or reasonably likely to concern a U.S. person that is the result of data mining on the condition that, prior to the commencement of such activity, DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the reidentification based on the existence of specific and articulable facts that:

  i The data is the result of data mining that otherwise complies with the requirements of this recommendation however enacted;

  ii The use of personally identifiable information is reasonably related to identifying or apprehending terrorists, preventing terrorist attacks, or locating or preventing the use of weapons of mass destruction;

  iii The reidentification is likely to yield information relevant to national security; and

  iv The continued use of anonymized data is not practicable in light of all of the circumstances (e.g., the type of data, type of search, the need for the personally identifiable information, and other issues affecting the timing of the search).

d Without obtaining a court order, the government may, in exigent circumstances, search personally identifiable information or reidentify anonymized information obtained through data mining if:

  i The agency head or his or her single designee certifies that it is impracticable to obtain a written order in light of all of the circumstances (e.g., the type of data, type of search, the need for the personally identifiable information, and other issues affecting the timing of the search), and provides a copy of that certification to the privacy officer;

  ii DOD subsequently applies to the court for a written order within 48 hours or, in the event of a catastrophic attack against the United States, as soon as practicable; and

  iii The agency terminates any on-going searches of personally identifiable information or use of reidentified information obtained through data mining if the court does not grant the order.

RECOMMENDATION 2.5

Auditing for compliance. Any program or activity that involves data mining known or reasonably likely to include personally identifiable information about U.S. persons should be audited not less than annually to ensure compliance with the provisions of this recommendation and other applicable laws and regulations.

RECOMMENDATION 3

DOD should, to the extent permitted by law, support research into means for improving the accuracy and effectiveness of data mining systems and technologies, technological and other tools for enhancing privacy protection, and the broader legal, ethical, social, and practical issues in connection with data mining concerning U.S. persons.

RECOMMENDATION 4

The Secretary should create a policy-level privacy officer. The privacy officer would be responsible for ensuring the training of appropriate DOD personnel on privacy issues; assisting in the design and implementation of systems to protect privacy; working with the general counsel, inspector general, other appropriate officials within the department and the services to ensure compliance with such systems; providing advice and

information on privacy issues and tools for protecting the privacy of U.S. persons; and advising the Secretary and other senior department officials on privacy matters and the implementation of these recommendations. The roles we recommend for the privacy officer significantly exceed those relating to compliance with the Privacy Act of 1974 that are performed by the current privacy officer. As a result, we recommend that the privacy officer should report directly to the Secretary, Deputy Secretary, or General Counsel; should have adequate staffing and financial resources to fulfill this expanded mandate; and should have no responsibilities unrelated to privacy.

The privacy officer should report to the Secretary, Deputy Secretary, or General Counsel at least annually on the DOD's compliance with applicable privacy laws and these recommendations however implemented; the number and nature of data mining systems within the department, the purposes for which they are used, and whether they are likely to contain individually identifiable information about U.S. persons; the number and nature of agency findings authorizing data mining; the number and nature of agency findings authorizing searches of individually identifiable information about U.S. persons; and other efforts to protect informational privacy in the agency's collection and use of U.S. person data.

Recommendation 5

The Secretary should create a panel of external advisors to advise the Secretary, the privacy officer, and other DOD officials on identifying and resolving informational privacy issues, and on the development and implementation of appropriate privacy protection mechanisms. The panel should be small (i.e., no more than seven people), politically diverse, and composed of people respected for their integrity, judgment, independence, and experience. Members of the panel should not include current employees of the federal government. Members should be appointed for defined terms and removable prior to the expiration of their terms only for cause.

The panel of external advisors should aid in the development and activities of the privacy officer; work with appropriate DOD personnel to enhance the consistency and effectiveness of privacy protections throughout the department and the services; provide advice and other assistance to ensure rapid, full, and consistent implementation of the framework of privacy protection mechanisms; propose modifications to that framework as necessary; and provide advice to the privacy officer on difficult questions and issues of first impression involving the protection of informational privacy.

The panel members should meet as necessary to carry out their charge. They should have access to all material within DOD involving the operation, development, or acquisition of data mining tools that are used or are likely to be used in connection with U.S. persons, consistent with the security clearances of its members. The panel should have a budget appropriate to the breadth of its responsibilities. The panel should report to the Secretary, Deputy Secretary, or General Counsel, and should provide a report at least annually commenting on the privacy officer's report and providing the panel members' views on the efficacy of DOD's efforts to protect privacy.

Recommendation 6

The Secretary should create and ensure the effective operation of meaningful oversight mechanisms. The creation of a policy-level privacy officer and of a panel of external advisors are critical steps in ensuring appropriate oversight of data mining activities that involve or are reasonably likely to involve data concerning U.S. persons.

In addition, we recommend that the Secretary should provide the reports of the privacy office and the external advisory panel to the appropri-

Data Mining Checklist

The Existence and Purpose of Data Mining

1 Is the proposed activity or system likely to involve the acquisition, use, or sharing of personally identifiable information about U.S. persons?

2 What purpose(s) does the data mining serve? Is it lawful? Is it within the agency's authority? Is it sufficiently important to warrant the risks to informational privacy that data mining poses?

3 Is data mining necessary to accomplish that purpose—i.e., could the purpose be accomplished as well without data mining?

4 Is the data mining tool designed to access, use, retain, and disseminate the least data necessary to serve the purposes for which it is intended?

5 Is the data mining tool designed to use anonymized data whenever possible?

Data Mining Personally Identifiable Information

6 Are there specific and articulable facts that data mining personally identifiable information (or reidentifying previously anonymized information) concerning U.S. persons will be conducted in a manner that otherwise complies with the requirements of applicable laws and recommendations; is reasonably related to identifying or apprehending terrorists, preventing terrorist attacks, or locating or preventing the use of weapons of mass destruction; is likely to yield information relevant to national security; and is not practicable with anonymized data?

The Sources and Nature of Data Concerning U.S. Persons

7 Are the data appropriate for their intended use, taking into account the purpose(s) for which the data were collected, their age, and the conditions under which they have been stored and protected?

8 Are data being accessed or acquired from third parties in violation of the terms and conditions (usually reflected in a privacy policy) under which they were collected?

9 If data are being acquired directly from data subjects, have the individuals been provided with appropriate notice, consistent with the purpose of the data mining activity?

10 Are data being sought in the order provided by Executive Order 12333—i.e., from or with the consent of the data subject, from publicly available sources, from proprietary sources, through a method requiring authorization less than probable cause (e.g., a pen register or trap and trace device), through a method requiring a warrant, and finally through a method requiring a wiretap order?

11 Are personally identifiable data being left in place whenever possible? If such data are being acquired or transferred, is there a system in place for ensuring that they are returned or destroyed as soon as practicable?

The Impact of Data Mining

12 What are the likely effect(s) on individuals identified through the data mining—i.e., will they be the subject of further investigation or will they be immediately subject to some adverse action?

13 Does the data mining tool yield a rate of false positives that is acceptable in view of the purpose of the search, the severity of the effect of being identified, and the likelihood of further investigation?

14 Is there an appropriate system in place for dealing with false positives (e.g., reporting false positives to developers to improve the system, correcting incorrect information if possible, etc.), including identifying the frequency and effects of false positives?

Oversight of Data Mining

15 Are data secured against accidental or deliberate unauthorized access, use, alteration, or destruction, and access to the data mining tool restricted to persons with a legitimate need and protected by appropriate access controls taking into account the sensitivity of the data?

16 Does the data mining tool generate, to the extent technologically possible, an immutable audit trail showing which data have been accessed or transferred, by what users, and for what purposes?

17 Will the data mining tool be subject to continual oversight to ensure that it is used appropriately and lawfully, and that informational privacy issues raised by new developments or discoveries are identified and addressed promptly?

18 Are all persons engaged in developing or using data mining tools trained in their appropriate use and the laws and regulations applicable to their use?

19 Have determinations as to the efficacy and appropriateness of data mining been made or reviewed by an official other than those intimately involved with the development, acquisition, or use of the data mining tool?

ate Congressional committees, and facilitate the appearance at least annually of the privacy officer before one or more of those committees in each house of Congress to provide additional information on data mining activities within DOD and their impact on the privacy of U.S. persons.

To the extent consistent with national security and applicable classification laws and regulations, the Secretary should also make the annual reports of the privacy officer and the external advisory panel public.*

RECOMMENDATION 7

The Secretary should work to develop a culture of sensitivity to, and knowledge about, privacy issues involving U.S. persons throughout DOD's research, acquisition, and operational activities. In addition to regulatory, technical, and other tools for protecting privacy, the experience with TIA, as well as other government data mining programs, suggests the important role that "culture" within a government agency plays in determining how much attention is paid to privacy at every level. Too little attention can result in significant threats to constitutionally protected rights of U.S. persons. Too much or misfocused attention can lead to timidity and the failure to make appropriate use of all legal tools in the fight against terrorism.

We recognize that the department is vast and includes many different units responsible for a diverse array of critical activities. These present a broad range of privacy issues. In some areas—for example, the conduct of foreign intelligence—those issues are the subject of established privacy regulations and well-defined systems to ensure that those regulations are followed. In other areas, privacy issues may be just emerging and

* Mr. Coleman argues against making the privacy officer's report public, on the basis that to do so would "educate the terrorist on what steps the U.S. is taking to prevent him or her from attacking the United States." See infra p. 81 (separate statement of William T. Coleman, Jr.). The committee believes this is highly unlikely given the nature of the report. Moreover, to the extent any risk might exist, it is eliminated by the limitation we recommend that only those portions be made public that are "consistent with national security and applicable classification laws and regulations." Current law would presently require the disclosure of the reports unless they were "specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy" and were "in fact properly classified pursuant to such Executive Order." 5 U.S.C. § 552(b)(1). The standard that TAPAC recommends therefore offers more protection than current law.

the systems for addressing them therefore not so well developed.

We understand that the department faces many concerns, and we do not expect all DOD personnel to become experts on privacy. We believe, however, that heightened sensitivity in all of the department's programs that may involve data mining concerning U.S. persons is necessary to identify potential privacy risks before they materialize and to ensure that programs presenting those risks are referred to the privacy office, general counsel, or other personnel skilled in privacy protection.

There are important initiatives already underway to ensure that personnel throughout DOD are equipped to respond to these challenges—for example, the development of a privacy training module within the Defense Acquisition University. These and other efforts are essential to ensuring not only that the privacy of U.S. persons is respected, but also that all DOD personnel are empowered to carry out their important missions confidently and without fear of being blindsided by unanticipated privacy concerns.

To aid the Secretary in this important task we offer a checklist of questions as a useful guide for identifying specific informational privacy issues related to data mining. This checklist may apply differently in the development, acquisition, and implementation contexts, but it should be useful in all three. We believe it will also aid in the development of a greater awareness of the privacy risks presented by data mining tools and a greater culture of appropriate privacy protection throughout the department.

Recommendations Concerning Government Data Mining

Identifying the risks posed by government data mining and the protections necessary to safeguard against those risks was the purpose for which the Secretary of Defense created TAPAC. That purpose is even more relevant today, as government data mining grows more prevalent, than when we were appointed.

As we have stressed throughout this report, the development and use of advanced information technologies to access and analyze personally identifiable information concerning U.S. persons is not limited to TIA or DOD. Moreover, the privacy issues presented by such data mining cannot be resolved by DOD alone. Action by Congress, the President, and the courts is necessary as well. Moreover, as the only external advisory committee concerned with addressing these questions, we believe it is important to contribute to a national debate on these issues.

While mindful that TAPAC was created by the Secretary of Defense and that we have accordingly focused our inquiry on TIA and other programs within DOD, we believe that the inconsistent and often outdated nature of laws and regulations addressing privacy threaten both our nation's efforts to fight terrorism and the constitutionally protected rights of U.S. persons. Resolving those broader issues is critical to enhancing privacy protection within DOD and to ensuring a more rational, consistent approach to privacy issues raised by mining data concerning U.S. persons throughout the government.

RECOMMENDATION 8

The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities. A government-wide approach is desirable to address the significant privacy issues raised by the many programs under development, or already in operation, that involve the use of personally identifiable information concerning U.S. persons for national security and law enforcement purposes. These issues transcend any one program or department. TIA was only one example. CAPPS II, terrorist watch lists, statutorily mandated data mining and other data analysis programs in DHS, ARDA and its Novel Intelligence from Massive Data project, FinCEN, statutorily mandated "Know Your Customer" rules, expanded Bank Secrecy Act reporting requirements, and MATRIX are other publicly identified examples of such programs. There very well may be others of which we are not aware.

We therefore believe that our recommendations to the Secretary of Defense concerning DOD's programs that involve data mining should also be implemented across the federal government and made applicable to all government departments and agencies that develop, acquire, or use data mining tools in connection with U.S. persons for national security or law enforcement purposes.*

Clearly, some modifications will be necessary. For example, when applied to government data mining for the purpose of law enforcement, the certifications we believe should be required in Recommendation 2 would have to be extended to law enforcement, as well as national security, purposes. Moreover, the court order that we believe should be obtained from the Foreign Intelligence Surveillance Court for data mining with personally identifiable information concerning U.S. persons for national security purposes, may be more appropriately be sought from a traditional federal court when the data mining is for law enforcement purposes. We do not express a view on this matter, other than to note that we recognize that the resolution of informational privacy issues likely will be different in different settings.

We believe that government efforts to protect national security and fight crime and to protect privacy will be enhanced by the articulation of government-wide principles and a consistent system of laws and processes. National standards will also help provide clear models for state and local government efforts as well.

RECOMMENDATION 9

The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities. The inter-agency committee would be composed of privacy officers and other appropriate policy-level personnel from each federal agency involved in national security or law enforcement activities. The committee should work to ensure rapid, full, and consistent implementation of the framework of privacy protection mechanisms; assist in the establishment and coordination of federal government agency privacy offices; work to enhance

* The inclusion of information used for law enforcement, as well as national security, in these last five recommendations does not mean that the committee is "thinking about criminal prosecution, not prevention," as suggested by Williams T. Coleman, Jr., in his separate statement. See infra p. 84 (separate statement of William T. Coleman, Jr.). Our first seven recommendations make no reference whatever to information for law enforcement purposes. We include it within these broader recommendations only because we believe a consistent standard for data mining in both law enforcement and national security contexts will facilitate the information-sharing that so many experts and advisory panels have concluded is essential for detecting and preventing terrorist attacks. See supra p. 8 and sources cited therein.

the consistency and effectiveness of privacy protections across the federal government; propose modifications to existing laws and regulations or the adoption of new laws and regulations as necessary; and provide advice to agency heads and privacy offices on difficult questions and issues of first impression involving the protection of informational privacy.

RECOMMENDATION 10

The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities. The external advisory panel should be small (i.e., no more than seven people), politically diverse, and composed of people respected for their integrity, judgment, independence, and experience. Members of the panel should not include current employees of the federal government. Members should be appointed for defined terms and removable prior to the expiration of their terms only for cause.

The external advisory panel should advise the President concerning implementation of the framework of privacy protection mechanisms; the consistency and effectiveness of privacy protections; and necessary modifications to existing laws and regulations or the adoption of new laws and regulations. The panel should provide advice to the inter-agency committee and government agencies on difficult questions and issues of first impression involving the protection of informational privacy. The panel should report to the President, Congress, and the public at least annually on the government's efforts to protect privacy.

The members of the panel should meet as necessary to carry out their charge. They should have access to all relevant material, consistent with the security clearances of its members. The panel should have a budget appropriate to the breadth of its responsibilities. The panel should report directly to the President or another high-ranking official as the President may designate. Because of the overlap among national anti-terrorism, national security, and law enforcement activities, it is preferable to have one panel carry out these functions in relation to all federal government agencies involved in the use of personally identifiable information in these contexts.

RECOMMENDATION 11

The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process. This vital role was clearly illustrated by Congress' enactment of the Right to Financial Privacy Act in response to the Supreme Court's *Miller* decision, and by the many other privacy statutes that Congress has adopted. Similar action to adopt new, consistent protections, along the lines of these recommendations, for information privacy in the law enforcement and national security contexts is needed today.

More immediately, we believe Congress and the President should authorize the Foreign Intelligence Surveillance Court to receive requests for orders under Recommendations 2.4 and 8 and to grant or deny such orders.

In addition, we believe there is a critical need for Congress to exercise appropriate oversight, especially given the fact that many of these data mining programs may involve classified information which would prevent their being disclosed in full publicly. At a minimum, we believe that each agency's privacy officer and agency head should report jointly to appropriate congressional committees at least annually on the agency's compliance with applicable privacy laws; the number and nature of data mining systems

within the agency, the purposes for which they are used, and whether they are likely to contain individually identifiable information about U.S. persons; the number and general scope of agency findings authorizing data mining; the number and general scope of agency findings and court orders authorizing searches of individually identifiable information about U.S. persons; and other efforts to protect privacy in the agency's collection and use of U.S. person data. We recommend that agency privacy reports be made available publicly to the extent consistent with national security and applicable classification laws and regulations.

One obstacle to effective Congressional oversight of data mining activities is the complex structure of Congressional committees and their overlapping jurisdiction. To facilitate this reporting process and consistent, knowledgeable oversight, each house of Congress should identify a single committee to receive all of the agencies' reports. Other committees may have jurisdiction over specific agencies and therefore also receive reports from those agencies, but we believe it is important for a single committee in each house to maintain broad oversight over the full range of federal government data mining activities. To the extent the jurisdiction of Congressional committees overlaps, we believe it is essential for Congress to clarify and clearly articulate the relative responsibilities of each committee, to avoid undermining either privacy protection or national security efforts.

RECOMMENDATION 12

The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons. The restrictions imposed by Congress in response to TIA in February and September 2003 have had the unintended effect of undermining research into privacy protection technologies and appropriate data mining systems that include those protections. Given the critical importance of these tools to national security and civil liberties, Congress should commit resources to research into these technologies, subject to the safeguards outlined above, and to the broader legal, ethical, social, and practical issues surrounding data mining and privacy protection.

The impact of our recommendations on government data mining efforts is summarized in the accompanying chart.

Impact of TAPAC Recommendations on Government Data Mining

(i.e., searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government)

Type of Information	New Recommended Requirements
Data mining that is not known or reasonably likely to involve *personally identifiable* information about *U.S. persons* (i.e., U.S. citizens and permanent residents)	No new requirements
Data mining limited to *foreign intelligence* that does not concern *U.S. persons*.	No new requirements
Data mining known or reasonably likely to involve *personally identifiable* information about *U.S. persons*:	
• If based on *particularized suspicion* about a specific individual, including searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship *passenger manifests* or other lists of names or other nonsensitive information about U.S. persons.	No new requirements
• If concerning *federal government employees* that is solely in connection with their employment.	No new requirements
• If limited to searches of information that is *routinely available without charge or subscription to the public*—on the Internet, in telephone directories, or in public records to the extent authorized by law.	1 Administrative authorization (set forth in Recommendation 2.1), which may be granted on a "per program" or "per search" basis; and 2 Regular compliance audits (set forth in Recommendation 2.5).
• If conducted with *deidentified data* (i.e., data from which personally identifying elements such as name or Social Security Number have been removed or obscured)	All new requirements apply (i.e., administrative authorization, compliance with technical requirements, special rules for third-party databases, and regular compliance audits, as set forth in Recommendations 2.1, 2.2, 2.3, and 2.5), *except for* need to obtain a Foreign Intelligence Surveillance Court order (set forth in Recommendation 2.4).
• If conducted with *personally identifiable information.*	All new requirements apply (as set forth in Recommendations 2.1-2.5), *including* application to the Foreign Intelligence Surveillance Court (Recommendation 2.4), which can be made on a "per program" or "per search" basis.

Conclusion

The United States faces new and daunting challenges from terrorism on U.S. soil. One critical—and rapidly expanding—tool for responding to that challenge is information technology, and especially the ability to search government and private sector databases for evidence of terrorist activity. When those searches involve personally identifiable information about U.S. persons they raise significant issues about informational privacy. Our nation should use information technology and the power to search digital data to fight terrorism, but should protect privacy while doing so.

