# The Challenge of Information Sharing

## Balancing National Security and Civil Liberties

Washington, DC
2003

The Brookings Institution

ITS

Computer Ethics Institute

Ascential™ Software

# THE CHALLENGE OF INFORMATION SHARING
## BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

This report is a summary of the round table discussion "The Challenge of Information Sharing: Balancing National Security and Civil Liberties" held at the Brookings Institution on June 5, 2003. The event was co-sponsored by the Brookings Institution ITS, the Computer Ethics Institute, and the Ascential Software Corporation. The co-chairs and organizing committee of the event are listed below. The ideas presented in this report are those of the participants of this discussion and do not represent the views of the sponsoring organizations, the co-chairs, or the organizing committee members.

**CO-CHAIRS:**

Jane Fishkin, Vice President and Chief Information Officer, Brookings Institution
Ramon Barquin, President, Computer Ethics Institute and President, Barquin International
Bob Zurek, Vice President, Ascential Software Corporation

**ORGANIZING COMMITTEE:**

Larry Meador, Chair (MGI)

Daniel Chenok, Office of Management and Budget

Scott Cragg National Imagery and Mapping Agency

Karen Evans Dept. of Energy

Bob Liscouski, Dept. of Homeland Security

Keith Rhodes, General Accounting Office

Jim Simon, Intelligent Enterprises

Allan Wade, Central Intelligence Agency

**ACKNOWLEDGMENTS:**

This report was written by Clayton Northouse with contributions from Cynthia Darling and Calvert Wallace Jones.

**CO-SPONSORS:**

Brookings Institution, ITS
1775 Massachusetts Ave.
Washington, DC 20036
www.brookings.edu

Computer Ethics Institute
1750 K Street, NW, Suite 450
Washington, DC 20006
www.brook.edu/its/cei/cei_hp.htm

Ascential Software Corporation
50 Washington Street
Westboro, MA 01581
www.ascential.com

The report can be downloaded from www.brook.edu/its/cei/cei_hp.htm or bound copies can be ordered for $5 per copy from the Computer Ethics Institute at 202-296-7147 x104.

# Contents

# Introduction

In an age of terrorism, the need to use information technologies to secure the homeland is of paramount concern. At the same time, a framework needs to be developed that is based on a focused examination of how these technologies can be deployed to minimize harm caused to rights of privacy and civil liberties. The Brookings Institution ITS, the Computer Ethics Institute, and the Ascential Software Corporation recognized this need and co-sponsored the discussion "The Challenge of Information Sharing: Balancing National Security and Civil Liberties," which was held on the 5th of June at the Brookings Institution and convened twenty-five senior government officials, public policy analysts, and legal scholars. It is the purpose of this report to summarize the findings of the discussion and outline a view of how the group plans to proceed.

The discussion pulled together a unique set of individuals including not only people who think about these issues on a daily basis but also people who manage and directly affect these issues. The group decided to work towards a framework for balancing security and liberty in the government's use of information technologies for data integration and information sharing. This framework must have the support of the government intelligence community while meeting the civil liberty concerns of the public. Section one of this paper gives a context for such a framework, section two discusses the challenges that the framework must address, section three describes those who would use the framework, and section four outlines the group's plans to develop, implement, and promote the framework.

# I. The Context

Balancing national security and civil liberties can be a polarized issue. The participants in this debate often break down into two camps, referred to in this paper as the advocate and the preemptive positions. The preemptive position states that we are in a new world, the post-9/11 world, and the government needs to do everything it can to protect the nation, even if this means temporarily suspending certain civil liberties. We cannot be restrained by a literal interpretation of the Constitution, because our safety and security is at stake. Unless we act now to prevent the next attack, there will be nothing left to protect.

The advocate position states that this country was founded on principles that define this nation and make it great. The right to protection against unreasonable searches and seizures, the right to equal protection under the law and other fundamental principles of our government need to be preserved in times of crises. If the terrorists force us to erode our civil liberties, we will have lost the war on terrorism, because we will have lost what makes us great as a nation. Therefore, the primary concern in times of crises should be the preservation of civil liberties.

One side argues that we will have nothing to protect if we do not secure the nation. The other side argues that we will have nothing to fight for if we do not preserve our civil liberties. This polarization, though, must be diffused. Civil liberties and national security do not form a zero-sum balance; rather, they are mutually dependent in three ways. First, the right to be secure can be seen as a civil liberty itself. The right to feel secure as a citizen and resident in the United States is a liberty that should be protected along with the right to free speech and other liberties protected in the Constitution. Second, the advocate position must recognize the preemptive pronouncement that we cannot have civil liberties without security. Civil liberties are dependent upon a secure nation. In order to enjoy the rights of a free nation, we must secure it against those who are trying to destroy it. Hence, in order to preserve civil liberties, we need to maintain a robust national security. Third, the preemptive position must recognize the advocate's statement that there is no reason to fight a war on terrorism if we lose the very thing we are fighting for. We are fighting this war, in part, because of the great freedoms that are preserved and recognized in the United States Constitution. If one enters this debate with the understanding that civil liberties and national security are mutually dependent, then the polarization of this issue can be diffused. It is possible to achieve national security and civil liberty and we must therefore strive to maintain both.