The recommendations outlined in this report reflect the essential principles that we believe are necessary to achieve this difficult task. They highlight the critical roles of law and technology. They extend to data mining conducted for both national security and law enforcement purposes, given the new reality that both terrorist threats and data flows ignore national borders. They are designed to respond to inevitable changes in terrorist strategies and technological capacity. They are therefore intended to help guide the development and use not only of data mining programs of which we are aware, but those we have not discovered and those not yet even developed.

While these recommendations impose additional burdens on government officials before they employ data mining tools, we believe that in the long-run they will enhance not only informational privacy, but national security as well. They are designed to help break down the barriers to information-sharing among agencies that have previously hampered national security efforts, to provide sufficient clarity concerning access to and use of personal information concerning U.S. persons so that DOD and other government officials can use such information appropriately, and to ensure that scarce national security resources are deployed strategically and effectively. Most significantly, these recommendations are intended to guard against sacrificing "essential liberty to purchase a little temporary safety," because as Benjamin Franklin warned, if we make that sacrifice we will neither deserve nor achieve either.

Our nation should use information technology and the power to search digital data to fight terrorism, but should protect privacy while doing so.

Separate Statement of Floyd Abrams

I join in the TAPAC report in all respects and add a few observations of my own in response to those of our esteemed colleague, William T. Coleman, Jr.

Mr. Coleman's separate statement begins with and is in good part based on a proposition with which I, and I am sure my colleagues, fully agree. That is that the murderous attack on this nation on September 11, 2001 warrants governmental responses that might previously have been unthinkable. If anything, I might phrase the problem even more hyperbolically than did Mr. Coleman. The threat of nuclear, biological, or chemical attacks within the United States by terrorists who are, at one and the same time, technologically skilled and suicidally oriented, may well pose the greatest threat to our people that we have ever faced before. The threat is not only real; it is long-term in nature, with no end in sight and, quite possibly, with no end at all. It may be the fate of our children and grandchildren always to be at risk.

Given the level of this threat, it is not only understandable but necessary that our government seek out new and creative ways to prevent acts of terrorism. Many dedicated and selfless public servants, both in and out of uniform, who testified before our committee are engaged in that effort and they deserve the nation's thanks for their contributions.

But that is only the beginning of our analysis and it is with respect to the remainder of Mr. Coleman's submission that I respectfully differ. For if, as I think we agree, the nation must adopt a long-term strategy of dealing with terrorism, we must also develop a long-term strategy of preserving civil liberties, including privacy, as we do so.

During other wars this nation has fought, or believed it was about to fight, civil liberties have been amongst the first victims. From the Alien and Sedition Acts of 1798 through Abraham Lincoln's suspension of *habeas corpus*, Woodrow Wilson's prosecution of socialists during World War I, and Franklin D. Roosevelt's incarceration of Japanese-Americans during World War II, our nation's record has not been admirable at resisting the primal instinct of shutting up dissenters and shutting down civil liberties during times of stress. The law has sometimes been useful in protecting civil liberties at such times but generally has not been. That is why, I suspect, the Secretary of Defense wisely asked us not only to focus on "what safeguards should be developed to ensure" that new technology developed within the Department of Defense "is carried out in accordance with U.S. law" but with "*American values related to privacy*"[268] as well. Law may sometimes fail us; our values remain, even if we sometimes forget them during times of strife.

What law are we speaking of? What values? The TAPAC report sets forth in detail the case law under the Fourth Amendment and otherwise protecting privacy interests. While not all privacy interests are protected and those that are are balanced against competing interests, I believe Mr. Coleman significantly understates the degree to which the Supreme Court has held that there is a constitutionally rooted privacy right. The Court's developing jurisprudence in this area has,

to be sure, been controversial.[269] Indeed, the Court has sometimes treated privacy (which is never mentioned in the Bill of Rights) so expansively that, in my view, its rulings have imperiled well established First Amendment rights in doing so.[270] For better or worse, however, that the Court has recognized a constitutionally-rooted right of privacy seems to me just as undeniable as the proposition that American values as well as law include some component of the right, as Justice Brandeis famously put it, "to be let alone."[271]

Any determination of the degree to which TIA threatened privacy values necessarily begins with an analysis of TIA itself. In that respect, Mr. Coleman suggests that "Congress did not really understand the TIA program"[272] and that this led, in turn, to its decision to deny funding to at least some of its activities. I do not know what Congress understood. Having served on TAPAC since its inception eight months ago and having listened to and read carefully all information about TIA provided by DARPA, I can attest without qualification that I too do not really understand the TIA program. DARPA bears considerable responsibility for that.

The TAPAC report sets forth in detail the ever-changing descriptions by DARPA of precisely what TIA would do. The May 20, 2003 DARPA report to Congress, submitted well after the explosion of public controversy about TIA and in direct response to the inclusion of the Wyden Amendment in the Consolidated Appropriations Resolution that became law on February 24, 2003, is illustrative. Its description of TIA's research and development efforts as "seek[ing] to integrate technologies developed by DARPA . . . into a series of increasingly powerful configurations that can be stress-tested in operationally relevant environments using real-time feedbacks to refine concepts of operation and performance requirements down to the technology component level" is simply not comprehensible.[273] Its description of "How TIA Would Work" is limited to a recitation of the creation of Red and Blue teams, the first of which would "imagine the types of terrorist attacks that might be carried out against the United States at home or abroad" and the second of which would seek to combat those imagined attacks.[274] That was, to be sure, one thing TIA would do but surely not the only one. It was affirmatively misleading to suggest that this and this alone was how TIA would work.

We do know this about TIA: it would make available to government employees vast amounts of personal information about American citizens who are not suspected of any criminal conduct. While all the information obtained would, we are told, have been lawfully gathered from government and private sources, that does not begin to assuage the justifiable concern that Big Brother could become far more than a literary reference.

Mr. Coleman observes more than once that he has "confidence in the present leadership of the Defense Department and of the Nation."[275] But the Bill of Rights is rooted in distrust of government and the judgment that government must be limited in its powers to assure that the public retains its liberties. That the "American public," as Mr. Coleman puts it, "does not like officious intermeddlers" is not the problem;[276] that the government may abuse its vast array of powers is. It is no criticism of this or any particular Administration to say that the more information the government amasses about each of us, the more we are at risk.

The proposals of TAPAC seek to minimize those risks while still permitting the government to go about its critical task of protecting our people. One of the most important proposals the committee makes is to urge the Secretary of Defense to recommend to the President and the Congress to involve the judiciary in the process of determining when and to what extent data mining activities can be engaged in by the government.

Mr. Coleman offers hypothetical examples of situations in which he maintains that the government should be able to seek to prevent potential acts of terrorism by reviewing airline passenger lists made available to it. The TAPAC report makes plain that it is urging no changes in law or practice with respect to the very situations posited by Mr. Coleman. In addition, it is worth noting that in truly exigent circumstances, no application need be made to the FISA court in advance—just as no application need be made for a search warrant in those rare circumstances in which public safety requires the promptest government action.[277]

The rule, however, should not be confused with the exception. Just as a general warrant is anathema to our civil liberties, so would be unlimited recourse by the government to all the "public" information that is now so promiscuously available about all of us.

In offering these views, I do not mean to minimize to the slightest degree the dangers we face as a nation that Mr. Coleman correctly identifies. Nor do I maintain that privacy claims must routinely trump efforts to protect our national security. But privacy matters, far more than Mr. Coleman appears willing to acknowledge. The TAPAC report offers an approach which accommodates privacy interests while not stifling the use of new technology to prevent acts of terrorism. American law and American values require no less.

Separate Statement of William T. Coleman, Jr.

I agree with and support completely the committee report's conclusion that research, development and deployment of Terrorist Information Awareness ("TIA") and similar technologies and even broader technology programs are essential to the nation's security, including the need to win the present war against terrorists.[278] I also agree that issues of privacy should always be part of such research, development and deployment. Finally, I agree with many of the committee's recommendations and appreciate the committee's efforts to alert the President, Congress, and the American people to programs which are developing, most with Congressional directions or approval, and some of the problems which could arise. But among the reasons I file these respectful, separate views and recommendations are the following:

1 The report does not sufficiently reflect appreciation of the extent of the security and national defense problems—many novel and new—facing the Nation today in the early stages of the war on terrorism, nor of the important, desirable, beneficial, needed results DARPA was attempting to achieve.

2 The report does not set forth or emphasize sufficiently the nature of the enemy facing us, not one of a foreign nation state, not one easily identified by uniform, but one who wears civilian clothes, one who purposely mixes with innocent U.S. persons, using their facilities (banks, airplanes, flying schools, etc.) and who otherwise immerses himself or herself in our free, open, friendly society, conceals themselves in civilian clothes among the American population living like other U.S. persons, until he or she commits the terrorist acts, then often disappears again into our free, open, trusting, friendly society, living again in civilian clothes and assuming again his or her previous lifestyle.

3 The report directly, or at least by implication, wrongly elevates the concept of privacy and protection thereof—an important American civilized value (every American school person knows and appreciates Mr. Brandeis' "right," said before he went to the bench, "to be let alone")—to the same constitutional level as the fundamental values of liberty, free speech, religion, the political process and racial discrimination issues, each expressly in the Constitution,*[279] and the report wrongly concludes that Government data mining "run[s] the risk of becoming the 21st-century equivalent of the general search" proscribed by the Bill of Rights,[280] and "has the potential to be a 21st-century equivalent of general searches."[281] Relying upon the foregoing concepts, TAPAC suggests that before Government agents can look at data that contain "personally identifiable information," which is there because such persons (or a third person who got the information willingly from the "personally identified" person) willingly gave it to the Government, must first obtain a court order

* The separate statement of our esteemed colleague Floyd Abrams confirms my reading of such pages of the report. See supra pp. 63-65 (separate statement of Floyd Abrams).

by the "Foreign Intelligence Surveillance Court."[282] The only exception to be made, was of immediate "airline or cruise ship passenger manifest or other lists of names" "to identify or locate a specific individual" but even then there would be conditions.[283] The Supreme Court of the United States, however, in repeated cases has rejected such position. Indeed, the report so concedes.[284] In fact, there is no Supreme Court case which held a wrongful invasion of privacy under the circumstances DARPA sought to achieve, or that the Government's search of data in its files willingly supplied by a person, as described immediately above, is within the prohibition in the Fourth Amendment, or violates any other provision in the Constitution of the United States.

With all due respect, my colleagues misunderstand the point I am trying to make when they state that I in any way am attempting to reduce liberty[285] when I say that there is a constitutional difference between how the Government deals with information freely given it by U.S. persons (or to a person who then freely gives it to the Government) as against when the Government has to obtain a search warrant to obtain such information or the Government got it from other than willing persons. And contrary to what our colleague Mr. Abrams[286] and the other committee members say,[287] I do acknowledge, and will continue to defend as I have in the past, that informational privacy does matter. It is an extremely "important American value," as preserving American lives from terrorist attack is as great if not a greater "American value," in fact, a constitutional duty of the President, the Secretary of Defense, and other Government officials and American soldiers. All I am trying to say is that my colleagues are avoiding the proper analysis when they lump such personal information so obtained by the Government with other type of information which the Government might obtain without the willing consent of the person involved.[288] My colleagues should pause to recall the newspaper story about the Assistant U.S. Attorney in the Midwest who had picked up information before the events of September 2001, about one who might well have been the 20th hijacker, but could not get authority from Washington to look at his computer. I am not urging a change in that law, or ignoring the law when one is seeking to search for material the Government never had and cannot obtain voluntarily from a third party who obtained it willingly from the complaining party. I am only urging that my colleagues follow the cases which clearly hold that if information is willingly given to the Government, with no restriction, the Government has the right to look at that information for other reasons. I am also asking them not avoid analysis by lumping privacy, which we all respect and we all wish for ourselves and others, with certain constitutional rights such as freedom of speech, freedom from racial discrimination, freedom from religious discrimination, and freedom to participate in the political process.[289] Also, I urge them not to ignore case law, and the problems that will be caused if they build in a court approval process for the Government to use information it already willingly and legally has, when that court process is not required by law, constitutional or statutory, and has never existed in the past.

The difference in classification of the subject of particular governmental action is of a prime significance in proper analysis under the Fifth and Fourteenth Amendments at least since the famous footnote four in the 1938 case of *United States v. Carolene Products Co.*:[290] if privacy is a subject of the magnitude of liberty, free speech, freedom from racial or religious discrimination, etc., then particular governmental action with respect to such actions' constitutionality is measured by "strict scrutiny," but if privacy is not within the Constitution, or even if it is, but is not in the category of "liberty," "racial discrimination," etc., then particular governmental action with

respect thereto requires a mere rational basis for such action not to violate the Constitution.* Valid constitutional concepts and distinctions, like appropriate words in intellectual discourse, are wise persons' counters especially when called upon to advise Cabinet Secretaries. Failures to make such distinctions are perhaps the basis, in part, for the TAPAC recommendation which I disagree with, to wit: "An agency within DOD may engage in data mining using personally identifiable information known or reasonably likely to concern U.S. persons on the condition that, prior to the commencement of the search, DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the search based on the existence of specific and articulable facts . . . ."[291] One can imagine the unmanageable time delay if there is reason to believe that a group of terrorists plan to be on European flights to the United States in the month of January and the U.S. security people wish to look at the passenger lists for all aircraft making such trips in January, and the airline companies and their governments agree to turn over such lists. Under the rule proposed by TAPAC, a judge would have to first review each list, hear why the Government wishes to look at it. Moreover, changes in such lists occur until the last moment before many flights.[292] This particular TAPAC recommendation also in part is perhaps caused by the failure to understand that the TIA programs are to develop technologies to prevent the terrorists from acting, not to gain evidence to put before the trial court to put the person in jail for committing a crime.

With all due respect, the TAPAC report falls into error because it insists upon equating "privacy," which is not specifically mentioned in the Constitution of the United States (a fact the report concedes[293]), though it is mentioned in some of the cases of the Supreme Court of the United States, with the concept of liberty ("and fundamental liberties"[294]), which clearly is in the Constitution.[295] But as quoted in this statement, the Supreme Court of the United States has clearly and more than once held that if persons willingly and voluntarily give personal information to the federal Government with no restrictions on its use, the federal Government can look at such information for many purposes, including those not contemplated by the person who gave the federal Government such information. It is striking that after such attempt to equate liberty and privacy, the report at the end says that its recommendations in part do not get their authority from any federal statute or any provision of the Constitution of the United States.† The TAPAC report in fact states: "Our recommendations . . . reach beyond the requirements of existing judicial interpretations, laws and regulations."[296]

As my colleagues know, I perhaps would have agreed with many of the recommendations if the governmental entities embraced in such recommendations had had an opportunity to examine them and had the opportunity to advise, when a recommendation went beyond existing law, whether such could be followed without seriously interfering with the ability

* Compare *Lawrence v. Texas*, 123 S. Ct. 2472 (2003) with the case *Lawrence* overrules, *Bowers v. Hardwick*, 478 U.S. 186 (1986). There is also an intermediate category best reflected in the cases dealing with distinctions based upon sex, especially where the state requirement has an adverse effect on women. Compare *United States v. Virginia*, 518 U.S. 515 (1996), with *Grutter v. Bollinger*, 123 S. Ct. 2325 (2003), and *Gratz v. Bollinger*, 123 S. Ct. 2411 (2003).

† Contrary to what the Report says, I do not "suggest[ ] that information disclosed to third persons does not warrant protection . . . ." Supra, pp. 23-24. I said only that *United States v. Miller*, 425 U.S. 435 (1976) so holds. See supra pp. 82-83. I here add only that such case has not been overruled.

to prevent other terrorist acts in the United States or in the lands of its allies causing even greater damage than the 9/11 events.

4 The report pays little attention to the initial problem—use of "personally indentifiable" information willingly supplied to the Government by such "personally identified" persons and legally in the Government's data files—at which the Secretary of Defense had asked TAPAC to look,[297] but instead the report embarks upon many other issues, e.g., "data mining," looked at much more broadly.[298] Some of these issues are certainly worthy of discussion, but not at the expense of ignoring, indeed excluding from separate and distinct analysis, the basic issue at which the Secretary of Defense asked the committee to look. For as I read the Secretary's request the basic question involves the use of "personally identified information" which the persons involved have already willingly turned over to the Government or to a third party who has willingly turned it over to the Government. In neither case is there a statute which limits the purpose for which the Government's agent can look at such information. Once a clear analysis is made of this issue, the approach to "data mining" looked at "more broadly" might take a different approach, but, in any event, what is described in the previous sentence should not call for court approval before proceeding.

5 The report makes recommendations to the President and the entire Government, which are in my judgment, beyond what the committee was asked to do. That does not mean that some of the ideas are not good ideas, but they should be put in a much less mandatory or specific form.

6 The report does not emphasize that in the TIA program there was *no* collection of *new* personal information and that instead the TIA program was dealing only with information already lawfully collected by the Government or perhaps a third person who legally and willingly turned it over to the Government,[299] and there was no statutory restriction against the use which the operating entity would make of such personal information if the DARPA research were successful.

7 The report shows little appreciation that privacy issues were, in fact, part of the DARPA research plans.[300] The report does not affirmatively state, as it should, that most, if not all, of the data mining programs described in the report (including the "broader ones") are approved (sometimes even directed) by Congress and that the public is aware of them. This omission perhaps will cause the critic to suggest that responsible public officials are presently acting wrongly or improperly.

First, in order to place in context the questions TAPAC was requested by the Secretary of Defense to answer—particularly the use of data willingly given to the Government by the person or willingly to a third person who willingly gives it to the Government—some background:

A hallmark of the United States is that its people—of all races, creeds, religions, color, ethnic groups, native and foreign-born or of U.S. or foreign-born ancestors—move freely about, seldom stopped by any checkpoint. Freedom and liberty are sometimes more important to most Americans than getting a good job or eating a good meal. Another hallmark of the United States is that it is a nation of great diversity of people, its welcoming mat is as open as any nation and it welcomes visitors as freely as any other nation in the world. Today also, most U.S. citizens, most U.S. persons, are repulsed by profiling by race, religion, national origin or ethnicity.

In the Census 2000, 281.4 million people were counted in the United States, a 13.2% increase from the 1990 census population. Assuming that there is a 1% growth per year since Census 2000,

there are in the United States as of January 1, 2004 a population of over 285 million people. Of the 285 million people, 18 million are non-U.S. citizens. In addition there are millions of people in the United States each day who are non-U.S. persons. For example, Government and academic estimates indicate that there are 9–11 million illegal aliens living in the United States. Both U.S. borders, north and south, are porous by any standard of other nations. Each month over three million foreign people cross through these borders, most with legal right to do so, others not. In the year 2002, more than 27.9 million non-immigrant admissions were counted by the Immigration and Naturalization Service. Many persons stay beyond their legally authorized time. The events of September 11, 2001 clearly demonstrate that some who cross the nation's borders, or have been in the United States for some time (even some of the status of "U.S. persons") have ill intent against the United States.

There is fair evidence that *if* governmental officials, agents and employees *had real-time, meaningful access* on September 10, 11, 2001 to the *knowledge then in governmental files—all* such information being *originally obtained legally, and there was no statutory restriction of which governmental agents could look at it*—the terrorist attacks of September 11 probably could have been prevented.

On September 11, 2001, a serious event happened in the United States which the United States never before had to contend with to the same degree.* Hijackers, all of whom were non-U.S. citizens, some non-U.S. persons, seized control of two civilian commercial passenger aircraft out of Boston, Commonwealth of Massachusetts, flew them into the World Trade Center in New York City, 157 persons aboard were killed, 2,645 persons in the buildings were killed, and over 400 other persons, mainly policemen or firemen, died while heroically attempting to rescue others. Millions of dollars worth of property was destroyed, many businesses and lives of many U.S. persons were, and still are, adversely affected.

Within less than an hour thereafter, hijackers (all non-U.S. citizens, some non-U.S. persons) flew a civilian commercial passenger aircraft, which had taken off from Dulles International Airport, in the Commonwealth of Virginia, into the Pentagon building, killing 64 persons on board, 125 persons in the building. Property damage to the Pentagon building exceeded two hundred million dollars, and lives of many U.S. persons were, and still are, adversely affected. In addition, another such aircraft was seized over Pennsylvania by non-U.S. citizens, some of whom were non-U.S. persons. Apparently some of the innocent passengers courageously, but vainly, fought back. The plane crashed in the Commonwealth of Pennsylvania, killing 46 persons. The best guess is that the hijackers of this aircraft were attempting to fly the airplane either into the White House or into the Capitol.

It bears repeating that in each event, some of the hijackers were non-U.S. residents, some were in the United States illegally, some were U.S. residents, all were non-U.S. citizens, the names of just about all were in data files in the United States.

Such attacks had never happened before in the United States, seldom elsewhere in the western world. When nation-states plan to attack another nation-state, usually there is some advance notice. We see armies, navies building up, equipment and uniformed human beings being moved. Here, while history might ultimately reveal that one or more nation-states were somehow involved, in the main the wrongdoers were nonstate actors, not nation-states.

* On February 26, 1993, about ten non-U.S. citizens, hoping to murder as many as 250,000 people, did try to knock down the World Trade Center by driving a truck loaded with explosives into it. Seven U.S. persons were killed and more than 1,000 were injured.

After the tragic events, when the names of the hijackers, by diligent research of Government records and other databases, became known, knowledge and facts were produced from Government and third person files once the names of the terrorists were know, which, if agents had known before the event, probably could have enabled them to have prevented the hijackers from boarding the planes, thus avoiding the purposeful crashes.

The highest duty of the officials of any nation-state, even in a free, open democracy with constitutional protection with respect to certain fundamental rights, and with a consensus that lesser privileges also should not be unreasonably intruded upon, is to protect the security of that nation and its people from outside threats.[301] Thus the public ought to appreciate and respect that responsible Government officials, agents and employees are trying to develop ways in which Government's officials, agents and employees get pre-notice in real time in an informative, useable way, free of clutter, and thus can thwart future such tragic events. Mr. Justice Jackson reminds us that the Constitution is not a suicide pact.[302] And as the Framers expressly recognized in the Federalist Papers, the "[d]ecision, activity, secrecy, and dispatch" that are the hallmarks of unitary executive power are "essential to the protection of the community against foreign attacks."[303]

Today the United States has over 150,000 U.S. military persons fighting in Afghanistan and Iraq, plus significant air force, marine, and naval forces around the same area, in addition naval personnel are at seas and oceans throughout the world intercepting ships carrying illegal items, some of which will yield cash to supply terrorists, others carrying items which can be used in assembly of weapons of mass destruction. In addition, there are CIA and other civilian U.S. personnel risking their lives each day to corner terrorists and prevent attacks on the United States, or U.S. facilities abroad, or on its allies. Recent news stories say that what led the leader of Libya to permit inspections of its possible weapons of mass destruction facilities and programs was that the U.S. and its allies had intercepted, as the result of intelligence gathered, a ship carrying parts for such facilities to Libya. Everyone agrees that obtaining accurate, quick, live intelligence in real-time, informative ways is often as invaluable as actual combat with the terrorists. No public official, public employee or agent would have other than a rough time living with himself or herself if it turned out there was information available, including personal information legally in Government files, with no restrictions on use, of which he or she did not avail himself—or herself—which caused a tragic act on American soil, facilities or U.S. persons, home or abroad, or allies.

The Secretary of Defense's responsibilities clearly include helping to find terrorists before they act. Once they act, if they are not U.S. military personnel or enemy combatants, the prosecution is generally by the U.S. Department of Justice. In the course of discharging his important task, the Secretary of Defense, not the President of the United States and not the Attorney General of the United States, formed our committee and asked it for advice on an important aspect of his mission, *to wit.,* how DARPA was performing its tasks with respect to seeking better means to make more, useable sense of data in real time which the Government already had in its possession legally, or would get legally, and to consider the relevant privacy issues in respect thereto.

This leads to DARPA.

There is an agency in the Department of Defense known as the Defense Advanced Research Agency (DARPA), created in 1958 in President Eisenhower's Administration in response to the trauma of Sputnik. The agency's responsibility is to start up and begin to develop, free from political interference, new ways of doing things from theories, intelligent imagination and guessing and hopes to technologies which work—so as to make the Defense Department or other

agencies of the federal Government, and perhaps also state and local governments, even more protective of the Nation's security. DARPA, one writer said: "is a total anomaly in our Government or any other. Creative by nature, revolutionary in its imagination like the brain at the beginning of the future. For some of them, the future begins with the gnawing awareness of a gap with the awareness that something is missing, that something could be better, that there's something the generals want and don't have yet."

DARPA uses its own highly skilled personnel, but it also seeks out universities and other scientific, intelligence and engineering experts to help it develop new ideas, new technologies which work. As I understand it, once such technologies are developed, DARPA does not operate such new equipment or other techniques. Instead, they get put into one or more of the operating agencies of the Department of Defense or other agencies of Government. Among the worthy ideas that got its start this way is ARPANet, the precursor of the Internet as a technological tool for linking defense researchers. DARPA, among many other projects, is working on a robotic human prosthesis that will control the injured person's actions by only human thought, and other technologies which will permit a soldier to survive in changing environments. It is also involved in creating technologies which will overcome the fact that few Americans read Farsi or other languages spoken and written in the Middle East. Such technologies have already resulted in a 95% accurate translation into English and in real time. The American people would marvel at other advancements in technology and results in which DARPA has so far played a significant role. And with vast amounts of data, technologies are needed to combine such data and get the really relevant data to the appropriate persons in real time in a significant, meaningful way, while eliminating the irrelevant or the redundant.

In early 2002, DARPA, as part of such efforts, began to do research for the development of a program known as Terrorist Information Awareness (TIA).* As I understand it, TIA is an attempt to develop advanced information technologies which will take information already legally collected by the Government, or that a third person had legally turned over to the Government, and see if it is possible to find certain patterns or connections in the data so as to predict persons who may be involved in future terrorist plans. It, *inter alia,* attempts to develop technologies, equipment and programs which "connect the dots" and to do it in real time certain. It bears repeating that (1) all of the information used by TIA is already in the hands of the Government by legal means,[304] (2) there is no statutory restriction which caused the person to file the information with the Government on its use by the Government, (3) TIA is not collecting new information, (4) part and parcel of the plan in the DARPA research was to develop mechanisms to avoid unreasonable invasion of privacy, (5) such information was being analyzed not to use to convict someone of a crime, but to prevent future acts of terrorism, and (6) such tools, when developed and before put into production would be turned over to another part of the Government for production and operation. Some of what TIA would develop would be technologies which, because of the speed and breadth of access to data already in Government or private files legally turned over to the Government might be within the phrase "data mining." But a lot of the TIA program did not fit such description.[305]

The TAPAC report, however, immediately jumps on, and concentrates on, "data mining,"[306] although, as I understand it, much of the TIA research program, as stated above, would not by any stretch of the mind be described as "data mining." Also, "data mining" is done every day

* When first announced to the public, the program was entitled "Total Information Awareness." The title was changed to "Terrorism Information Awareness." (TIA) in May 2003. Obviously, the original title caused some to think Orwell, *1984*.

by many of the nation's most respected businesses. The report recognizes that many private companies do data mining, but citing the Markle report, the committee suggests that it is worse when the Government does it.[307] Apparently, the Attorney General of the United States does not find such distinction a valid one.[308] I also have some difficulty with the distinction. Perhaps I am still misled by the fact that in my youth my parents taught me that policemen on the beat and other law enforcement officers are friends, not enemies, and in my life, most often, it has turned out that way. Today, because of selection, training, supervision, and press scrutiny, police, FBI agents, and security agents are far from what they were in colonial days. This, of course, does not mean there is never fault by such, but to compare it with the King's colonial days is like comparing the early automobile to today's cars. Also, I find it hard to have less confidence in the security people and their respect for privacy, who worked over the Christmas and New Year's holidays defending the nation's security than in some of the private employees who have worked for private companies. Also, I find it hard to say that a person's privacy is invaded when a Government agent, seeking to avoid a terrorist attack, sees many innocent persons' names on an aircraft's passenger list among others, as against when an employee of a private company sees the same person's name on a shopping list and decides to call him or her during the evening meal to solicit a subscription.

As correctly stated by the report, the concerns developed by certain editorial critics or some members of Congress centered on the possible use by Government of personal information on U.S. citizens and permanent residents ("U.S. persons") without their knowledge or consent, even though (and the report does not point this out): (1) that personal information had been lawfully collected by public or private entities, (2) such information had originally come into the Government's possession by legal and constitutional means, (3) most, if not all, was willingly filed with the Government by the persons whose names are in the list, and (4) there were no statutory restrictions on its use. The report, in fact, states that "[t]he common feature of all of these programs is that they involve shifting through data about identifiable individuals, even though those individuals have done nothing to warrant Government suspicion, in research of useful information. This is what we understand to be 'data mining.'"[309] This—with all due respect—misstates the "common feature of all these plans . . ." Actually the difficulty is caused by the fact that the information relevant to the terrorist is in the same data as that of other persons who are perfectly innocent. In other words, the few possible terrorists' names are interwoven with the overwhelming number of innocent persons.* For, in this war, the nation's enemies often are attempting to carry out attacks within the United States and often conceal themselves among the innocent civilian population, and use civilian facilities in order to do so or in order to obtain money and skills to do so.

The TIA program soon got into trouble with the Congress. Also, some respectable writers who cover various departments of the federal Government commented adversely about the TIA program.

In February 2003, Secretary of Defense Donald Rumsfeld appointed two committees to address these and other concerns about TIA. One is the

* No doubt today the name of every person is on the list of those who board U.S. commercial planes for a flight. Every non-U.S. citizen's name is on the list of such who go through immigration after landing in the United States. Now the U.S. is in the process of getting foreign carriers and their governments to agree that at least one hour before takeoff for the United States the United States must receive the name of every person—foreign and U.S.—on such aircraft. The Government having obtained all those names legally, the American people would be critical if the Government did not have in place an effective process to look at the entire list for possible terrorists. Sometimes in looking at the entire list the Government can pick "in lieu of names," also people who live in the same house as the terrorist whose name is also on the same passenger list. Such might cause the would be terrorist to be excluded from the flight.

Internal Oversight Board, to establish "policies and procedures for use within the DOD of TIA-developed programs and procedures for transferring these capabilities to entities outside DOD . . . .in accordance with existing privacy protection laws and policies."

Ours is the other committee. It is known as the Technology and Privacy Advisory Committee ("TAPAC"). TAPAC is charged by the Secretary of Defense with examining "the use of advanced information technologies to help identify terrorists before they act." The report accurately describes the members of such committee, their backgrounds and the helpful, brilliant and tremendous work of the staff led by Fred H. Cate and Lisa A. Davis.[310] We and the Nation owe each a debt of gratitude.

TAPAC was requested by the Secretary of Defense to answer four questions:

1. Should the goal of developing technologies that *may help identify terrorists before they act* be pursued?
2. What safeguards should be developed to ensure that the application of *this* or *any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy?*
3. *Which public policy goals are implicated by TIA and what steps should be taken to ensure that TIA does not frustrate those goals?*
4. How should the Government ensure that the application of *these technologies* to global databases respects international and foreign domestic law and policy? (Italics supplied.)[311]

The report—and I agree—states that the Secretary of Defense should be thanked and complimented by the American people for being so far the only head of a Department to set up a committee to review the privacy implications of the development and use of the emerging information technologies, even those which on occasion set forth personal information.

The TAPAC report, in the main, with a few changes, fairly describes what happened when the existence of the TIA program first came to Congress and other public knowledge, so I have put that part of the TAPAC report[312] in my views and recommendations in quotes with my few suggested changes italicized, or where words in the report are dropped, a bracket. Citations to footnotes have been omitted without notice. Also, the chart on page 15 of the report is not reproduced, but it is incorporated by reference in this statement.

"TIA and [ ] *Certain* Government Programs Involving Data Mining

Early Descriptions of TIA

"TIA was first cited publicly *on* April *10,* 2002 by the Director of DARPA, *Dr. Tony Tether* in testimony before the Senate Armed Services Committee. In May, *2002* the newly created DARPA IAO described TIA on its website. The program first attracted significant public notice after an August 2002 speech by the then-Director of *DARPA* IAO, *Admiral John Poindexter*. Speaking at the DARPATech 2002 Conference, he described the need to become 'much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options.' To accomplish these purposes, he articulated the need for a 'much more systematic approach.' 'Total Information Awareness—a prototype system—is our answer.'

"The *DARPA* IAO Director went on to identify 'one of the significant new data sources that needs to be mined to discover and track terrorists'—the 'transaction space.' 'If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space.' He then showed a slide of transaction data that included 'Communications, Financial, Education, Travel, Medical, Veterinary, Country Entry, Place/Event

Entry, Transportation, Housing Critical Resources, and Government' records.

Early Public and Congressional Reaction to TIA

"The IAO Director mentioned the importance of protecting privacy in his speech. [ ] *In fact*, six months earlier, in March 2002, IAO had begun funding research on *privacy-enhancing technologies.* Nevertheless, *at least some felt already* the seeds had been sown for serious concerns about privacy. On November 24, 2002, at the height of the debate over enactment of the Homeland Security Act, William Safire wrote a column in the *New York Times* critical of TIA. Safire wrote:

> 'Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as 'a virtual, centralized grand database.'
>
> 'To this computerized dossier on your private life from commercial sources, add every piece of information that Government has about you—passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the FBI, your lifetime paper trail plus the latest hidden camera surveillance—and you have the supersnoop's dream: a 'Total Information Awareness' about every U.S. citizen.'

"Although DARPA officials and others argued that Safire misstated facts about TIA, his criticism sparked a [ ] *significant* reaction. In the seven months between the initial disclosure of TIA and Safire's column, only 12 press reports had appeared about the program. In the next 30 days, the press carried 285 stories." [ ] By the time TAPAC was created, that figure had risen to 508.

"In December 2002, the Assistant to the Secretary of Defense for Intelligence Oversight, who is responsible for ensuring DOD compliance with the laws and regulations governing the collection and use of intelligence information, conducted an internal review of TIA and related programs. The review included not just DARPA, but other units within DOD and the armed services, (*departments of DOD*) and The Rand Corporation, a DARPA contractor.

"The review found that neither DARPA nor IAO are 'intelligence organizations,' because they develop but do not use technological tools for information gathering. Nevertheless, the review noted that the same legal constraints that regulate intelligence activities involving data on U.S. persons would apply to the use of TIA by any part of the Defense Intelligence Community to 'collect, retain, or disseminate information' on U.S. persons. The review concluded that no legal obligations or 'rights of United Sates persons' had been violated.

"The review did determine, *however*, that some DARPA officials, because they were not, *and had not been*, involved in intelligence activities, had only a 'limited understanding of Intelligence Oversight regulations.' As a result of the review, DARPA 'Quickly took Intelligence Oversight concerns into account' and 'institutionalized' training and awareness of Intelligence Oversight for its personnel. The review remains open and the Assistant to the Secretary of Defense for Intelligence Oversight has committed to engage in 'ongoing monitoring' so long as DARPA is involved in developing tools for intelligence gathering.

No one has contested the conclusion stated in the last sentence of the preceding paragraph.

"Opposition to TIA, however, continued to mount. In late 2002 Senators Charles E. Grassley (R-Iowa), Chuck Hagel (R-Neb.), and Bill Nelson (D-Fla.) wrote separately to the DOD Inspector General asking him to review TIA. On January 10, 2003, the Inspector General announced an audit of TIA, including 'an examination of safeguards regarding the protection of privacy and civil liberties.' As discussed below, the audit concluded that '[a]lthough the DARPA development of TIA-type technologies could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility for governmental abuse of power and to help ensure the successful transition of the technology into an operational environment.'

"On January 23, 2003, the Senate adopted an amendment to the Omnibus Appropriations Act proposed by Senator Ron Wyden (D-Ore.) prohibiting the expenditure of funds on TIA unless the Secretary of Defense, the Director of the CIA, and the Attorney General jointly reported to Congress within 90 days of the enactment of the law about the development of TIA, its likely efficacy, the laws applicable to it, and its likely impact on civil liberties. The amendment also prohibited deployment of TIA *for actual operation* in connection with data about U.S. persons without specific congressional authorization. Congress adopted the amendment as part of the Consolidated Appropriations Resolution on February 13, and the President signed it into law on February 24.

May 20, 2003 DARPA Report

"The *DARPA* report [ ] *required* by the Wyden Amendment was delivered to Congress on May 20, 2003. It divided DARPA's IAO programs into three categories—TIA, High-Interest TIA-Related Programs, and Other IAO Programs—and described the latter two categories in far greater detail than TIA itself. The report described TIA as:

> 'a research and development program that will integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and *privacy protection technologies* into an experimental prototype network focused on combating terrorism through better analysis and decision making.'

"In addition, the report described eight other 'High-Interest TIA-related Programs' being developed by the IAO in connection with TIA, and ten 'Other IAO Programs' that may provide technology as possible components of TIA prototype but are considered of secondary interest within the context of this report.'

"With regard to the privacy issues posed by TIA and related programs, the *DOD* report *to Congress* provided:

> 'The Department of Defense's TIA research and development efforts address both privacy and civil liberties concerns in the following ways:
>
> - The Department of Defense must fully comply with the laws and regulations governing intelligence activities and all other laws that protect the *privacy and constitutional rights of U.S. persons.*
> - As an integral part of its research, the TIA program itself is seeking to develop "*new technologies* that will *safeguard the privacy of U.S. persons*.
> - TIA's research and testing activities are conducted using *either* real intelligence information *that the federal government has already legally obtained*,

or *artificial synthetic information* that, ipso facto, does not implicate the privacy interests of U.S. persons.'*

Congressional Response

"On September 25, 2003, Congress passed the Department of Defense Appropriations Act, 2004. Section 8131 of the Act terminated funding for TIA, with the exception of 'processing, analysis, and collaboration tools for counter-terrorism foreign intelligence' specified in a classified *secret* annex to the Act. Under the Act, those tools may be used only in connection with 'lawful military operations of the United States conducted outside the United States' or 'lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens." *(Note: The Act does not say wholly against "non-United States persons," it says "wholly against non-United States citizens.")*

"In its report accompanying the Act, the Conference Committee directed that the IAO itself be terminated immediately, 'but permitted continuing research on four IAO projects: Bio-Advanced Leading Indicator Recognition, Rapid Analytic Wargaming, Wargaming the Asymmetric Environment, and Automated Speech and Text Exploitation in Multiple Languages.' The Act thus terminated the IAO and further research on privacy enhancing technologies, while keeping open the possibility of 'processing, analysis, and collaboration tools for counter-terrorism foreign intelligence' being developed outside of DARPA in secret. The President signed the Act on September 30, 2003.

Inspector General's Report

"On December 12, 2003, the DOD Inspector General released the results of an audit of TIA announced in January in response to Congressional inquiries. The audit concluded that '[a]lthough the DARPA development of TIA-type technologies could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility for governmental abuse of power and to help ensure the successful transition of the technology into an operational environment.'

"With specific regard to privacy, the audit found that DARPA failed to perform any form of privacy impact assessment, did not involve appropriate privacy and legal experts, and 'focused on development of new technology rather than on the policies, procedures, and legal implications associated with the operational use of technology.' The report acknowledged that DARPA was sponsoring 'research of privacy safeguards and options that would balance security and privacy issues,' but found that such measures 'were not as comprehensive as a privacy impact assessment would have been in scrutinizing TIA technology.'

"'As a result,' the audit concluded, 'DOD risk[ed] spending funds to develop systems that may not be either deployable or used to their fullest potential without costly revision.' The report noted that this was particularly true with regard to the potential deployment of TIA for law enforcement: 'DARPA need[ed] to consider how TIA will be used in terms of law enforcement to ensure that privacy is built into the developmental process.'

Understanding the TIA Controversy

"Many factors have contributed to the controversy over TIA. One of the most important was DARPA's inability—or *perhaps* unwillingness—to describe TIA, its objectives, and the data to

* This bullet (the third bullet), see also infra p. 80 (separate statement of William T. Coleman, Jr.), seems to contradict any suggestion that TIA research was using any personal information of U.S. persons other than that permitted by *United States v. Miller*, 425 U.S. 435 (1976) and *Whalen v. Roe*, 429 U.S. 589 (1977).

which it would apply clearly, consistently, and coherently. For example, DARPA's May 2003 report described TIA in these words:

> 'TIA research and development efforts seek to integrate technologies developed by DARPA (and elsewhere, as appropriate) into a series of increasingly powerful prototype configurations that can be stress-tested in operationally relevant environments using real-time feedback to refine concepts of operation and performance requirements down to the technology component level.'