"It is possible to achieve national security and civil liberties and we must therefore strive to maintain both."

We now turn to the context of the debate. In the Cold War era, intelligence gathering was much easier: the United States had a better understanding of who the enemy was, where the enemy was located, and what constituted good intelligence. Now in the

face of terrorism, it is more difficult to know who or what constitutes a threat, where the threat is located, and where the terrorists might target the next attack. Developing rules to govern intelligence gathering and sharing is therefore all the more challenging as difficult questions arise. Who should receive threat information? Whom should the intelligence agencies follow and about whom should they collect information?

A second important note about the context pertains to information technologies. With the widespread use of databases and data migration technologies, a vast amount of information is collected and stored in the private sector. Information pertaining to credit card transactions, air travel, financial transactions, and other such activities is stored in databases of the companies involved in these transactions. When pursuing a suspected terrorist, the government must often go to the private sector to collect information. Moreover, because the private sector often has better, more precise information, companies frequently inform the government of threats that they encounter. The relationship between the private sector and government intelligence agencies should be tackled head on in the framework for creating a balance between security and liberty. What kinds of information can be stored by the private sector and what kinds of information can be shared with the government? What intelligence guidance should be given to the private sector?

"The relationship between the private sector and government intelligence agencies should be tackled head on in the framework for creating a balance between security and liberty."

The United States tends to swing between the two positions noted earlier: preserving liberties by restricting the investigative powers of the government and enhancing the powers of the government to establish and maintain national security at the expense of preserving civil liberties. The threat level determines which position dominates the agenda. As demonstrated throughout the history of the United States, when the national security threat level is high, we focus on preserving security ignoring many civil liberty concerns, and when the threat level is low, we tend to focus on preserving civil liberties and repairing any harm caused during the previous national security crisis. During World War II, the country went to extreme measures to preserve national security, even to the extent of interning many innocent Japanese Americans. Later when the threat level decreased, the government recognized and attempted to repair the harm caused. The threat level is currently very high within the United States due to the tragedies of 9/11, and the highest priority of the government is to preempt the next attack. We need to create a framework for safely negotiating the balance between security and civil liberties that will guide the efforts to secure the nation while minimizing the harm caused to civil liberties.

In this preemptive environment, a framework for balancing security and liberty needs to answer four fundamental areas of inquiry. These questions go to the heart of addressing the higher threat level and the unique challenges of stopping terrorism in the post-Cold Ware era.

1. What are the new threats and what information is relevant to these threats?
2. How can we get this information in the most effective manner?
3. What institutions should take the praise or blame in gathering information regarding these threats? Who should provide oversight?
4. How do we harness technology to meet these threats?

As the group moves forward, these questions will serve as guideposts for building a framework to inform how to balance national security and civil liberties. Before taking that step forward, the specific challenges to building this framework must be assessed.

## II. The Challenges

First, there is a challenge pertaining to a lack of rules and oversight to guide intelligence gathering and sharing. During the Cold War there were no rules governing the collection of intelligence, and in this environment, the definition of enemy frequently expanded to include innocent Americans. Watergate brought the call for accountability and ushered in an era of strict judicial oversight. Now with the threat of terrorism, we are drifting back towards this pre-Watergate period in which intelligence agencies lack clear guidelines for intelligence management and the definition of terrorist is expanding. In addition, with the rapid advancement of technologies, many of the existing policies are outdated. Data mining, in particular, is a highly effective tool used to search for and find suspicious individuals. It may involve creating a profile of a terrorist and then searching large amounts of data for individual matches. Although there are currently many agencies under intense pressure to mine vast amounts of data, they lack clear rules of procedure and structured oversight.

"We are operating under a rule of discretion and the government needs an accountability system with a clear set of guidelines."

Immediately after September 11, 2001, there was a rush to pass legislation that would bolster the ability of the United States government to fight and protect against terrorism. The USA PATRIOT Act, for instance, lowered many of the restraints on the collection and use of data in the private sector. In addition, there are no rules governing the sharing of data between the private and government sectors. Legislation only covers the use of data stored in government-owned databases, not the government's use of data stored in the private sector. A participant in the discussion noted that we are operating under a rule of discretion and the government needs an accountability system with a clear set of guidelines.