"The changing and inconsistent descriptions of TIA have been documented. In August 2002, DARPA's descriptions of TIA focused on 'significant new data sources that [need] to be mined to discover and track terrorists' and 'transactional data' found in 'Communications, Financial, Education, Travel, Medical, Veterinary, Country Entry, Place/Event Entry, Transportation, Housing, Critical Resources, and Government' records. By 2003, all such references had been removed from TIA materials, the diagram depicting them had been removed from TIA's website, and in DARPA's May 2003 report to Congress, data mining was not even mentioned.

"Similarly, when the IAO Director presented TIA to the DARPA Tech 2002 Conference in August 2002, he told his *civilian* audience that '[t]he relevant information extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task.' The diagram accompanying his presentation and available on TIA's website until early 2003, referred to 'Automated Virtual Data Depositories' and depicted 'Transactional Data' flowing into those depositories. The phrase 'virtual, centralized grand database' has been widely quoted from DARPA documents. But in its May 2003 report to Congress, DARPA wrote that 'the TIA Program is not attempting to create or access a centralized database that will store information gathered from various publicly or privately held databases.'

"In that same report, DARPA described 'How TIA Would Work' in terms of 'Red Teams'

> 'imagin[ing] the types of terrorist attacks that might be carried out against the United States at home or abroad. They would develop scenarios for these attacks and determine what kind of planning and preparation activities would have to be carried out in order to conduct these attacks. . . . The red team would determine the types of transactions that would have to be carried out to perform these activities . . . . These transactions would form a pattern that may be discernable in certain databases to which the U.S. government would have lawful access.'

"The government would then identify those specific patterns that 'are related to potential terrorist planning.' Rather than trying to prevent terrorist attacks by searching databases for 'unusual patterns,' intelligence agencies would 'instead [search] for patterns that are related to predicted terrorist activities.' This explanation is the sole description of how the TIA program would work in DARPA's May 20, 2003 report to Congress.

"Clearly, the objectives of programs may change or one official may describe a program differently than another, but DARPA's failure to acknowledge or explain significant inconsistencies contributed to undermining public and Congressional confidence in the agency. DARPA exacerbated the controversy over TIA in other ways as well.

"For example, the TIA logo on the IAO website, depicting an all-seeking eye atop a pyramid, surrounded by the Latin motto '*Scientia Est Potentia*'—Knowledge Is Power—suggested George Orwell's all-knowing 'Big Brother' government in his classic novel *1984*. Changing the name from 'Total' to 'Terrorism' Information Awareness after the controversy

erupted, as if the title rather than the potential substance of TIA was the problem, did not help.

"Controversy over other IAO projects, such as the planned FutureMAP program, helped to fuel Congressional skepticism. FutureMAP involved the creation of an Internet-based futures market in which traders could bet on the occurrence and timing of events such as terrorist attacks, assassinations, and the like. Although similar markets are used in commercial settings today for purposes as diverse as predicting the weather affecting Florida orange crops and estimating the success of a forthcoming Hollywood movie, the subject matter of FutureMAP and the perception that it was both ill considered and unseemly caused an outcry so great that DoD terminated further consideration of the program and the director of IAO ultimately resigned.

"Other factors beyond DARPA's control contributed as well. As a research agency charged with developing, but not implementing, technological tools, DARPA was unprepared to answer critics' questions about the privacy implications of how TIA might be used. Historically, DARPA had engaged in high-risk, high-pay-off research for the DOD, conducted out of the limelight. Much of its research has resulted in spectacular advances, with benefits far beyond the defense establishment—for example, DARPA created DARPANet, the precursor to the Internet, as a technological tool for linking defense researchers—but never before had the agency been required to account for the potential impact on privacy of future uses of a tool it was in the process of developing.

"This led to sustained miscommunication between DARPA and its critics. DARPA answered questions about privacy by repeatedly assuring the public that *it* was not aggregating personally identifiable information on U.S. persons or using TIA to access any such information, and that any such activities in the future would be by *other agencies* which would bear responsibility for complying with the laws and regulations applicable to *them.* Some observers found these responses evasive especially in the light of DARPA's public rhetoric promoting TIA. *Although the Assistant to the Secretary of Defense for Intelligence Oversight found no evidence that TIA was at any time using personally identifiable information on U.S. persons, DARPA's assurances failed to resolve critics' concerns.*

"The timing of the release of information about TIA also contributed to the controversy surrounding the program. [ ] *Some* Americans were growing increasingly uneasy about government actions, in the aftermath of the September 11, 2001 terrorist attacks, that appeared to threaten civil liberties: the detention of non-U.S. persons without charge or access to counsel,* monitoring of inmate telephone calls with their attorneys, passage of the USA PATRIOT Act with the new powers it conferred on the government to conduct—in some cases secret—searches and seizures, physical searches of airline passengers and their luggage, and the Attorney General's Operation TIPS program (later abandoned) under which delivery, repair, and other workers who entered people's homes would report to the government on what they saw there. Moreover, news of TIA was breaking during the fall of 2002, just as Congress was debating the Homeland Security Act, with the goal of centralizing many of the government's surveillance programs within a new Cabinet-level department. All of this coalesced to heighten concerns among legislators and members of the public to the potential threat of government use of personal data."[313]

The other members of TAPAC conclude:

> Another significant contributor to the controversy was DARPA's failure to build protections for privacy into TIA technologies as they were being developed.

* The Supreme Court of the United States on January 9, 2004 denied petition for a writ of certiorari in a case where the Court of Appeals for the District of Columbia has not found such practice illegal. *Center for National Security Studies v. Dep't of Justice,* 331 F.3d 918 (D.C. Cir. 2003, cert. denied 03-472, Jan. 9, 2004.

> We recognize that DARPA had underway separate initiatives to develop privacy-protecting technologies, but these were not part of the TIA tools that DARPA was demonstrating in 2002 and 2003. As the Inspector General noted, these research projects "were not as comprehensive as a privacy impact assessment would have been in scrutinizing TIA technology."
>
> Informational privacy is respected and meaningful policy oversight guaranteed only when they are made a central part of the technology development process and when the tools necessary to ensure them are developed as an integral part of writing software and building systems. DARPA failed, in the words of the Inspector General's report, "to ensure that privacy is built into the developmental process." DARPA was by no means unique in its failure to do this, but that failure ultimately contributed to the elimination of TIA. . . .[314]

I do not join with the above quoted conclusion of our Committee, or what is in the executive summary in a similar vein.[315] For, as I review the evidence and read the material, I think failure came about because the Congress did not really understand the TIA program and did not appreciate that it was a research venture rather than the use, operation and application of what such research showed would be worthwhile to develop, produce and put into use by others. Congress ignored that privacy issues and protection thereof were also being considered by TIA and DARPA in the research. This in part occurred because DARPA did not explain the project to Congress in the informing way one would expect of DOD. To that extent, DARPA is at fault. One should also recognize, however, that there is a secret Appendix attached to the Congressional act. While the act outwardly rejected TIA, there is a great possibility nevertheless that some of the program survived by Congressional consent. Indeed it is striking that, at the same time that Congress was taking the limitation action with respect to DOD, the same Congress in Section 201 of the Homeland Security Act, signed into law in November 2002, was requiring at the same time DHS "to establish and utilize . . . . a secure communications and information technology infrastructure, including data mining and other advanced analytical tools" to access, receive, and analyze data, detect and identify threats of terrorism against the United States. In addition, there were other statutes also enacted around the same time which authorized and in some cases directed the collection and analysis of data of U.S. persons. The TIA program, moreover, in fact did consider the privacy issues.[316] Perhaps the involvement of Admiral John Poindexter in the TIA programs, who had a previous controversy with the Congress when he was President Reagan's National Security Adviser, had something to do with the negative action of the Congress.

Thus, I cannot support the conclusion that failure to recognize privacy issues and deal with them should have been the basis for the Congressional action. I thus do not join the second paragraph of the TAPAC report under the heading of *TIA and the Secretary's Questions to TAPAC*,[317] or similar statements in the executive summary.[318] I would rewrite such paragraph as follows to state almost the opposite:

TIA was and is a worthwhile effort to achieve worthwhile ends. Its presentation was flawed, by Congress' insensitivity to DARPA's attempt to show actual inclusion of critical privacy issues in its research and flawed by its failure to emphasize even more that privacy issues were being considered. A division of DARPA thus stumbled in its handling of TIA, for which the Agency unfortunately has paid perhaps a significant price in terms of its credibility in Congress. Congress also stumbled in that it failed to see the basic value of what TIA was assigned and attempting to do, and that it never clearly recognized that DARPA and other parts of DOD understood the necessity to address the privacy issues and DARPA and DOD were doing and would do

even more with respect to privacy before any program went into actual operation. This Congress-DARPA failure comes at a time when DARPA's historically creative and ambitious research capacity is more necessary than ever. By maintaining its focus on imaginative, far-sighted research, at the same time it takes account of informational privacy concerns, DARPA will rapidly regain its bearings. It is in the best interest of the Nation for it to do so. Congress must regain and appreciate the value of such an asset to this Nation. It is in the best interest of the Nation for it likewise to do so.

My basic difficulty, however, is that the report talks mainly about "data mining" in the broader sense,[319] thus putting databases where the U.S. person has willingly supplied the data to the Government or a third person (and that person has willingly given it to the Government) in the same category as when the Government obtains the data by another method.* Even more basic, the report attempts to wrap the ringing words of "liberty," free speech and "general search" around the concept of privacy,[320] and thus it uses precedents applicable to these concepts to reach conclusions regarding privacy issues not supported in law,† and would be a hard excuse to those who in the future suffer hard personal losses. The TAPAC report in several places suggests that the Fourth Amendment prevents the Government from looking at data which a U.S. person previously has filed willingly with the Government or willingly filed with a third person who has then willingly turned it over to the Government. The report puts it under the rubric of "Protection Against Government Disclosure of Personal Matters" or "informational privacy." The report summarizes the state of constitutional law as follows: "The Supreme Court has interpreted the Fourth Amendment, as well as other constitutional provisions, to provide varying degrees of protection to informational privacy when the Government engages in surveillances or searches or seizes personally identifiable information."[321] With all due respect, this is incorrect. First, this is not what TIA was about, and even when the inquiry becomes all types of data mining, case law does not support such a broad conclusion. The Supreme Court of the United States has rejected the notion that there is a constitutional privacy right when the person willingly has given the information to the Government, or a third person who then willingly gives it to the Government. In addition, there is no seizure or search in actual fact or within the prohibitions of the Fourth Amendment when the individual not only is not present and the material is not in his or her dwelling or on other property he or she controls, or when the Government wishes to look at a document for security purposes which

* The report's definition of "data mining" does not give an escape hatch to information willingly given to the government by the individual. See supra pp. vi, 4 n. *, 46, 48.

† In fact, the report concedes:

> Professor Daniel Solove has summarized the Court's logic: "since information maintained by third parties is exposed to others, it is not private, and therefore not protected by the Fourth Amendment." Congress reacted to the decision by enacting a statutory right of privacy in bank records, but this logic has served as the basis for another important exclusion from the protection of the Fourth Amendment: information about (as opposed to the content of) telephone calls. The Supreme Court has found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, when the call was placed, the duration of the call, etc.), because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call. "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."
>
> . . . . The exclusion from Fourth Amendment protection of information disclosed to (or possessed by) a third party raises significant issues when applied to government mining of commercial databases and other government efforts to aggregate personally identifiable information held in the private sector. Such information, by definition, will be held by third parties, so government use of those data, under the Supreme Court's current interpretations, is unlikely to be limited by the Fourth Amendment, no matter how great the intrusion into informational privacy.
>
> Supra p. 23 (citations omitted).

the individual has already willingly given to the Government or a third person who in turn willingly gives it to the Government.[322] In *United States v. Miller,* the Court said:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly *that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.*[323]

As Daniel Solove wrote: "since information maintained by third parties is exposed to others, it is not private and therefore not protected by the Fourth Amendment."[324] And, in *Whalen v. Roe,* the Court wrote that even if the constitutionally protected "zone of privacy" included "the individual interest in avoiding disclosure of personal matters," strict scrutiny did not apply, and thus a statute could force disclosure of copies of prescriptions for certain drugs to the state.[325] Also much in TIA research was not about data mining, and, even more relevant, all such research used only "either real intelligence information that the federal Government has already legally obtained or artificial synthetic information . . . ."[326]

The report suggests "The Supreme Court has interpreted the Fourth Amendment, as well as other constitutional provisions, to provide varying degrees of protection to informational privacy when the Government engages in surveillance or searches or seizes personally identifiable information,"[327] but never cites or describes such other constitutional provisions. The report, in fact, says only "Most of the provisions that protect informational privacy from intrusion by the Government are statutory, rather than constitutional, in origin."[328] But once again it makes no reference or gives any direction to such constitutional provisions.

My colleagues try to present arguments which support a position that privacy is within the prohibitive provisions of the United States Constitution, even where the Government got the information willingly from the party.[329] They also try strongly to suggest that the governmental issue thereunder are subject to the same type of constitutional analysis as if the governmental issue were free speech, freedom from racial discrimination, freedom from religious discrimination. They do not, however, dispute that the cases referred to in my statement reflect the state of law today. Not I,[330] but the Supreme Court of the United States is the one which has held more than once that where a party willingly files information with a third party or the Government, such filing is deemed to be "willingly" given and the use thereof thereafter by the Government, even for a different purpose, is not an invasion of privacy.[331]

By statute of course, Congress could give such protection,[332] but it has not. When Congress does, TIA would, of course, have to be developed so as to exclude such data obtained by the Government or a third person where there is such a restriction. Likewise, if the data gets into the Government's hands from a foreign government which has restrictions on its use, TIA would have a mechanism for blocking its use.

Thus, as I understand it, what DARPA was trying to do under TIA does not violate the Fourth Amendment and would not be an undue invasion of the zone of privacy of a U.S. person or, even if it were, the standard of "strict scrutiny" of review would not apply, but that of "a rational reason." Most would find it surprising if a court or the American people would conclude a lack of rationality when the public official would look at a passenger list given by the airline willingly to find the names or the pseudonyms of terrorists which are also on the list of many innocent U.S. persons.

The erroneous conclusion of the committee unfortunately leads in part to its requirement of preapproval by the Foreign Intelligence Surveillance

Court[333] as does the committee's thinking about criminal prosecution, not prevention of the terrorist action.[334]

My conclusions to the contrary of TAPAC, of course, do not mean that the Department of Defense should not impose safeguards, for, as Mr. Justice Holmes said somewhere, "To say that a government action is constitutional is the least one can say about it."* Of course there should be restriction on who can look at such personal information, checks to see that it not be misused and there should be a system where there is a record of who used it. Moreover, it would be good public policy to establish a privacy office in DOD which reports to an Undersecretary or higher level at least twice a year, and reports at least once a year to the Secretary of Defense and to a Special Joint Committee of the Congress. But in my judgment the use of a judge or magistrate to get advance permission to call up such information already out of the possession of the U.S. person seems of no necessity. Nor should an annual public report be required. After all, there is no need at this time to educate the terrorist on what steps the U.S. is taking to prevent him or her from attacking the United States. The person cannot claim an invasion of his or her privacy, as the Government already has the information as the result of the person voluntarily filing, or at least such information has already been given to a third person who willingly turns it over to the Government. To get at the file of the terrorist one would also see the names and data of the innocent, also already given willingly to the Government or to a third person who willingly turned it over to the Government, but is this more offensive than the inquiry made 1,000 times a day of the lady's suitcase, with all her personal wear, trying to get at the baggage of the one which has explosives in it?

Those who know me, also know the respect of and confidence I have for and in the other members of TAPAC. Professor Cate, moreover, has been a real professional, brilliant, able, articulate reporter, with his own ideas, but a great feel for what the majority of the committee earnestly believes, and a real talent to put their consensus, fairly into words. He also has had the courtesy and patience to hear out completely my views. Thus, all must appreciate the difficulty I have to disagree. Perhaps it is because I saw the brilliant work of the CIA and other intelligence agencies of our nation when I was a Senior Counselor to the Warren Commission, but later saw, when Secretary of Transportation and thereafter, and even today, the adverse effect on the CIA and other intelligence workers imposed by the

* The point I am trying to make is that: (1) Privacy is not a constitutional right on the same level as race discrimination, etc. (2) In fact, one cannot find in the Constitution any reference to privacy. See supra p. 69 (separate statement of William T. Coleman, Jr.). (3) I concede that as set forth on p. 21 of the report, the word "privacy" is used in some of the opinions limiting restrictions on the sale or use of contraceptives, abortions or in other cases such as marriage, procreation, child-rearing and education, but I rely upon that well respected legal scholar, the late Dean and Professor, John Hart Ely, Jr., though he, like I, do not disagree with the result in most of those cases, finds no basis in any written provision of the United States Constitution. See John Hart Ely, "The Wages of Crying Wolf: A Comment on *Roe v. Wade*," 82 *Yale Law Journal* 920, 928, fn. 58, 60, 943-949, (1972-1973). (4) *United States v. Miller*, 425 U.S. 435, clearly holds that when the person freely and willingly gives the personal information to the Government, or to a third person who freely and willingly gives it to the Government, there is no invasion of privacy if the Government thereafter uses such information. See also *Whalen*, 429 U.S. 589. (5) To the extent Supreme Court cases do use privacy, they make it clear that (a) it is not at the same level as racial discrimination, restriction on liberty, religious restrictions, free speech and political restrictions, only the latter group requiring strict scrutiny, and (b) the Government reasons for invading privacy require only that it have some rational connection with a permissible governmental goal; (c) it bears repeating that the Supreme Court has specifically held that when a U.S. person, including a U.S. citizen, gives information, though personal in nature, willingly to the federal Government or to a third person who willingly gives it to the federal Government, the federal Government can look at that information and use it provided there is no federal statute which limits its use. None of the above means that as a matter of human decency—not that there is otherwise a violation of civil liberties or other constitutional rights or other "American values"—there should not be restrictions on its use, which restrictions I support so long as it is made clear that the restrictions are not required by any federal statute or constitutional provision and do not need the prior approval of a federal judge before use.

Church Committee. Or perhaps it is caused by the fact that when Secretary of Transportation in the Ford Administration I had to deal with hijacking of U.S. commercial aircraft, though fortunately such hijacked planes were not flown into U.S. buildings. (I regret that subsequent Department of Transportation leaders rejected my conclusion that commercial passenger aircraft should not leave the loading gate without the pilot first locking and keeping locked the door to the cockpit. Subsequently someone apparently accepted the pilots' complaint that it restricted their use of the toilet in flight.) Or perhaps it is because I assumed there is real difficulty in getting the foreign airlines to respond as they have, and I feel that some of the committee's recommendations might cause them to insist upon similar provisions. Or perhaps I just have such confidence in the present leadership of the Defense Department and of the Nation that I know they are equally sensitive to privacy issues.*

Perhaps a hypothetical will help analysis:

1. There are 300 Iraqis trained in an Al Qaeda class which graduated in December 1998. The CIA or another U.S. foreign intelligence agency knows the names of all 300. It passes such information to Homeland Security if it then existed.

2. Whenever these people legally or illegally come from abroad into the United States those names, and other information are on airplane records, immigration records and perhaps other records, each freely given by those who enter the United States. On the same lists are the names and other information about thousands of U.S. citizens, U.S. residents, others who fall into the definition of U.S. persons and countless foreigners who come into the United States on the same planes or through the same U.S. gateways for periods of time.

3. Someone in the U.S. Government has picked up information that 19 of those who were in Al Qaeda were planning to hijack a plane out of Boston one day in September, 2001. Such individuals, other than being in the group of 300 graduates in December 1998 are not, at this point, further identified.

4. Through equipment and technology developed by TIA, it is possible to ascertain the names and certain other facts, although not to know which of the 300 were the 19. DARPA has turned the techniques and procedures over to an agency in Homeland Security or another entity in the United States Government. Through processes developed by TIA and now in the hands of an operation agency of the Homeland Security Department, if it then existed, the group of suspects is reduced to 90, some of whom are clearly not terrorists, in fact are lawful students at the colleges and universities in Boston. The entity also knows that the majority of the 90 have been in the United States before, in fact some have legal green cards. It is also known that, separately and independently—having nothing to do with the possible crisis—there are 200 Iraqi graduate students now in Boston colleges and universities who have a meeting at the University of California in early

* Mr. Floyd Abrams writes that the "Bill of Rights is rooted in distrust of government." Supra p. 64 (separate statement of Floyd Abrams). This is a point many recent scholars assert. Sometimes when such point is made I wonder whether the speaker is aware of all the improvements in the security and police forces—much less racial discrimination, much more racial inclusion, better training, more supervision, more rules requiring civilized conduct, more public scrutiny, more newspaper, television, and radio coverage of more investigations. Democracy has to put such trust in its elected leaders or those confirmed by the Senate or else the business of the people can never be done, or, in this case, some of the people's physical being might be actually eliminated, and is it not a mockery to put the daily decisions in the hands of the one who was not elected, has a term existing for life, when the issue is not based on the Constitution or is not a fundamental right or not a civil liberty. The Congressional review process, the constant media process, the election process today are, in my judgment, a much greater deterrent on a public servant than *ex parte* proceedings, in secret, before the Foreign Intelligence Surveillance Court, even though I have great respect and gratitude for what the Court has done over the years.

September. This information is on the same lists and files as those described in paragraph two above. At this point, the operation agency of the Department of Homeland Security says "we cannot narrow the Al Qaeda group of 90 any more but if we could get the names of all persons who had tickets for the plane out of Boston to California, we could stop those with the names which we know were in the Al Qaeda Camp in 1998, when they try to board in Boston on September 11." We also know of the tendency of Al Qaeda-trained persons to use pseudonyms which are in some rhythm with their given names or the Al Qaeda classes such persons were in as this helps the leaders of the terrorist groups to track those actually trained by Al Qaeda. The issue is: Can those names and the entire list be given by the operator of equipment and technology previously developed by DARPA to another governmental agency so that when a person with that name or a pseudonym tries to get on the plane, he or she can be stopped, told not to get on the plane? The person responsible, of course, could say that no Iraqi could take a flight that month or day, but that would be racial profiling. The Fourteenth Amendment (which does not apply to the federal Government) and implicitly the Fifth Amendment (which does) prohibit profiling with respect to race, national origin, ethnicity, or religion. There is no intent at this time to prosecute anyone. When the persons the entity seeks are taken into custody, if he or she is, and thereafter there is a criminal prosecution, none of the above evidence will be used to bring about his or her conviction.*

* My esteemed colleague, Floyd Abrams, writes that President "Franklin D. Roosevelt's incarceration of Japanese-Americans during World War II" was one of the events which showed "our nation's record has not been admirable at resisting the primal instinct of shutting up dissenters and shutting down civil liberties during times of stress." Supra p. 63 (separate statement of Floyd Abrams). What DARPA is attempting to do here in TIA comes nowhere near what he accuses President Franklin D. Roosevelt of doing, but even more important, such comment fails to reflect that in *Hirabayaski v. United States*, 320 U.S. 81 (1943), what the Government did was to provide a curfew in parts of California for persons of Japanese descent and in *Korematsu v. United .States*, 323 U.S. 214 (1944), what the Government did was to exclude Japanese from certain defined areas. Of course, by today's standards, an American President probably would not do that, see supra pp. 2, 18, 68 (separate statement of William T. Coleman, Jr.), but, in fairness to President Roosevelt, one should point out that the Attorney General of California who requested the curfew was Earl Warren, whose record, before and after, certainly does not put him in the class of one who "shut [ ] down civil liberties." Also, the Secretary of War, who signed the request, was Mr. Henry L. Stimson, who was such a civilized man that when he was earlier Secretary of State in the Hoover Administration, he closed the Department of State's code breaking office in 1929, saying that "Gentlemen do not read each other's mail." But Mr. Stimson, when Secretary of War, after the Japanese sneak attack on Pearl Harbor, after press reports and evidence that Japanese people living in Hawaii as civilians for years had driven their trucks down the runways at Hickam Field in Hawaii, destroying U.S. military planes, after rumors that Japanese submarines lay off the immediate coasts of California, and after the duplicity of the Japanese Ambassador calling upon Secretary Hull at the moment of the attack, Mr. Stimson decided such action had to be taken. This was the same human being who, when U.S. Attorney for the Southern District of New York, often would require attorneys in his office to go along with the FBI agents to make sure they did not violate the Fourth Amendment when doing search and seizures under a warrant duly issued by a federal judge. Of course, the acts done in 1942-43, measured by today's standards, were wrong, but it was at a time when those of color whose ancestors in the Civil War had stormed Lookout Mountain Tenn. and Fort Sumter, S.C., and whose sons or grandsons made up the Quartermaster Corps which helped General Patton get to Berlin from the coast of Normandy in 1943-5, nevertheless were required to go into a segregated Army and often given inferior training. The above is not to say any such actions today would be tolerated, but only to suggest that there were brave men (and now, thank God, also brave women) who were before and after Agamemnon. In addition, those who criticize President Roosevelt should hastily add that the Supreme Court of the United States, after the U.S. Marines, sailors and soldiers began to turn back the Japanese at Iwo Jima and Okinawa and elsewhere, decided *Ex Parte Endo*, 320 U.S. 285 (1944), which held that citizens of Japanese ancestry whose loyalty was conceded could not be held in relocation camps in the midwest. In addition, by 1944 Japanese citizens were volunteering for the U.S. Army and fighting extremely well in Italy and other places in Europe. It takes more than an optimist to say that those trained by Al Qaeda will soon begin to join the U.S. Army and help us fight terrorists. Mr. Justice Frankfurter long ago reminded the Nation that "action is not to be stigmatized as lawless because like actions in time of peace would be lawless." And it bears repeating that the simple issue here involving TIA is whether the Government has the right to look at records freely given it by American citizens in an effort to find also on such lists the names of those who might be terrorists, not to put them in jail, but to prevent a future act of terrorism.

It seems to me that to reveal the names to an operational Government agent under the circumstances outlined above in no way requires as a condition precedent that any governmental official go before a federal judge or magistrate to get permission before revealing the names of all 90, or of all who seek to board such planes out of Boston to California during that time in September to such requesting governmental agency. I also fail to see how the privacy of any of the 90 or, in fact, any on the list is invaded in an unlawful or offensive way.

Or like the events of recent days. U.S. intelligence sources, according to the press from overseas electronic intercepts had picked up "chatter" that terrorists were planning to attack the U.S. using one or more airplanes or by use of a range of devices that included biological or chemical weapons and "dirty" bombs, the terrorists flying out of Paris to the United States. Clearly there are records on file in U.S. agencies of the pilots and other personnel who fly those planes, of the passengers who board these planes, of the employees who work on or about such planes. Some, no doubt, are U.S. persons. The intelligence personnel probably also wished to check in similar fashion U.S. planes and planes of other nations who fly Paris to the United States. Also by now I have every confidence that one or more U.S. agencies have the names of all who trained at flying schools, particularly those who sought to learn only how to fly a plane in the air or to land it on a specific place. Also, by now the U.S. has one or more terrorist lists hopefully by now combined into one master list, constantly brought up to date. I hope by now the U.S. has developed the technologies to explore such information in a meaningful, real time way, also recognizing pseudonyms. Of course on the lists there are many U.S. persons who are completely innocent, have done and plan no wrong. But perhaps mixed in the same list or lists are those who are terrorists and plan to do wrong. Since all names and information was freely given to the various governments by the individuals or, a third party there is no legal reason why the Government can't see those lists for purpose of trying to discover terrorist before they attack. The Constitution does not prohibit such access; there is no federal statute which prohibits such access; if there is a foreign statute that does the technology has been adjusted. There is a public interest that such information be widely available to those whose duty it is to prevent terrorists from acting. As a matter of American values, not constitutional or statutory rules, procedures should be developed to prevent needless invasion of the zone of privacy, as most intelligence and security officers do today even when such procedures are not required by statute.

Of course, DOD might, and should, establish procedures to sure up even more privacy issues, but they need not be, nor should they be, of the sweep suggested by the report.

In the course of the committee's work, it was informed by DOD of many other programs in development in DOD which did attempt to use information technologies to scrutinize personally identifiable data on U.S. persons.[335] All of this information was freely provided by DOD to the committee. In addition, the report correctly sets out the "privacy" risks (and other risks) inherent in the use of such data—*i.e.,* Data Aggregation Risks, Data Inaccuracy Risks, Individual Identification problems, False Positives, Mission Creep, Data Processing Risk, Data Retention. These inherent risks, however, should not be reasons why such technologies should not be developed. Certainly, however, the Department should be urged to use technologies which keep such risks to a minimum such mistakes and misleading information and develop technologies to eliminate as many mistakes as possible as soon as possible. None, however, change the nature of the privacy issues, nor should they lead to the banning of such technologies if otherwise effective with the "privacy risks" kept to the minimum.

The report should point out clearly and forcibly that none of these seven risks should cause

Congress to stop the development of TIA or data mining programs, none of the seven risks should be used by a court as the basis for an injunction against such use.

The report goes on to describe other programs throughout the Government. This performs a great public service, but affords no justification for the TAPAC setting up guidelines for each of them as the agency involved might, if asked, point out differences and other problems. For example, the Department of Justice or the Department of Homeland Security may have, and I feel confident that the Federal Aviation Administration would have, problems with some of the recommendations as written. Likewise, I find it difficult to advise the President that he must by Executive Order, setup a scheme for the whole Government; of course, he and his staff might consider it.

So I would answer the four questions put by the Secretary of Defense to TAPAC as follows:

1 **Should the goal of developing technologies that may help identify terrorists *before they act* be pursued?** (Italics supplied.)

Yes, without qualifications. It will be greatly in the national interest to have such technologies in operation, so by terrorist information awareness and acquisition of knowledge, in real time, with the dots connected and the clutter removed, before terrorists act, the Nation can detect the terrorist and prevent such terrorist from action. It, however, will be in keeping with American values, plus get more affirmative support and understanding from the Congress, the American people and our allies, if the safeguards identified below in Recommendations 2 and 3 can be incorporated into the programs before such technologies are put into actual operation, in fact, as part of the research and development plan. Indeed, DARPA should make clear that such are actively planned as part and parcel of the research programs. Such programs thus will get more acceptance, from the public and the Congress if the safeguards identified below under Recommendations 2 and 3 are developed, and when not inconsistent with national security are publicly identified as part of such technologies.

2 **What safeguards should be developed to ensure that the application of this or like technology, developed with DOD is carried out in accordance with U.S. law and American values related to privacy?**

DOD should appoint a privacy officer who reports to one of the Under Secretaries of Defense, or at least a civilian official of DOD who requires Senate confirmation. There should be frequent reports to the Secretary, no less than twice a year, and there should be a report to a Special Congressional Joint Committee at least twice a year. Such privacy officer should be fully informed of the research and development of such technologies, should be consulted with respect to privacy issues and should have the power to promulgate standards and procedures in re the privacy issues. The need for "a board of external advisors to advise the Secretary, the privacy officer, and DOD officials on identifying and resolving informational privacy issues and on the development and implementation of appropriate privacy protection mechanisms"[336] is unnecessary and, in any event, their terms should end no later than when an administration ends. There is no need for a provision that their terms cannot end before a certain time.[337] They are not to perform an adjudicatory function. My response to question three below suggests appropriate safeguards.

3 **Which public policy goals are implicated by TIA and what steps should be taken to ensure that TIA does not frustrate these goals?**

The most important public policy goal is the safety and security of the Nation. So nothing should be put in the way of developing

technologies which can get to those whose duty it is to protect the nation's inhabitants all information available which will give real time knowledge to them with dots connected, and free of clutter, so as to prevent terrorist attack.

American citizens, in fact, all U.S. persons, however, want minimum intrusion on their zone of privacy and thus safeguards should be built in to the technologies, as research is being developed, but in all events before such technologies are deployed to the operation entity. National security interests should play a role in how and if these safeguards, or parts thereof, should be stated to the public, but, of course, they should be briefed to the Congressional Special Joint Committee. Safeguards should include:

a As the TAPAC report shows, some of the information which the Government has in its files gets there under federal or state statutes or agreements with foreign countries or with private persons or entities with certain specific provisions for its use thereafter. The technologies must be developed to protect and carry out those restrictions.

b The TAPAC report shows some of the risks of imperfection.[338] These observations and warnings are an invaluable contribution to the process. The technology must be developed to keep these risks to a minimum, and when new risks develop, new knowledge and technology, must be developed to get such errors out of the system as soon as possible. But none of these risks are or should become reasons for abandoning such technologies or the search for improvement thereof, or be the bases for enjoining their use by a court.

c The American public does not like the officious intermeddlers—whether a private person or any part of Government—and does not want some of his or her personal affairs known to others, so no one should be authorized, using such DOD-developed technologies, to look through personal files for other than legitimate Governmental reasons that do not conflict with the federal statute which required their production to the Government. So the technology should have a system as part thereof which (i) limits those who can see personal identity data, (ii) records the name and time of entry by those people into the system, (iii) records the reason or reasons for such entry, (iv) records when the entry was over, (v) requires a certificate that the person did not look at the "personal information" data for any other reason, or reasons other than those originally listed without first also recording the subsequent reason or reasons, and (vi) prohibits the looking at the personal records if the statute which required the filing with the Government has such prohibition or specificity for its use.

Violating these rules for access and use should be a serious offense, leading to punishment ranging from oral criticism or reprimand to firing and on some occasions criminal and/or civil penalties.

Certain recommendations made in the report I urge nonacceptance of:

DOD should not be required to file each year a public report. There is no reason to educate the terrorist as to what the U.S. is doing to thwart later actions of terrorism in the United States. In my judgment, the reporting to and supervision by the DOD privacy office and at least twice a year to the Secretary of Defense, and to the Special Joint Committee of the Congress are sufficient. I also urge the Secretary of Defense not to recommend that a search warrant from a federal magistrate or a federal judge is required

before access to such databases.* The DOD's purpose in seeking access is to discover and prevent an attack before it happens. Of course, if there is going to be a criminal proceeding, there should be consultation with the Justice Department before they access data if the evidence obtained is going to be used in a court proceeding. The Department of Justice might advise application to a court before examining data with such mixed purposes.

I would reserve on the recommendation that DOD put a restriction on how to look at publicly available data[339] since the Attorney General of the United States authorizes "online search activity and access [to] online sites and forums on the same terms and conditions as members of the public generally" "for the purpose of detecting or preventing terrorism."[340] I see no reason to add for DOD the requirement of a "written finding by the agency head that the data mining is both necessary and appropriate for the lawful purpose for which the information is being sought."[341]

I would reserve on the recommendations concerning Government data mining throughout the entire federal establishment[342] without first a lot of consultation with other Cabinet officers, other entities, as I think they will raise valid issues TAPAC has not considered.

I feel uncomfortable with any recommendation with respect to criminal prosecution and other courtroom procedures without first discussion with the head of the U.S. Department of Justice, including heads of various divisions, the FBI and other officers of the department who have responsibilities for some of what TAPAC recommends. Likewise, I have every confidence that under the leadership of the Secretary of Homeland Security, Governor Tom Ridge, and others, there is knowledge beyond that of most, if not all, of TAPAC members, thus some of TAPAC recommendation might be inconsistent or unduly restrict what other things are important to the Nation's security and still are consistent with constitutional provisions, civil liberties principles or our American values.

* See TAPAC recommendations to the contrary, supra p. vi.

List of Abbreviations and Defined Terms

ARDA	Advanced Research and Development Activity
"General Crimes Guidelines"	Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations
CAPPS II	Second generation Computer-Assisted Passenger Prescreening System, a TSA project
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
"Data Mining"	Searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government
DHS	Department of Homeland Security
DOD	Department of Defense
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GAO	General Accounting Office
IAO	Information Awareness Office, a former DARPA office
INS	Immigration and Naturalization Service
IT	Information technology
MATRIX	Multistate Anti-Terrorism Information Exchange
OECD	Organization for Economic Cooperation and Development
"OECD Guidelines"	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the OECD Committee of Ministers in 1974
OMB	Office of Management and Budget
SSNs	Social Security Numbers
TALON	Threat Alerts and Locally Observed Notices
TAPAC	Technology and Privacy Advisory Committee
TIA	Terrorism (formerly "Total") Information Awareness, a former DARPA project
TSA	Transportation Security Administration
"U.S. person"	Defined by Executive Order 12333 as an individual who is a U.S. citizen or permanent resident alien, a group or organization that is an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States (except if directed and controlled by a foreign government or governments). Because TAPAC is concerned only with the privacy interests of individuals, the report uses the term to refer only to a U.S. citizen or permanent resident alien.
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

APPENDIX A BIOGRAPHIES OF TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE MEMBERS AND STAFF

TAPAC MEMBERS

Newton N. Minow, Chairman, is Senior Counsel to the law firm of Sidley Austin Brown & Wood. He was a managing partner with Sidley & Austin from 1965–1991. He served as a U.S. Army Sergeant in the China-Burma India Theater in World War II. He served as a Law Clerk to the Honorable Fred M. Vinson, Chief Justice of the United States, and as Assistant Counsel to Governor Adlai E. Stevenson. In 1961, President John F. Kennedy appointed him Chairman of the Federal Communications Commission. Mr. Minow has served as Chairman of the Carnegie Corporation, the Public Broadcasting Service, and The RAND Corporation, and as a trustee of the Mayo Clinic. He is a life trustee of Northwestern University and the University of Notre Dame. He co-chaired the 1976 and 1980 presidential debates and is Vice Chairman of the Commission on Presidential Debates, which sponsors the debates. He has served on numerous presidential commissions. A graduate of Northwestern University, he is the Walter Annenberg Professor Emeritus there, as well as the author of four books and numerous professional journal and magazine articles and the recipient of 12 honorary degrees.

Floyd Abrams is a partner in the New York law firm of Cahill Gordon & Reindel LLP and is the William J. Brennan, Jr. Visiting Professor of First Amendment Law at the Columbia Graduate School of Journalism. Mr. Abrams has argued frequently in the Supreme Court in a large number of its most significant First Amendment cases. He graduated from Cornell University in 1956 and the Yale Law School in 1960. He was a Visiting Lecturer at the Yale Law School from 1974 to 1980 and 1986 to 1989 and the Columbia Law School from 1981 to 1985. He is a recipient of the William J. Brennan, Jr. Award for outstanding contribution to public discourse; the Learned Hand Award of the American Jewish Committee; the Thurgood Marshall Award of the Association of the Bar of the City of New York; the New York Press Club John Peter Zenger Award; the Judge Louis J. Capozzoli Award of the New York County Lawyers Association; the Democracy Award of the Radio Television News Directors Foundation; Ross Essay Prize of the American Bar Association; and many others. Mr. Abrams was Chairman of the Communications Committee of the Association of the Bar of the City of New York; the Committee on Freedom of Speech and of the Press of the Individual Rights Section of the American Bar Association; the Committee of the Freedom of Expression of the Litigation Section of the American Bar Association; and of Mayor Edward Koch's Committee on Appointments. He currently chairs the New York State Commission on Public Access to Court Records.

Zoë Baird is president of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies ("IT") to address critical public needs, particularly in the areas of health care and national security. Since joining the Foundation in 1998, Ms. Baird has developed it into an operating foundation that, in addition to its work in health care and

national security, has been instrumental in working with the governments of the G-8 countries and major developing countries to establish mechanisms to address international IT policy and to enable the use of IT to achieve development goals. Ms. Baird's career spans business, government and academia. She has been senior vice president and general counsel of Aetna, Inc., a senior visiting scholar at Yale Law School, counselor and staff executive at General Electric, and a partner in the law firm of O'Melveny & Myers. She was Associate Counsel to President Jimmy Carter and an attorney in the Office of Legal Counsel of the U.S. Department of Justice. She served on President Clinton's Foreign Intelligence Advisory Board and on the International Competition Policy Advisory Committee to the Attorney General. Ms. Baird is a member of the American Law Institute and served on the Congressional Commission on the Roles and Missions of the Intelligence Community. She serves on a number of private and non-profit boards of directors.