Another problem facing the implementation and use of technology concerns the importance of trust. Discussions tend to gravitate towards what technology can do, but there is no way that the best technologies available will be implemented in the near future without addressing the problem of a lack of trust. If trust is not developed, technology

solutions cannot be implemented. Can we merge disparate sources of data from the FBI, NSA, CIA, and DIA? Yes, as a technology issue, it is relatively simple to merge data from disparate sources, but, as a human issue where lack of trust may inhibit collaborative intelligence work, it is a difficult and complicated matter.

One participant noted that the intelligence community operates under a slogan of the Cold War—"Trust but verify." Intelligence agencies are perfectly willing to trust as long as they can verify the management of entrusted goods. The "trust but verify" model applies to three different relationships: between federal government agencies, between the private and public sectors, and between the local and federal governments. In the case of intra-governmental information sharing, an agency must have the assurance that it will be able to verify the use of the shared data before it is willing to trust, but the agency is unable to verify. Moreover, because the intelligence communities inhabit a competitive environment, people often want to maintain control of the "good stuff" and are unwilling to share it. Therefore, the participant concluded, sharing of data becomes difficult if not impossible.

"To develop policy that can ensure the verification of shared data, we need to understand how technology works by looking inside the system."

To develop policy that can ensure the verification of shared data, we need to understand how technology works by looking inside the system. A member of the group stated that technology does not drive policy; rather, it sets up the environment. We need to engage the policy people with the technologists, so that they can be better informed about how the technology is actually used. Policy makers' lack of knowledge about the inner working of information technologies leads to ill-conceived policy which in turn disables agencies from verifying the use of data. For instance, a participant noted, it is common practice of some intelligence agencies to strip the meta-data from intelligence when it is acquired, which then prevents one from investigating the provenance of intelligence. In the end, the ability to verify the management of data is lost, and the willingness to trust another agency with data is lost. The participant stressed that because of the practices currently employed by government agencies, there is no easy way to integrate all the intelligence being collected.

A member of the group suggested that the Federal government should look at local governments for a model of how to share data. At the local level, administrators can track, share, and handle the information better, because they have been doing it for longer. For years local police have been sharing information from one district to another and from one state to another. Hence, in the end, they have more comprehensive and better integrated data than the Federal government.

A participant noted that another problem regarding the use of information technologies in the Federal government is that everyone is focused on developing applications (profiling tools for data mining, extraction tools, etc.) and making the current systems

more useful. Instead of looking for ways to collect more data, the technologists are focused on finding better ways to analyze the data already in our possession. Hence, the technologies cannot find things that are beyond the radar screen.

## III. Players in the Field

In the discussion, the group identified many players in the field. This section describes some of the players and identifies their specific functions.

First, there is the newly created Department of Homeland Security (DHS). The objective of DHS is to achieve a balance between national security and civil liberties such that the impact on privacy is minimized while the nation is secure and protected. Protecting the liberties of individuals is central to the DHS mission, because if they fail to do this, then they will fail as a department.

"The objective of DHS is to achieve a balance between national security and civil liberties such that the impact on privacy is minimized while the nation is secure and protected."

The chief privacy officer serves an important function in helping departments meet the mission of achieving security while protecting privacy. The chief privacy officer must play two roles: first, he or she must be a solid member of the agency or department and second, he or she must have a viewpoint from outside the department or agency and must build a relationship with those outside the government. The people within the organization must see the chief privacy officer as someone they can turn to when in need of solutions for meeting objectives that minimize privacy concerns. The chief privacy officer must also gauge the implications the organization has on the individuals' privacy.

At the center of the technology/policy arena, the Office of Management and Budget (OMB) serves an important function in the balance between liberty and security. OMB takes congressional policy and manages its implementation within government agencies. This involves working with Chief Information Officers within government agencies to ensure that each agency complies with the policies. One of the recent responsibilities of OMB is to oversee the use of privacy assessment statements by government agencies instituted in the E-Government Act of 2002. Before OMB releases funding for a technology project, the agency must perform a privacy impact assessment to determine how the chosen project will minimize harm to privacy.

The role of the press in this issue cannot be overlooked. The press influences public opinion, and public opinion has a tremendous impact on policy makers. The group agreed that a relationship will have to be established with the press in order to promote the framework for balancing security and liberty. With the press, there is often a spotlight effect in which one or two events are given an intense focus but peripheral issues fail to get covered ("If it wasn't on TV then it didn't happen"). The group concluded

that a productive and cooperative relationship with the press should be developed to bring the issue of balancing national security and civil liberties, including its technological components, to the forefront of debate and policymaking.

"The courts have traditionally erred on the side of national security in times of national crises, and the courts will most likely continue this precedent if or when the issue reaches the judiciary."