Griffin Bell joined King & Spalding as a partner in 1953 and became Managing Partner in 1958. In 1961, President John F. Kennedy appointed him to serve as a United States Circuit Judge on the Fifth Circuit Court of Appeals. He served as the 72nd Attorney General of the United States from 1977–79. He is a member of the American College of Trial Lawyers, serving as its President from 1985–86. He is also a member of the American Law Institute. Judge Bell was the initial Chairman of the Atlanta Commission on Crime and Juvenile Delinquency. During 1980, he headed the American delegation to the conference on Security and Cooperation in Europe, held in Madrid. In 1984, Judge Bell received the Thomas Jefferson Memorial Foundation Award for Excellence in Law. From 1985-87, Judge Bell served on the Secretary of State's Advisory Committee on South Africa, and in 1989, he was appointed Vice Chairman of President Bush's Commission on Federal Ethics Law Reform. During the Iran Contra investigation, he was counsel to President Bush. Judge Bell graduated *cum laude* from Mercer University Law School in 1948.

Gerhard Casper is President Emeritus of Stanford University and the Peter and Helen Bing Professor in Undergraduate Education at Stanford. He is also a Professor of Law, a Senior Fellow at the Institute for International Studies, and a Professor of Political Science (by courtesy). Professor Casper studied law at the universities of Freiburg and Hamburg, where, in 1961, he earned his first law degree. He attended Yale Law School, obtaining his Master of Laws degree in 1962. He then returned to Freiburg, where he received his doctorate in 1964. He has been awarded honorary doctorates, most recently in law from Yale and in philosophy from Uppsala. In the fall of 1964, Professor Casper immigrated to the United States, spending two years as Assistant Professor of Political Science at the University of California at Berkeley. In 1966, he joined the faculty of the University of Chicago Law School, and between 1979 and 1987 served as Dean of the Law School. In 1989, he was appointed Provost of the University of Chicago. He served as President of Stanford University from 1992–2000. Professor Casper is the author of numerous scholarly books and articles and occasional pieces. From 1977 to 1991, he was an editor of *The Supreme Court Review*. He has been elected to membership in the American Law Institute (1977), the International Academy of Comparative Law, the American Academy of Arts and Sciences (1980), the Order pour le mérite für Wissenschaften und Künste (Order pour le mérite for the Sciences and Arts) (1993), and the American Philosophical Society (1996). Professor Casper serves as a successor trustee of Yale University, a member of the Board of Trustees of the Central European University in Budapest, and a member of the Trilateral Commission. He is also a member of various additional boards, including the Council of the American Law Institute and the Board of the American Academy in Berlin.

William T. Coleman, Jr. is a Senior Partner and the Senior Counselor in the law firm of O'Melveny and Myers. He received his A.B. *summa cum laude* from the University of Pennsylvania and his LL.B. *magna cum laude* from Harvard University, where he was an editor of the *Harvard Law Review*. He clerked for the Honorable Herbert F. Goodrich on the U.S. Court of Appeals for the Third Circuit, and for the Honorable Felix Frankfurter on the U.S. Supreme Court. He was Secretary of the Department of Transportation during the Ford Administration. He is a member of the Executive Committee of the Trilateral Commission, the Council on Foreign Relations, and the Boards of Trustees of the Carnegie Institution of Washington, the Brookings Institution, the Philadelphia Museum of Art (Vice President), and the New York City Ballet, Inc. He was a member of the Board of Directors of the National Symphony Orchestra, a Trustee of the National Gallery of Art, and an Advisory Director of the Metropolitan Opera. He is a former member of the Board of Overseers of Harvard University and of the Boards of Directors of AMAX, Chase Manhattan Bank, N.A., Chase Manhattan Corporation, CIGNA Corporation, IBM Corporation, Pan American World Airways, PepsiCo., Inc., Philadelphia Electric Company, and New American Holdings. He is the author of many scholarly articles and a fellow of the American College of Trial Lawyers, the American Academy of Appellate Lawyers, of the American Law Institute, the American Academy of Arts and Sciences, and of the American Philosophical Association. He served as President and as Chair of the NAACP Legal Defense and Educational Fund. Mr. Coleman has received the French Legion of Honor and the Presidential Medal of Freedom.

Lloyd N. Cutler is a founding partner of the law firm of Wilmer, Cutler & Pickering. He served as Counsel to Presidents Clinton and Carter; Special Counsel to the President on Ratification of the Salt II Treaty (1979–1980); the President's Special Representative for Maritime Resource and Boundary Negotiations with Canada (1977–1979); and Senior Consultant, President's Commission on Strategic Forces (Scowcroft Commission, 1983–1984). He was a member and former Chairman of the Quadrennial Commission on Legislative, Executive and Judicial Salaries, and was a member of the President's Commission on Federal Ethics Law Reform (1989). Mr. Cutler is a graduate of Yale University (B.A. 1936; LL.B. 1939) and was awarded a Yale honorary Doctor of Laws degree in 1983. He also was awarded an honorary Doctor of Laws degree from Princeton University in 1994; the Jefferson Medal in Law at the University of Virginia in 1995; the Fordham-Stein Prize, Fordham University School of Law, 1995; and the Marshall-Wythe medal of the Law School of William and Mary. Mr. Cutler was a founder and Co-Chairman of the Lawyers Committee on Civil Rights Under Law. He has served as Chairman of the Board of the Salzburg Seminar; Co-Chairman of the Committee on the Constitutional System; a member of the Council of the American Law Institute; a trustee emeritus of The Brookings Institution and a member of its Executive Committee; and an Honorary Bencher of the Middle Temple. He also has served as a director of a number of national business corporations.

John O. Marsh, Jr. is a Distinguished Professor of Law at George Mason University, concentrating on cyberterrorism and national security law. He enlisted in the U.S. Army in 1944 and was commissioned a second lieutenant at age 19. He later served in the Army Reserve and the Virginia National Guard, much of his service being in the 116th Infantry Regiment. He graduated from the Army Airborne and Jumpmaster Schools and earned Senior Parachutist Wings. He received his law degree in 1951 from Washington and Lee University and began his practice of law in Strasburg, VA. He was elected to four terms in Congress from the Seventh District of Virginia (1963–71), and

served on the House Appropriations Committee. Choosing not to seek a fifth term, he resumed the practice of law. In March 1973, he returned to federal service as Assistant Secretary of Defense for Legislative Affairs. In January 1974, he became Assistant for National Security Affairs to Vice President Ford, and in August 1974 became Counselor, with Cabinet rank, to President Ford. He chaired the Presidential Committee for the Reorganization of the U.S. Intelligence Community in 1975–76. From 1981–1989, he served as Secretary of the Army; his tenure was the longest of any Secretary in American history. Secretary Marsh has been awarded the Department of Defense Distinguished Public Service Award on six occasions, has been decorated by the governments of France and Brazil, and holds the Presidential Citizens Medal. He was selected as Virginian of the Year for 1990 by the Virginia Press Association and has received the George Catlett Marshall Medal for public service from the Association of the United States Army. He is a member of the advisory council of the Virginia Institute of Marine Science, chairs the advisory committee of Virginia Inland Port, and is a member of the Special Congressional Panel on Terrorism to Assess Federal, State and Local Response to Weapons of Mass Destruction (the Gilmore Commission).

Executive Director and Designated Federal Official

Lisa A. Davis serves as the Executive Director and Designated Federal Official of the Technology and Privacy Advisory Committee. Mrs. Davis was appointed Principal Assistant Deputy Under Secretary of Defense for Industrial Policy on December 3, 2001. Her responsibilities include world-wide industrial base management initiatives, such as E-business solutions, acquisition management improvements, and best business practices. She brings to this position extensive experience in defense contracting and acquisition policy, management, and legislation from positions in the Defense Department, industry, and Capitol Hill. She has negotiated and managed major systems acquisitions for the Army, Navy, and Marine Corps, and has held positions of increasing responsibility in the office of the Secretary of Defense. Mrs. Davis graduated with honors from Ball State University, and earned the title Certified Contracts Manager from the National Contract Management Association/Defense Systems Management College.

Reporter

Fred H. Cate is the reporter for TAPAC. He is a Distinguished Professor and director of the Center for Applied Cybersecurity Research at Indiana University. He appears regularly before Congress, government agencies, and professional and industry groups on privacy, security, and other information law matters. Professor Cate directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities, and was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He is a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams, a member of Microsoft's Trustworthy Computing Academic Advisory Board, and a member of the board of editors of *Privacy & Information Law Report*. He has led projects for the American Enterprise Institute, The Annenberg Washington Program, and the Brookings Institution. He is the author of many articles and books, including *Privacy in the Information Age*, *Privacy in Perspective,* and *The Internet and the First Amendment*. A member of the American Law Institute and a Senator and Fellow of the Phi Beta Kappa Society, he received his J.D. and his A.B. with Honors and Distinction from Stanford University.

APPENDIX B TAPAC WITNESSES

The Hon. E.C. Aldridge, Under Secretary of Defense (Acquisition, Technology and Logistics)

Lieutenant General Keith B. Alexander, Deputy Chief of Staff for Intelligence, U.S. Army

Stewart Aly, Associate Deputy General Counsel, Department of Defense

Maureen Baginski, Executive Assistant Director of Intelligence, Federal Bureau of Investigation

Stewart Baker, Attorney at Law, Steptoe and Johnson, LLP

Jennifer Barrett, Chief Privacy Officer, Acxiom

Jerry Berman, President, Center for Democracy and Technology

John Brennan, Director, Terrorist Threat Integration Center

Scott Charney, Chief Trustworthy Computing Strategist, Microsoft Corp.

Gary Clayton, Founder and CEO, Privacy Council, Inc.

William P. Crowell

Michael de Janes, General Counsel and Secretary, ChoicePoint

Robert L. Deitz, Deputy General Counsel (Intelligence), Department of Defense

Jim Dempsey, Executive Director, Center for Democracy and Technology

Viet Dinh, Professor of Law, Georgetown University Law Center

Brigadier General George R. Fay, Commanding General, U.S. Army Intelligence & Security Command

Dr. Usama Fayyad, President, DMX Group; Chairman, Revenue Science, Inc.

Dr. Edward W. Felten, Professor of Computer Science and Director of the Secure Internet Programming Laboratory, Princeton University; Co-Chairman of DARPA Information Science and Technology Advisory Board

Dan Gallington, Senior Research Fellow at the Potomac Institute for Policy Studies

The Hon. Governor James S. Gilmore, III, Chair, Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

Jamie Gorelick, Partner, Wilmer, Cutler & Pickering

Jeff Green, Senior Attorney, Standards of Conduct Office, Department of Defense

Carol Haave, Deputy Under Secretary of Defense (Security and Information Operations)

Dr. David Jensen, Research Assistant Professor of Computer Science and Director of the Knowledge Discovery Laboratory, University of Massachusetts–Amherst

Jeff Jonas, Chief Scientist and Founder, Systems Research & Development

Dr. Takeo Kanade, U.A. Helen Whitaker University Professor of Computer Science and Robotics, Carnegie Mellon University

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security

Dr. Thomas H. Killion, Acting Deputy Assistant Secretary for Research and Technology/Chief Scientist, Department of Defense

George B. Lotz, II, Assistant to the Secretary of Defense (Intelligence Oversight)

Teresa Lunt, Principal Scientist and Area Manager of Security Group and Area Manager of Theory Group, Palo Alto Research Center

The Hon. Paul McHale, Assistant Secretary of Defense for Homeland Defense

Judith A. Miller, Williams & Connolly

Lieutenant Colonel Ronald K. Miller, United States Air Force

Vahan Moushegian, Director, Privacy Office, Department of Defense

The Hon. Representative Jerry Nadler (D-N.Y.)

Major General Paul D. Nielsen, Commander, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio

Sue Payton, Deputy Under Secretary of Defense (Advanced Systems & Concepts)

Dr. Gregory Piatetsky-Shapiro, President, KDnuggets

Dr. Robert Popp, Special Assistant to the Director for Strategic Matters, DARPA

Vito Potenza, Acting General Counsel, National Security Agency

Michael R. Ramage, General Counsel, Florida Department of Law Enforcement

Thomas M. Regan, Executive Director for Privacy and Regulatory Affairs, LexisNexis

Martha Rogers, Partner, Peppers & Rogers

Paul Rosenzweig, Senior Legal Research Fellow, Heritage Foundation

Dr. Nils R. Sandell, Jr., President and CEO, ALPHATEH, Inc.

Brian Sharkey, Senior Vice President, Advanced Systems and Concepts, Hicks & Associates

Jeffrey H. Smith, Arnold & Porter

Jim Smyser, Associate Deputy General Counsel (Military Personnel and Reserve Policy)

David Sobel, General Counsel, Electronic Privacy and Information Center

Jay Stanley, Communications Director, American Civil Liberties Union

James B. Steinberg, Vice President and Director, Foreign Policy Studies, Brookings Institution

Dr. Latanya Sweeney, Director, Laboratory for International Data Privacy, Carnegie Mellon University

Captain David C. Taylor, United States Navy, Chief, J6 Director's Action Group

Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency

Stephen Thayer, Deputy Director, Office of National Risk Assessment, Department of Homeland Security

Michael Vatis, Executive Director, Markle Foundation Task Force on National Security in the Information Age

Allan Wade, Chief Information Officer, Central Intelligence Agency

The Hon. Senator Ron Wyden (D-Ore.)

The Hon. Michael W. Wynne, Acting Under Secretary of Defense (Acquisition, Technology and Logistics)

Lee M. Zeichner, President, Zeichner Risk Analytics, LLC

APPENDIX C BIBLIOGRAPHY

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty* (2003).

Philip E. Agre & Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (MIT Press, 1998).

Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (Knopf, 1995).

Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (New York 1994).

Fred H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States," 33 *Indiana Law Review* 173 (1999).

_____ & Robert E. Litan, "Constitutional Issues in Information Privacy," 9 *Michigan Technology & Telecommunications Law Review* 35 (2002).

_____, Robert E. Litan, Michael Staten & Peter Wallison, *Financial Privacy, Consumer Prosperity, and the Public Good: Maintaining the Balance* (Brookings Institution Press, 2003).

_____, "Principles for Protecting Privacy," *Cato Journal*, vol. 22, no. 1, at 33 (2002).

_____, "Privacy Protection and the Quest for Information Control," in Adam Thierer & Clyde Wayne Crews Jr., eds., *Who Rules the Net? Internet Governance and Jurisdiction* 297 (Cato Institute, 2003).

_____, "Privacy, Consumer Credit, and the Regulation of Personal Information," in *The Impact of Public Policy on Consumer Credit* (Kluwer, 2001).

_____, *Privacy in Perspective* (American Enterprise Institute Press, 2001).

_____, *Privacy in the Information Age* (Brookings Institution Press, 1997).

_____, *Privacy and Other Civil Liberties in the United States After September 11* (American Institute of Contemporary German Studies, 2002).

_____, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It*, The Freedom Forum (2003).

_____, "Privacy Regulation and What is at Risk," *Corporate Governance: Implications for Financial Services Firms* 61 (2003).

Electronic Frontier Foundation, EFF Review of May 20 Report on Total Information Awareness (2003).

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

Federal Trade Commission, *Privacy Online: A Report to Congress* (1998).

_____, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* (2000).

Benjamin Franklin, *Historical Review of Pennsylvania* (1759).

General Accounting Office, *Federal Agencies' Fair Information Practices* (GAO/AIMD-00-296R) (2000).

Ken Gormley, "One Hundred Years of Privacy," 1992 *Wisconsin Law Review* 1335 (1992).

Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, S. Rept. No. 107- 351, H. Rept. No. 107-792, 107th Congress, 2d Session (2002).

Stan Karas, "Privacy, Identity, Databases," 52 *American University Law Review* 393 (2002).

Charles H. Kennedy & Peter P. Swire, "State Wiretaps and Electronic Surveillance After September 11," 54 *Hastings Law Journal* 971 (2003).

Orin S. Kerr, "Internet Surveillance Law After The USA PATRIOT Act: The Big Brother that Isn't," 97 *Northwestern University Law Review* 607 (2003).

Raymond Shih Ray Ku, "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance," 86 *Minnesota Law Review* 1325 (2002).

Christopher Kuner, *European Data Privacy Law and Online Business* (2003).

Craig L. LaMay, *Journalism and the Debate over Privacy* (2003).

Richard C. Leone & Greg Anrig, Jr., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (Century Foundation, 2003).

John Locke, *Two Treatises of Government* 305 (Peter Laslett, ed., 1988).

Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age* (2002).

_____, *Creating a Trusted Network for Homeland Security* (2003).

Michael E. O'Hanlon, et al. *Protecting the American Homeland—One Year On* (Brookings Institution Press, 2003).

Richard A. Posner, "The Right of Privacy," 12 *Georgia Law Review* 393 (1978).

Report to Congress Regarding the Terrorism Information Awareness Program (May 20, 2003).

Paul Rosenzweig, *Balancing Liberty and Security*, Heritage Foundation Commentary (2003).

_____ & Ha Nguyen, *CAPPS II Should be Tested and Deployed*, Heritage Foundation Backgrounder #1683 (2003).

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

Alan Charles Raul, *Privacy and the Digital State: Balancing Public Information and Personal Privacy* (Progress & Freedom Foundation, 2002).

Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2001).

Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)," 2001 *Stanford Technology Law Review* 1.

_____, "Privacy and Secrecy after September 11," 86 *Minnesota Law Review* 1115 (2002).

Paul H. Rubin & Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information* (Progress & Freedom Foundation, 2002).

Paul M. Schwartz, "Administrative Law—The Oversight of Data Protection Law" (Book Review), 39 *American Journal of Comparative Law* 618 (1991).

_____, "European Data Protection Law and Restrictions on International Data Flows," 80 *Iowa Law Review* 471 (1995).

_____, "German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance," 54 *Hastings Law Journal* 751 (2003).

_____, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States," 80 *Iowa Law Review* 553 (1995).

Daniel J. Solove, "Access and Aggregation: Public Records, Privacy and the Constitution," 86 *Minnesota Law Review* 1137 (2002).

_____, "Conceptualizing Privacy," 90 *California Law Review* 1087 (2002).

_____, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083 (2002).

_____, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 *Stanford Law Review* 1393 (2001).

Michael E. Staten & Fred H. Cate, *The Impact of National Credit Reporting Under the Fair Credit Reporting Act: The Risk of New Restrictions and State Regulation*, Financial Services Coordinating Council (2003).

_____ & Fred H. Cate, "The Impact of Opt-in Privacy Rules on Retail Credit Markets: A Case Study of MBNA," 52 *Duke Law Journal* 745 (2003).

Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, Congressional Research Service RL31730 (2003).

Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 129 (2003).

Peter P. Swire & Lauren Steinfeld, "Security and Privacy After September 11: The Health Care Example," 86 *Minnesota Law Review* 1515 (2002).

K.A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 5 *Columbia Science & Technology Law Review* 2 (2003).

Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You," 52 *Stanford Law Review* 1049 (2000).

Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193 (1890).

Darrell M. West, *Assessing E-government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (2000).

Alan F. Westin, *Privacy and Freedom* (New York 1967).

_____, "Social and Political Dimensions of Privacy," 59 *Journal of Social Issues* 431 (2003).

NOTES

[1] Tony Blair, Address before a Joint Session of Congress, Washington, DC, July 17, 2003.

[2] Id.

[3] U.S. Department of Defense, Technology and Privacy Advisory Committee Charter (Mar. 25, 2003).

[4] Id.

[5] John Poindexter, Overview of the Information Awareness Office, prepared remarks for delivery at DARPATech 2002, Anaheim, CA, Aug. 2, 2002, at 1.

[6] Department of Defense Appropriations Act, 2004, Pub. L. No. 108-84,£ 8183 (Sept. 25, 2003).

[7] Memo from CIA Director George Tenet (May 11, 1998).

[8] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 201(d)(1), (d)(14) (Nov. 25, 2002).

[9] Alexander Hamilton, "The Consequences of Hostilities Between the States" (Federalist Paper 8), *New York Packet*, Nov. 20, 1787.

[10] Kennedy v. Mendoza-Martinez, 372 U.S. 144, 165 (1963).

[11] Benjamin Franklin, *Historical Review of Pennsylvania* 1 (1759).

[12] U.S. Department of Defense, Total Information Awareness (TIA) Update, News Release 060-03 (Feb. 7, 2003).

[13] *Establishment of the Technology and Privacy Advisory Committee*, 68 Fed. Reg. 11,384 (2003) (DOD, notice).

[14] U.S. Department of Defense, Technology and Privacy Advisory Committee Charter (Mar. 25, 2003).

[15] Id. (paragraphs reordered).

[16] Department of Defense Appropriations Act, 2004, Pub. L. No. 108-84 (Sept. 25, 2003).