The judiciary also plays an important role in this balance, but one of the participants stated that it cannot solve this issue. The judiciary, another participant noted, is like a "fixed cannon. It can fire cannon balls, but it can only fire at things that come before it." In other words, the judiciary cannot force this issue and thereby create a balance; it has to wait for a controversy to arise and be brought to the courts before they can enter formally into the debate. The courts have traditionally erred on the side of national security in times of national crises, and the courts will most likely continue this precedent if or when the issue reaches the judiciary. Hence, this participant concluded, "If a meaningful balance is to be found and implemented, it will take place in one of the other branches of government."

## IV. Moving Forward

The issue of balancing national security and civil liberties will not result in an end state, but rather will take constant and persistent fine-tuning. No ultimate resolution of this problem may ever be reached and the group agreed that this discussion must continue. Three ideas were presented as to how the group could proceed.

First, the group proposed the creation of a repository of ethical cases to be run under the aegis of a department of the Executive Branch. This repository would store public concerns and actual incidents regarding the government's use of information technologies and possible civil liberty violations, privacy concerns, and identity theft issues. The model for this program has already taken root within hospitals. Hospital ethics committees have been successfully implemented to alleviate worries and concerns of patients and have helped build an environment of greater trust between doctors, administrators and patients. Based on this model, the program will consist of a politically and professionally diverse committee of ethicists, technologists and government scholars who will:

1. Review the cases in the repository.
2. Help alleviate concerns the public may have regarding the government's use of information technologies.
3. Recommend government policies regarding the ethical use of technologies.
4. Help foster awareness within the government of the ethical issues facing the use of information technologies to protect the nation.

By creating a repository of cases and formulating guidelines based on the public's concerns, the group believes that a well-informed answer to the following question can be developed and deployed: How can the government maximize the benefits and minimize the harm of implementing information technology solutions in the post-9/11 era? Through collaboration among technologists, ethicists, theologians, government officials and businesspeople, the group can provide a forum for discussing the advancement of technology and its effects on ethical values. The group can help build the knowledge necessary to meet the government's objective of securing the nation without causing unnecessary harm to civil liberties.

"The group can help build the knowledge necessary to meet the government's objective of securing the nation without causing harm to civil liberties."

Second, the group suggested an expansion to incorporate a wider array of interests by joining forces with other organizations in this area like the Chief Information Officers Council and the Markle Foundation Task Force on National Security in the Information Age. This expanded group would focus on a particular project and develop a framework for it. The framework would address two objectives:

1. Clarify the national security mission of the project.
2. Define the civil liberties issues by discussing the specific goals for protecting privacy and clarifying reasonable expectations of privacy.

The group would attempt to find solutions for using technology while minimizing the harm done to privacy for specific projects of government agencies.

Third, the group agreed that a project involving the press should be deployed. As noted earlier, it is imperative that the group involve the media in the promotion of a framework for balancing security and liberty. This is the most effective means to educating the public and motivating policy makers. The group plans to start by holding small briefing sessions with select members of the press. As the discussion begins to move towards a framework for balancing civil liberties and national security, the group may start holding press briefings after its meetings. This would serve to summarize the findings of the discussion and thereby begin informing the public.

"It is imperative that the group involves the media in the promotion of a framework for balancing security and liberty."

## Conclusion

The Brookings Institution ITS, the Computer Ethics Institute, and Ascential Software Corporation held "The Challenge of Information Sharing: Balancing National Security and Civil Liberties" in order to initiate a discussion regarding how the government should use information technologies to secure the homeland. The discussion focused on three questions:

1. How can information technologies assist in maintaining a secure homeland?

2. What issues – legal, cultural, ethical – may arise from the implementation of these IT solutions?

3. What operational framework should policy makers use to assist them in maximizing the benefits and minimizing the harm of implementing these information technology solutions in the post-9/11 environment?

Among technologists, government officials, lawyers, legislators, and public policy scholars, the discussion isolated problems that are in urgent need of address and sketched a view of how to work our way towards a safe and free America. The group plans to launch a number of programs and continue to craft a framework for balancing national security and civil liberties in the government's use of information technologies in the post-9/11 era.

# APPENDIX

## Participants' Affiliations

Ascential Software Corporation

Brookings Institution

Center for Democracy and Technology

Central Intelligence Agency

Computer Ethics Institute

Defense Advanced Research Projects Agency, Department of Defense

Department of Energy

Department of Justice

Department of Homeland Security

Federal Bureau of Investigation, Department of Justice

Foreign Intelligence Surveillance Court

General Accounting Office

General Services Administration

Georgetown University Law Center

House of Representatives

In-Q-Tel

National Imagery and Mapping Agency

Office of Management and Budget

Steptoe & Johnson LLP

Brookings Institution, ITS
1775 Massachusetts Ave.
Washington, DC 20036
www.brookings.edu

Computer Ethics Institute
1750 K Street, NW, Suite 450
Washington, DC 20006
www.brook.edu/its/cei/cei_hp.htm

Ascential Software Corporation
50 Washington Street
Westboro, MA 01581
www.ascential.com