[17] Id., § 8183(a).

[18] Id., § 8183(b).

[19] *Conference Report on Making Appropriations for the Department of Defense for the Fiscal Year Ending September 30, 2004, and for Other Purposes*, House Rpt.108-283 (2003). The four permitted projects are: Bio-Advanced Leading Indicator Recognition, Rapid Analytic Wargaming, Wargaming the Asymmetric Environment, and Automated Speech and Text Exploitation in Multiple Languages.

[20] Letter from Newton N. Minow, TAPAC Chair, to the Hon. James Haynes, DOD General Counsel (Sep. 30, 2003). In subsequent conversations, TAPAC agreed that DOD need not report on personnel and related programs solely involving data about DOD employees and contractors. In response to TAPAC's request, communicated by the Under Secretary of Defense (Acquisition, Technology and Logistics) to units within DOD and the

armed services thought likely to be hosting or developing such programs, the committee's Executive Director received reports on dozens of programs, which she reviewed with the Chairman to determine those on which the committee should be briefed in detail.

[21] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 201(d)(1), (d)(14) (Nov. 25, 2002).

[22] Torch Concepts, "Homeland Security—Airline Passenger Risk Assessment," presented at the Southeastern Software Engineering Conference, Huntsville, AL, Feb. 25, 2003; "JetBlue Chief's Message to Customers," *New York Times*, Sept. 20, 2003, at C14; Ryan Singel, "JetBlue Shared Passenger Data," *Wired*, Sept. 2003.

[23] Memo from CIA Director George Tenet (May 11, 1998).

[24] See <ic-arda.org>.

[25] *Privacy Act of 1974: System of Records*, 68 Fed. Reg. 45,265 (2003) (TSA, DHS, interim final notice).

[26] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 201(d)(1), (d)(14) (Nov. 25, 2002).

[27] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[28] *Financial Crimes Enforcement Network; Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity*, 67 Fed. Reg. 60,579 (2002) (Treasury) (final rule).

[29] *Transactions and Customer Identification Programs*, 68 Fed. Reg. 25,089 (2003) (Treasury, Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Commodity Futures Trading Commission, Securities and Exchange Commission) (final rules and proposed rule).

[30] *Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations—Requirement that Nonfinancial Trades or Businesses Report Certain Currency Transactions*, 66 Fed. Reg. 67,679 (2001) (Treasury) (interim rule, final and proposed rules).

[31] Robert O'Harrow, Jr., "U.S. Backs Florida's New Counterterrorism Database," *Washington Post*, Aug. 6, 2003, at A1.

[32] Id.; Thomas C. Greene, "A Back Door to Poindexter's Orwellian Dream," *The Register*, Sept. 24, 2003.

[33] For an excellent recent discussion of data mining, see K.A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," 5 *Columbia Science & Technology Law Review* 2 (2003).

[34] S. Amend. 59 to H.J. Res. 2 (Jan. 23, 2003).

[35] Kennedy v. Mendoza-Martinez, 372 U.S. 144, 165 (1963).

[36] United States v. Robel, 389 U.S. 258, 264 (1967).

[37] See infra pp. 72, 84.

[38] Letter from George Washington, President of the Constitutional Convention, to the President of the Continental Congress, Sep. 17, 1787.

[39] Alexander Hamilton, "The Consequences of Hostilities Between the States" (Federalist Paper 8), *New York Packet*, Nov. 20, 1787.

[40] Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 61 (2004) (separate statement of Floyd Abrams).

[41] Presentation by the Hon. Governor James S. Gilmore, III, Chair, Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, before the Technology and Privacy Advisory Committee, Washington, DC, Nov. 20, 2003.

[42] *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001,* Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, S. Rept. No. 107- 351, H. Rep. No. 107-792, 107th Congress, 2d Session (2002).

[43] Id. at xv.

[44] Id. at xvi.

[45] Id.

[46] Id.

[47] Benjamin Franklin, *Historical Review of Pennsylvania* (1759).

[48] George W. Bush, Remarks by the President at the 20th Anniversary of the National Endowment for Democracy, United States Chamber of Commerce, Washington, D.C., Nov. 8, 2003.

[49] John Locke, *Two Treatises of Government* 305 (Peter Laslett, ed., 1988).

[50] U.S. Constitution preamble.

[51] Presentation by the Hon. Senator Ron Wyden (D-Ore.) before the Technology and Privacy Advisory Committee, Washington, DC, Nov. 20, 2003.

[52] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty* 4 (2003).

[53] Markle Foundation Task Force on National Security in the Information Age, *Protecting America's Freedom in the Information Age* 2, 9 (2002).

[54] Tony Blair, Address before a Joint Session of Congress, Washington, DC, July 17, 2003.

[55] Id.

[56] Presentation by the Hon. Paul McHale, Assistant Secretary of Defense for Homeland Security, before the Technology and Privacy Advisory Committee, Washington, DC, Nov. 20, 2003.

[57] Infra p. 71 (separate statement of William T. Coleman, Jr.).

[58] Infra p. 73 (separate statement of William T. Coleman, Jr.) (citation omitted).

[59] Infra p. 63 (separate statement of Floyd Abrams).

[60] TAPAC Charter, supra.

[61] Infra p. 63 (separate statement of Floyd Abrams).

[62] Infra p. 72 (separate statement of William T. Coleman, Jr.).

[63] Blair, supra.

[64] *Fiscal 2003 Defense Request: Combating Terrorism*, Hearing before the Senate Armed Services Committee, April 10, 2002 (statement of Dr. Tony Tether).

[65] John Poindexter, Overview of the Information Awareness Office, prepared remarks for delivery at DARPATech 2002, Anaheim, CA, Aug. 2, 2002, at 1.

[66] Id.

[67] Id. at 2.

[68] Id.

[69] Id.

[70] William Safire, "You Are a Suspect," *New York Times*, Nov. 14, 2002, at A35.

[71] Statement of George B. Lotz, II, Assistant to the Secretary of Defense (Intelligence Oversight), to TAPAC, July 22, 2003, at 2.

[72] Id.

[73] Letter from Joseph E. Schmitz, DOD Inspector General, to Senator Charles E. Grassley, Chairman, Committee on Finance, Jan. 17, 2003).

[74] Department of Defense, Office of the Inspector General, *Information Technology Management: Terrorism Information Awareness Program* (D-2004-033) 4 (2003).

[75] S. Amend. 59 to H.J. Res. 2 (Jan. 23, 2003).

[76] Consolidated Appropriations Resolution, Pub. L. No. 108-7, Division M, § 111(b) (Feb. 24, 2003).

[77] *Report to Congress Regarding the Terrorism Information Awareness Program* (May 20, 2003).

[78] Id., Executive Summary, at 3-4. According to the report, five major "investigation threads" were being pursued as part of TIA:

- **Secure Collaborative Problem Solving.** A collaborative environment is sought that would enable ad hoc groups to quickly form within and across agency boundaries to bring together relevant data, diverse points of view, and experience to solve the complex problems associated with countering terrorism.
- **Structured Discovery with Sources and Methods Security.** A wide range of intelligence data, both classified and open source, may need to be searched to find relevant information for understanding the terrorist intent. DARPA believes that to have any hope of making sense of this wide range of data, a more structured and automated way of approaching the problem is needed.
- **Link and Group Understanding.** One of the characteristics of the terrorist threat is that terrorist organizational structures are not well understood and are purposefully designed to conceal their connections and relationships. IAO is researching software that can discover linkages among people, places, things, and events related to possible terrorist activity.
- **Context Aware Visualization.** DARPA believes that better ways are needed to visualize information than text-based lists, tables, and long passages of unstructured text. Such visualization concepts should respond to a broad range of potential users with wholly different roles and responsibilities.
- **Decision Making with Corporate Memory.** Decision-makers must consider a full range of possible options to deal with complex asymmetric threats, particularly in light of rapidly changing circumstances. DARPA's activities in this area are premised on the view that understanding how certain decisions played out in the past is critical to formulating current decision options.

Id. at 2-3.

[79] The "High-Interest TIA-related Programs" are:

Genisys. The Genisys Program seeks to produce technology for integrating and broadening databases and other information sources to support effective intelligence analysis aimed at preventing terrorist attacks on the citizens, institutions, and property of the United States. DARPA's goal is to make databases easy to use so users can increase the level of information coverage, get answers when needed, and share information among agencies faster and easier. DARPA's vision is that Genisys technologies will make it possible for TIA properly to access the massive amounts of data on potential foreign terrorists.

Genisys Privacy Protection. The Genisys Privacy Protection Program aims to create new technologies to ensure personal privacy in the context of improving data analysis for detect-

ing, identifying, and tracking terrorist threats. The Genisys Privacy Protection Program aims to provide *security with privacy* by providing certain critical data to analysts while controlling access to unauthorized information, enforcing laws and policies through software mechanisms, and ensuring that any misuse of data can be quickly detected and addressed.

Evidence Extraction and Link Discovery ("EELD"). The objective of the EELD program is to develop a suite of technologies that will automatically extract evidence about relationships among people, organizations, places, and things from unstructured textual data, such as intelligence messages or news reports, which are the starting points for further analysis. In DARPA's view, this information can point to the discovery of additional relevant relationships and patterns of activity that correspond to potential terrorist events, threats, or planned attacks.

Scalable Social Network Analysis ("SSNA"). The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people, based on their patterns of interactions, and to identify when a terrorist group plans to execute an attack.

MisInformation Detection ("MInDet"). The purpose of the MInDet Program is to reduce DOD vulnerability to open source information operations by developing the ability to detect intentional misinformation and to detect inconsistencies in open source data with regard to known facts and adversaries' goals. MInDet seeks to improve national security by permitting the intelligence agencies to evaluate the reliability of a larger set of potential sources and, therefore, exploit those determined to be reliable and discount the remainder. Other potential uses include the ability to detect misleading information on various government forms (e.g., visa applications) that would suggest further investigation is warranted, to identify foreign sources who provide different information to home audiences and to the United States, and to identify false or misleading statements in textual documents.

Human Identification at a Distance ("HumanID") Program. The HumanID Program seeks to develop automated, multimodal biometric technologies with the capability to detect, recognize, and identify humans at a distance. Once these individual technologies are developed, HumanID will develop methods for fusing these technologies into an advanced human identification system. This system will be capable of multimodal fusion using different biometric techniques with a focus on body parts identification, face identification, and human kinematics. Biometric signatures will be acquired from various collection sensors including video, infrared and multispectral sensors. The goal of this program is to identify humans as unique individuals (not necessarily by name) at a distance, at any time of the day or night, during all weather conditions, with noncooperative subjects, possibly disguised and alone or in groups.

Activity, Recognition and Monitoring ("ARM"). The ARM Program seeks to develop an automated capability to reliably capture, identify and classify human activities in surveillance environments. ARM capabilities will be based on human activity models. From human activity models, the ARM Program will develop scenario-specific models that will enable operatives to differentiate among normal activities in a given area or situation and activities that should be considered suspicious. The program aims to develop technologies to analyze, model, and understand human movements, individual behavior in a scene, and crowd behavior. The approach will be multisensor and include video, agile sensors, low power radar, infrared, and radio frequency tags.

Next-Generation Face Recognition. Face recognition technology has matured over the last decade, with commercial systems recognizing faces from frontal still imagery (e.g., mug shots). These systems operate in structured scenarios where physical and environmental characteristics are known and controlled. The ability to operate in operational scenarios, such as unstructured outdoor environments, is critical if these technologies are to be deployed in military, force protection, intelligence, and national security applications. DARPA believes that new techniques have emerged that have the potential to significantly improve face recognition capabilities in unstructured environments. These include three-dimensional imagery and processing techniques, expression analysis, use of temporal information inherent in video, and face recognition from infrared and multispectral imagery.

Id., Detailed Information, at 5-12.

The "Other IAO Programs" are:

Genoa II will provide collaborative reasoning tools for TIA that will enable distributed teams of analysts and decision-makers to more effectively use the information resources available.

Wargaming the Asymmetric Environment seeks to develop automated predictive models "tuned" to the behavior of specific foreign terrorist groups to facilitate the development of more effective force protection and intervention strategies.

Rapid Analytical Wargaming seeks to develop a faster than real-time analytical simulation to support U.S. readiness for asymmetric and symmetric missions across analytical, operational, and training domains.

Futures Markets Applied to Prediction would provide DOD with market-based techniques for avoiding surprise and predicting future events. [This project has been subsequently abandoned by DARPA.]

Effective, Affordable, Reusable Speech-to-Text aims to create effective speech-to-text (automatic transcription) technology for human-human speech, focusing on broadcasts and telephone conversations (the most critical media for a wide range of national security applications) to produce core-enabling technology that can be ported rapidly to many languages and a number of applications.

Translingual Information Detection, Extraction and Summarization aims to make it possible for English speakers to find and interpret needed information quickly and effectively, regardless of language or medium.

Global Autonomous Language Exploitation aims to make it possible for machines to discover critical foreign intelligence information in a sea of human language (speech and text) from around the globe, delivering it in actionable form to military operators and intelligence analysts without requiring them to issue specific requests.

Babylon seeks to develop natural language two-way translation technology to support military field operations and other agencies requiring real-time field-oriented translation support.

Symphony is targeted at the development of natural language dialog technology to support military field operations and other agencies requiring real-time, field-oriented dialog systems.

Bio-Advanced Leading Indicator Recognition Technology seeks to develop technology for early (i.e., prior to when people begin to seek professional medical care) detection of a covert biological attack.

Id. at B1-B25.

[80] Id., Executive Summary, at 3.

[81] Department of Defense Appropriations Act, 2004, Pub. L. No. 108-84 (Sept. 25, 2003).

[82] Id. § 8183(a).

[83] Id. § 8183(b).

[84] *Conference Report on Making Appropriations for the Department of Defense for the Fiscal Year Ending September 30, 2004, and for Other Purposes*, House Rpt.108-283 (2003).

[85] Department of Defense, Office of the Inspector General, *Information Technology Management: Terrorism Information Awareness Program* (D-2004-033) 4 (2003).

[86] Id.

[87] Id. at 9.

[88] Id. at 4.

[89] Id. at 7.

[90] *Report to Congress*, Detailed Information, supra at 3.

[91] See, e.g., Electronic Privacy Information Center, *Poindexter's Recent Op-Ed Reflects Inconsistencies in Statements Regarding Total Information Awareness (TIA)* (2003); National Security and Data Analysis, Hearing before the House Comm. on government Reform Subcom. on Technology, Information Policy, Intergovernmental Relations, and Census, May 20, 2003 (statement of Barry Steinhardt, Director of ACLU Technology and Liberty Program).

[92] Poindexter, Overview of the Information Awareness Office, supra.

[93] *Report to Congress*, Detailed Information, supra at 27.

[94] *Report to Congress*, Detailed Information, supra at 14.

[95] Inspector General's Report, supra at 9.

[96] Id. at 7.

[97] Katz v. United States, 389 U.S. 347 (1967).

[98] Griswold v. Connecticut, 381 U.S. 479 (1965).

[99] Roe v. Wade, 410 U.S. 113 (1973).

[100] Id. at 152-53.

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

[102] NAACP v. Alabama, 357 U.S. 449 (1958).

[103] Stanley v. Georgia, 394 U.S. 557 (1969).

[104] Rowan v. Post Office, 397 U.S. 728 (1970).

[105] Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726 (1978).

[106] Frisby v. Schultz, 487 U.S. 474 (1988); Carey v. Brown, 447 U.S. 455 (1980).

[107] Widely varying views of what is "private" are reflected in laws as well. In Europe, for example, General Motors and other companies have discovered it is illegal for a corporate telephone directory that includes the office numbers of individual employees to be accessible from non-European countries. See David Scheer, "Europe's New High-Tech Role: Playing Privacy Cop to the World," *Wall Street Journal*, Oct. 10, 2003, at A1.

[108] See Fred H. Cate, *Privacy in the Information Age* 49-66 (1997).

[109] U.S. Constitution amend. IV.

[110] Exceptions to the warrant requirement include: searches or seizures of items in the "plain view" of a law enforcement officer, Coolidge v. New Hampshire, 403 U.S. 443 (1971); searches conducted incident to valid arrests, U.S. v. Edwards, 415 U.S. 800 (1974); and, in some limited circumstances, searches involving national security. Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, supra at 136, n.16 (Jeffrey H. Smith & Elizabeth L. Howe, "Federal Legal Constraints on Electronic Surveillance").

[111] Richards v. Wisconsin, 520 U.S. 385 (1997).

[112] Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 129 (2003).

[113] Coolidge v. New Hampshire, 403 U.S. 443 (1971).

[114] U.S. v. Edwards, 415 U.S. 800 (1974).

[115] Smith & Howe, supra at 136, n.16.

[116] 389 U.S. 347, 361 (1967).

[117] Camara v. Municipal Court, 387 U.S. 523 (1967).

[118] G.M. Leasing Corp. v. United States, 429 U.S. 338 (1977).

[119] United States v. Chadwick, 433 U.S. 1 (1977); Arkansas v. Sanders, 442 U.S. 753 (1979); Walter v. United States, 447 U.S. 649 (1980).

[120] United States v. Knotts, 460 U.S. 276 (1983).

[121] United States v. Dionisio, 410 U.S. 1 (1973).

[122] Smith v. Maryland, 442 U.S. 735 (1979).

[123] United States v. White, 401 U.S. 745 (1971).

[124] New York v. Belton, 453 U.S. 454 (1981).

[125] United States v. Ross, 456 U.S. 798 (1982).

[126] South Dakota v. Opperman, 428 U.S. 364 (1976).

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

[128] Id. at 440.

[129] Id. at 442.

[130] Id. at 443 (citation omitted) (emphasis added).

[131] Daniel Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1087 (2002).

[132] Right to Financial Privacy Act, 12 U.S.C.£§ 3401-3422.

[133] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[134] Paul Schwartz, "German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance," 54 *Hastings Law Journal* 751, 770 (2003) (quoting 18 U.S.C. §§ 2703, 3121 (2003)).

[135] 18 U.S.C. §§ 3121, 1841.

[136] See infra pp. 67-70, 73, 80-83 (separate statement of William T. Coleman, Jr.).

[137] 425 U.S. at 435.

[138] See infra p. 73.

[139] U.S. v. U.S. District Court for the Eastern District of Michigan, 407 U.S. 297 (1972) (commonly referred to as the *Keith* decision).

[140] Jeffrey H. Smith & Elizabeth L. Howe, "Federal Legal Constraints on Electronic Surveillance," *Protecting America's Freedom in the Information Age* 133 (2002).

[141] See U.S. v. Bin Laden, 126 F. Supp. 2d 264, 271-72 (S.D.N.Y. 2000).

[142] Whalen v. Roe, 429 U.S. 589, 599-600 (1977).

[143] Id. at 599-600.

[144] Id. at 603-04.

[145] Id. at 604, n.32.

[146] Tavoulareas v. Washington Post Company, 724 F.2d 1010 (D.C. Cir. 1984); Barry v. City of New York, 712 F.2d 1554 (2d Cir. 1983); Schacter v. Whalen, 581 F.2d 35 (2d Cir. 1978); Doe v. Southeastern Pennsylvania Transportation Authority, 72 F.3d 1133 (3d Cir. 1995); United States v. Westinghouse Electric Corporation, 638 F.2d 570 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119 (5th Cir. 1978); Doe v. Attorney General, 941 F.2d 780 (9th Cir. 1991).

[147] Walls v. City of Petersburg 895 F.2d 188, 192 (4th Cir. 1990); J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981).

[148] Doe v. Attorney General, 941 F.2d at 796.

[149] U.S. Constitution, amend. XIV.

[150] Personnel Administrator v. Feeney, 442 U.S. 256 (1979). See generally Eric Braverman & Daniel R. Ortiz, "Federal Legal Constraints on Profiling and Watch Lists," *Protecting America's Freedom in the Information Age* 149, 155 (2002).

[151] United States v. Weaver, 966 F.2d 391 (8th Cir. 1992); see Braverman & Ortiz, id. at 155.

[152] Village of Arlington Heights v. Metropolitan Housing Development Corporation, 429 U.S. 252 (1977); Washington v. Davis, 426 U.S. 229 (1976); see Braverman & Ortiz, supra at 156.

[153] 5 U.S.C. §§ 552a(e)(1)-(5).

[154] Id.

[155] Id. § 552a(b).

[156] Id. § 552a(e)(4).

[157] Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, supra at 127, 128 (Sean Fogarty & Daniel R. Ortiz, "Limitations Upon Interagency Information Sharing: The Privacy Act of 1974").

[158] 5 U.S.C. § 552a(b),

[159] Id. § 552a (b)7

[160] Id. § 552a (b)3

[161] *OMB Guidelines*, 52 Fed. Reg. 12,900, 12,993 (1987). See generally Fogarty & Ortiz, supra at 129-130.

[162] Petrus v. Bowen, 833 F.2d 581 (5th Cir. 1987).

[163] Perez-Santos v. Malave, 23 Fed. App. 11 (1st Cir. 2001); Ortez v. Washington County, 88 F.3d 804 (9th Cir. 1996).

[164] Flowers v. Executive Office of the President, 142 F. Supp. 2d 38 (D.D.C. 2001).

[165] Standley v. Department of Justice, 835 F.2d 216 (9th Cir. 1987).

[166] U.S. v. Miller, 643 F.2d 713 (10th Cir. 1981). See generally Fogarty & Ortiz, supra at 128.

[167] 5 U.S.C. § 552a(b).

[168] Id. § 552a(a)(5).

[169] Henke v. United States DOC, 83 F.3d 1453, 1461 (D.C. Cir. 1996) (quoting Bartel v. F.A.A., 725 F.2d 1403, 1408 n.10 (D.C. Cir. 1984)).

[170] Fogarty & Ortiz, supra at 129 (citing to Bowyer v. United States Dep't of Air Force, 804 F.2d 428 (7th Cir. 1986); Chapman v. NASA 682 F.2d 526 (5th Cir. 1982)).

[171] 5 U.S.C. §§ 552, 552(b)(6), (b)(7)(C).

[172] 425 U.S. 435.

[173] 12 U.S.C. §§ 3401-3422.

[174] 42 U.S.C. § 1305 (1997).

[175] 26 U.S.C. §§ 6103, 7431 (1997).

[176] 13 U.S.C. §§ 8-9 (1994).

[177] Most of the legal protections of informational privacy in the private sector reflect a similar purpose: to give consumers a legal right to control the collection and use of information about them. This is the dominant trend of recent privacy statutes and of the FTC's push for privacy policies, reflecting a definition of privacy articulated by the dean of American privacy scholars, Alan Westin, in his 1967 path-breaking study *Privacy and Freedom*: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan F. Westin, *Privacy and Freedom* 7 (1967). The Supreme

Court appears to embrace this understanding of privacy as well. Justice Stevens wrote for the unanimous Court in 1989: "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *Reporter's Committee*, 489 U.S. at 749.

Sector-specific statutes and regulations impose obligations on data processors, or give individual data subjects rights, with regard to the collection and use of personal information. Some of these laws have been in place for decades. For example, the Fair Credit Reporting Act, adopted in 1970, permits disclosure of credit information only for statutorily specified purposes, restricts the dissemination of certain types of obsolete information, requires consent (in some cases opt-in) for specified uses of information, mandates disclosures that must be given to data subjects, guarantees their right to access and correct information about them, and provides for close oversight and enforcement by the Federal Trade Commission ("FTC"). Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

Similarly, the Electronic Funds Transfer Act of 1978, 15 U.S.C. §§ 1693-1693r, the Fair Credit Billing Act of 1974, 15 U.S.C. § 1666, the Fair Debt Collection Practices Act of 1977, 15 U.S.C. § 1692c(b), all restrict the use and disclosure of certain financial information about individuals. The Electronic Communications Privacy Act prohibits the interception or disclosure of the contents of any electronic communication, such as telephone conversations or e-mail, or even of any conversation in which the participants exhibit "an expectation that such communication is not subject to interception under circumstances justifying such an expectation." 18 U.S.C. §§ 2510-11. The Telecommunications Act of 1996, 47 U.S.C. § 222, restricts the use of information about customer calls without consumer consent. The Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(1), restricts the collection, storage, and disclosure of personally identifiable information without the subscriber's consent, and requires that service providers provide their subscribers with access to information collected about them. The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, prohibits the disclosure of titles of particular videos rented by identifiable customers. The Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009, prohibits an employer's use of lie detectors and the results of lie detector tests. The Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, restricts the disclosure of student records by educational institutions that receive public funds, and guarantees students and parents a right of access to records.

There has been a considerable amount of recent activity on both the federal and state level to adopt broader sectoral privacy laws. For example, the Children's Online Privacy Protection Act of 1998 requires that operators of websites who collect personally identifiable information from children under 13 must provide parents with notice of their information practices, and obtain prior, verifiable opt-in parental consent for the collection, use, and/or disclosure of personal information from children. The law gives parents the right to review the personal information collected from their children, and to prevent the further use of personal information that has already been collected, or the future collection of personal information. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

Title V of the Gramm-Leach-Bliley Financial Services Modernization Act, which took effect on July 1, 2001, regulates the collection and use of information about customers in the financial services sector The law requires financial institutions, subject to enumerated exceptions, to "clearly and conspicuously" provide consumers with an annual notice about their

information disclosure policies, and to provide consumers with the opportunity to opt out of transfers of "nonpublic personal information" to nonaffiliated third parties. Gramm-Leach-Bliley Financial Services Modernization Act, 106 Pub. L. No. 102, 113 Stat. 1338, tit. V (1999).

Finally, in April 2001, the Department of Health and Human Services adopted rules protecting the privacy of personal health information. "Covered entities" may use personal health information to provide, or obtain payment for, health care only after first providing the patient with notice and making a "good faith effort" to obtain a written acknowledgment. A covered entity may use personal health information for other purposes only with an individual's opt-in "authorization." Signing an authorization may not be a condition of receiving treatment or participating in a health plan. Covered entities must make reasonable efforts to limit the use and disclosure of personal health information to the minimum necessary to accomplish the intended purpose. The rules contain a number of exceptions, for example, for public health activities; to report victims of abuse, neglect, or domestic violence; in judicial and administrative proceedings; and for certain law enforcement activities. *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

[178] 47 U.S.C. § 551.

[179] Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, supra at 161, 167 (Stewart A. Baker, "The Regulation of Disclosure of Information Held by Private Parties").

[180] Pub. L. No. 107-56, supra, Title II, § 211.

[181] 18 U.S.C. § 2710.

[182] 20 U.S.C. § 1232g.

[183] 18 U.S.C. §§ 2510-2522.

[184] *Internet Security and Privacy*, Hearing before the Senate Judiciary Com., May 25, 2000 (statement of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology).

[185] Electronic Privacy Information Center, *Title III Electronic Surveillance 1968-2002*.

[186] See, e.g., Smith v. Maryland, 442 U.S. 735 (1979).

[187] 18 U.S.C. §§ 1367, 2521, 2701-2711, 3121-3127.

[188] Id. §§ 3122-23.

[189] Pub. L. No. 107-56, supra, Title II, § 216(a).

[190] 18 U.S.C. § 2703(d).

[191] Id. § 2703(a).

[192] Id. §§ 2703(a), (b), (d).

[193] Baker, supra at 163.

[194] 50 U.S.C. §§ 1801 et seq., 1841 et seq. & 1861 et seq.

[195] Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-2002*; see generally Smith & Howe, supra at 140-41.

[196] 3 C.F.R. pt. 200.

[197] Id., Preamble ¶¶ 2.1, 2.3.

[198] Id., ¶ 2.4.

[199] *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, DOD 5240.1-R (2002).

[200] U.S. Department of Justice, Office of Legal Policy, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* at 21-22 (2002).

[201] Id. at 22.

[202] Id.

[203] Id.

[204] U.S. Department of Justice, Office of Legal Policy, *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (2003).

[205] Id. at 1.

[206] For more detail lists of laws applicable to government collection and use of personal information see *Report to Congress*, Detailed Information, supra at 5-12; Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, Congressional Research Service RL31730 (2003).

[207] 15 U.S.C. § 45(a)(1).

[208] *Privacy Online* (2000), supra at 4.

[209] Federal Trade Commission, *Privacy Online: A Report to Congress* 23, 27-28 (1998); Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress 11 (2000).

[210] Memorandum from OMB Director Jack Lew (Memorandum M-99-18) (June 2, 1999).

[211] General Accounting Office, *Federal Agencies' Fair Information Practices* (GAO/AIMD-00-296R) at 3 (2000).

[212] Darrell M. West, *Assessing E-government: The Internet, Democracy, and Service Delivery by State and Federal Governments* (2000).

[213] E-government Act of 2002, Pub. L. No. 107-347, § 208 (2002).

[214] Id. § 208(c)(1)(B).

[215] Id. § 208(b).

[216] *OMB Guidance for Implementing the Privacy Provisions of the E-government Act of 2002*, M-03-22 (Sept. 26, 2003).

[217] Id. § II.B.3. "*National Security Systems" are defined to mean* "an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management." Id.

[218] See generally, Amelia Gruber, "Agencies' Efforts to Protect Personal Information Vary Widely," GovExec.com (Dec. 17, 2003) (available at http://www.govexec.com/dailyfed/1203/121703a1.htm).

[219] Cate, supra at 32.

[220] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281) (Data Protection Directive).

[221] See generally Scheer, supra at 1.

[222] O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

[223] Secretary's Advisory Commission on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens* (1973).

[224] O.E.C.D., supra.

[225] Children's Online Privacy Protection Act, supra.

[226] Gramm-Leach-Bliley Financial Services Modernization Act, supra.

[227] *Standards for Privacy of Individually Identifiable Health Information*, supra.

[228] *Data Protection Directive*, supra art. 8.

[229] Id. art. 25.

[230] Id. art. 18. See generally Christopher Kuner, *European Data Privacy Law and Online Business* (2003).

[231] James Gleick, "Behind Closed Doors; Big Brother is Us," *New York Times*, Sep. 29, 1996, at 130. For an excellent overview of sources of personally identifiable information in the United States, see Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security* 150 (2003) (Appendix H: Jeff Jonas, "The Landscape of Available Data").

[232] See Alan F. Westin, "Social and Political Dimensions of Privacy," 59 *Journal of Social Issues* 431, 444-449 (2003).

[233] Id.

[234] See infra pp. 67-89 (separate statement of William T. Coleman, Jr.).

[235] Jeremy Bentham, *The Panopticon Writings* 16 (Miran Bozovic ed. 1995). See also Jeffrey H. Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," 11 *Santa Clara Computer & High Technology Law Journal* 27 (1995).

[236] Christopher Slobogin, "Symposium: Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity," 72 *Mississippi Law Journal* 213, 240 (2002).

[237] Hubert H. Humphrey, Foreword to Edward V. Long, *The Intruders* at viii (1967).

[238] See Paul M. Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States," 80 *Iowa Law Review* 553 (1995).

[239] Philip B. Heymann, *Investigative Uses of Files of Data About Many People Collected for Other Purposes* 9 (2003) (unpublished ms.).

[240] Tommy Peterson, "Data Scrubbing," *Computerworld*, Feb. 10, 2003, at 32.

[241] National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

[242] United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

[243] General Accounting Office, Coordinated Approach Needed to Address the Government's Improper Payment Problems (GAO-02-749), Aug. 9, 2002).

[244] Hall, supra at 1A.

[245] Editorial, "Glitches Repeatedly Delay Innocent Air Travelers," *USA Today*, June 25, 2003, at 11A.

[246] Markle Task Force Report, *Creating a Trusted Network for Homeland Security*, supra at 72 (Appendix A: Amitai Etzioni, "Reliable Identification for Homeland Protection and Collateral Gains").

[247] Id. at 4-6, and sources cited therein.

[248] *Privacy Act of 1974; Implementation*, 68 Federal Register 14140 (2003) (DOJ, final rule).

[249] *Privacy Act of 1974: Implementation of Exemption*, 68 Federal Register 49410 (2003) (DHS, final rule).

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

[251] Hearing before the Subcom. on Treasury and General government of the Senate Appropriations Committee (April 15, 1997) (Statement of Margaret Milner Richardson, Commissioner of Internal Revenue).

[252] 15 U.S.C. § 1681c(a). The restrictions do not apply if the information is used in connection with an employment application for a position with a salary over $75,000, a credit transaction over $150,000, or the underwriting of life insurance over $150,000. Id. § 1681c(b).

[253] United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 763 (1989).

[254] Id. at 764.

[255] Id. at 767.

[256] Id. at 794 (quoting Whalen v. Roe, 429 U.S. at 605).

[257] Presentation by the Hon. Representative Jerrold Nadler (D-N.Y.) before the Technology and Privacy Advisory Committee, Washington, DC, Nov. 20, 2003.

[258] TAPAC Charter, supra (emphasis added).

[259] Hugh Dellios, "U.S. Data Mining Investigated," *Chicago Tribune*, Oct. 12, 2003, at A1.

[260] Steve Boggan, "Privacy: The New Security Alert," *The Times* (London), Oct. 14, 2003, at 2.

[261] Infra p. 73 (separate statement of William T. Coleman, Jr.).

[262] Infra p. 69 (separate statement of William T. Coleman, Jr.).

[263] See infra pp. 67-68, 80-83 (separate statement of William T. Coleman, Jr.).

[264] Markle Foundation Task Force, *Protecting America's Freedom in the Information Age*, supra at 1.

[265] Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security*, supra at 52 (Michael Vatis, "Working Group I: Networking of Federal Government Agencies with State and Local Government and Private Sector Entities").

[266] The Markle Foundation Task Force on National Security in the Information Age noted that:

> [M]any argue that it should be no more difficult for the government to gather information than it is for a commercial company or private citizen. We believe, however, that different considerations apply to government acquisition and use of personally identifiable data, even when it is widely available to the public. Although there are consequences associated with the data's being available in the private sector (such as loss of job opportunities, credit worthiness, or public embarrassment), the consequences of government access to and use of data can be more far-reaching, and can include loss of liberty and encroachment on the constitutionally rooted right of privacy (both in the Fourth Amendment and more generally), which is designed to protect citizens from intrusion by government, not neighbors or credit bureaus. Therefore, we believe that the government should not have routine access to personally identifiable information even if that information is widely available to the public.

Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security*, id. at 33.

[267] The Markle Foundation Task Force on National Security in the Information Age noted that:

> [A]nonymizing technologies could be employed to allow analysts to perform link analysis among data sets without disclosing personally identifiable information. By employing techniques such as one-way hashing, masking, and blind matching, analysts can perform their jobs and search for suspicious patterns without the need to gain access to personal data until they make the requisite showing for disclosure.

Id. at 34.

[268] TAPAC Charter, supra.

[269] See Griswold v. Connecticut, 381 U.S. 479 (1965); Lawrence v. Texas, 123 S. Ct. 2472 (2003).

[270] See Hill v. Colorado, 530 U.S. 703 (2000); see, Bartnicki v. Vopper, 532 U.S. 514, 523 (2001); id. at 535, 537-38 (Breyer, J., concurring); id. at 541 (Rehnquist, C.J., dissenting).

[271] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[272] Infra p. 78 (separate statement of William T. Coleman, Jr.).

[273] *Report to Congress*, Detailed Information, supra at 3.

[274] Id. at 14.

[275] Infra p. 84 (separate statement of William T. Coleman, Jr.).

[276] Infra p. 88.

[277] See, Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 298-99 (1967) ("The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others."); United States v. Karo, 468 US 705, 718 (1984) ("if truly exigent circumstances exist no warrant is required under general Fourth Amendment principles.").

[278] See supra pp. viii, 7, 8, 13, 43.

[279] See supra pp. viii, ix, xii, 2, 6-8, 13, 34-35, 48, 59-60.

[280] Supra p. viii.

[281] Supra pp. 47-48.

[282] See supra pp. 47, 50-51.

[283] Supra pp. ix, 45-46, 48.

[284] See supra pp. 21-24, 31, 43.

[285] See supra pp. 7, 12, 63, 65 (separate statement of Floyd Abrams).

[286] See supra p. 65 (separate statement of Floyd Abrams).

[287] See supra p. 34.

[288] See infra pp. 81-82 (separate statement of William T. Coleman, Jr.).

[289] See supra pp. viii, ix, xii, 2, 6-8, 13, 34-35, 48, 58-60.

[290] 304 U.S. 144 (1938).

[291] Supra p. 50.

[292] Supra pp. 45-46, 50.

[293] See supra pp. 21, 13.

[294] Supra p. 7.

[295] See supra pp. 7, 13, 21.

[296] Supra pp. 43, 47.

[297] See supra p. 1 (quoting TAPAC Charter).

[298] Supra pp. viii, 9.

[299] See supra pp. viii, 14, 19.

[300] See supra pp. 15-16.

[301] See Thomas Hobbs, *Leviathan*, ch. 28, ch. 14, Section 4; John Jay, Federalist Paper No. 3, at 10-11; William Godwin (1756-1836), *An Enquiry Concerning Political Justice,* in Mencken, *A New Dictionary of Quotations on Historical Principles from Ancient and Modern Sources* (1982) ("government can have no more than two legitimate purposes—the suppression of injustice against individuals within the community and the common defense against external invasion"); Justinian I (483-565), Emperor of Byzantium, *The Twelve Tables* ("The safety of the State is the highest law"); Alexander Hamilton, Federalist Paper No. 8,

Nov. 20, 1787 ("Safety from external danger is the most powerful director of national conduct"); President Franklin D. Roosevelt, Annual Message to Congress, Jan. 6, 1941, in Podell, *Speeches of the American Presidents* (1988) ("First, by an impressive expression of the public will and without partisanship, we are committed to all-inclusive national defense"); St. Thomas Aquinas, in Coker, *Readings in Political Philosophy* 218 ("The aim of any ruler ought to be to secure the safety of that which he [or she] has undertaken to rule"); Demosthenes (385?-322 B.C.), in Eigen & Siegal, *The Macmillan Dictionary of Political Quotations* Ch. 16, No. 15 ("Defend yourselves instantly, and I say you will be wise; delay it, and you may wish in vain to do so thereafter"); No. 33 (Alexander Hamilton, 1755-1804); No. 55 (James Madison, 1751-1836); No. 70 (Franklin D. Roosevelt); No. 77 (Caterina Sforza, 1492-1509).

[302] Terminello v. Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting) ("There is danger that, if the Court does not temper is doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact.").

[303] Berenson, "Rule of Law," *Wall Street Journal*, at A15 (Dec. 29, 2003).

[304] See supra pp. 14, 19.

[305] See supra pp. 14-20, 17 nn. 77-78.

[306] See supra pp. vii-viii, 2-5.

[307] See supra pp. ix, 33 n. 231, 34-35, 45-47.

[308] See supra p. 29.

[309] Supra p. 4.

[310] See supra pp. xiv-xv; infra pp. 92-96 (separate statement of William T. Coleman, Jr.).

[311] U.S. Department of Defense, Technology and Privacy Advisory Committee Charter (Mar. 25, 2003) (paragraphs reordered).

[312] Supra pp. 14-19.

[313] Id.

[314] Supra pp. 19-20 (citations omitted).

[315] See supra p. viii.

[316] See supra pp. 14-20.

[317] See supra p. 43.

[318] See supra p. viii.

[319] See supra pp. vii-viii, 2-5.

[320] Supra pp. 2, 7-8, 13.

[321] Supra p. 31.

[322] See, e.g., United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); Whalen v. Rose, 427 U.S. 589 (1977).

[323] Supra pp. 21-22 (quoting 425 U.S. at 443) (citation omitted).

[324] Supra p. 23 (quoting Daniel Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *Southern California Law Review* 1083, 1087 (2002)).

[325] Supra p. 25 (quoting 429 U.S. 589 (1977)).

[326] Supra p. 16.

[327] Supra p. 31.

[328] Supra p. 25.

[329] Supra pp. 21-31.

[330] See supra p. 31.

[331] See supra pp. 82-83 (separate statement of William T. Coleman, Jr.).

[332] See the statutes collected in the report, supra pp. 25-29.

[333] Supra pp. 50-51.

[334] Supra pp. 55-57.

[335] See supra p. 14.

[336] Supra p. 51.

[337] Id.

[338] See supra pp. 32-42.

[339] See supra pp. 46-48.

[340] Supra p. 29 (quoting U.S. Department of Justice, Office of Legal Policy, *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* at 21-22 (2002)).

[341] See supra p. 46.

[342] See supra pp. 55-57.