Prepared Statement of
James X. Dempsey
Executive Director
Center for Democracy and Technology

before the

House Committee on Government Reform

"Moving from 'Need to Know' to 'Need to Share:'
A Review of the 9-11 Commission's Recommendations"

August 3, 2004

Chairman Davis, Congressman Waxman, members of the Committee, thank you for the opportunity to testify today at this first hearing in the House of Representatives on the recommendations of the 9/11 Commission.

I am Executive Director of the Center for Democracy and Technology. CDT is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the digital age. Our core goals include enhancing privacy protections as government and businesses adopt new technologies for collecting and using personal information. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security issues. I am also privileged to serve as a member of the steering committee of the Markle Foundation Task Force on National Security in the Information Age and as chair of one of its working groups. The Markle Task Force, co-chaired by Zoë Baird and Jim Barksdale, is comprised of leading experts from the fields of national security, technology, and privacy, including CDT's President Jerry Berman. Its members have extensive experience in and out of government at the federal and state level, in both the legislative and executive branches, from the administrations of Presidents Carter, Reagan, George H.W. Bush and Clinton. The Task Force has published two reports, "Protecting America's Freedom in the Information Age" (2002) and "Creating a Trusted Information Network for Homeland Security" (2003).[1] The Task Force, which is continuing its work, has offered concrete recommendations for strengthening national security while protecting civil liberties by creating a decentralized network for sharing and analyzing information within a framework of accountability and oversight.

Terrorism poses an imminent and grave threat to our nation. Hostile groups are continuing to plan attacks in this country and abroad. To prevent terrorism to the greatest extent possible and to swiftly punish it when it occurs, the government must have adequate legal authorities and must develop a strong organizational structure. Improved

[1] *Available at* http://www.markletaskforce.org.

intelligence collection and better sharing of information are central to success. Information sharing will be effective only if –

- it is managed well, with some entity within the Executive Branch having clear responsibility for setting standards and ensuring implementation;
- it takes full advantage of available technology, which can be leveraged both to facilitate appropriate information sharing and to protect privacy; and
- it is subject to guidelines and oversight mechanisms that will protect civil liberties.

The importance of protecting civil liberties bears emphasizing as Congress and the President move forward implementing the recommendations of the 9/11 Commission. Privacy protection, checks and balances, accountability and redress are not incompatible with effectively fighting terrorism. To the contrary, clear guidelines and oversight mechanisms are part of the solution. As the 9/11 Commission stated: "The choice between security and liberty is a false choice." The shift in government power and authority that is occurring in response to terrorism, the 9/11 Commission concluded, "calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."

This conclusion – that privacy protection and accountability must be built into the design and implementation of counterterrorism information sharing systems -- is central to the recommendations not only of the Markle Task Force but also of other recent bi-partisan expert bodies that have taken the time to carefully study information technology and its role in fighting terrorism. "We must not sacrifice liberty for security," concluded the Technology and Privacy Advisory Committee (TAPAC) appointed by Secretary of Defense Rumsfeld to study the Total Information Awareness program and related activities. Likewise, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by former Virginia Governor James Gilmore, repeatedly stressed that personal freedoms must be at the foundation of the nation's efforts to counter terrorist threats.[2]

The elements of an effective oversight and accountability framework must involve each branch of government, as well as the public, and should include:

- clear and publicly available guidelines on the collection and sharing of information to ensure investigative focus and prevent fishing expeditions;
- robust and regularized periodic internal audits of information collection, retention and dissemination;
- privacy technology – anonymization, permission controls, audit trails -- built into the design of information sharing systems;
- more effective congressional oversight;

---

[2] The five reports of the Gilmore Commission are available at http://www.rand.org/nsrd/terrpanel/.

- due process redress mechanisms when individuals face adverse consequences from the use of information.

Sharing Information More Efficiently

In the past three years, steps have been taken at the federal, state, and local levels to broaden the sharing and improve the analysis of terrorist-related data among government agencies at all levels. To date, however, the government still does not have a dynamic, decentralized network for sharing and analysis of information. The sharing of terrorist-related information between relevant agencies at different levels of government is still dependent on multiple systems that cannot communicate with each other and still limited by institutional and technical barriers. Fragments of data collected by different agencies are likely to remain in different places with no way to find them and therefore no way to make sense of what is happening.

A key finding of the Markle Task Force is that technologies exist *today*, *off-the-shelf*, that can both facilitate information sharing and protect privacy. The second Markle Task Force report explains in detail how commercially available technologies can be adopted to create a government-wide information sharing network. The Task Force calls this the SHARE Network, for "Systemwide Homeland Analysis and Resource Exchange Network." It is intended to foster better analysis and sharing of information among all relevant participants at every level of government, with built-in practical and technological safeguards for civil liberties.

The SHARE Network would represent a fundamentally new way of using information to facilitate better, faster decision-making at all levels of government. It has several key features:

- SHARE is a decentralized, secure network that sends information to and pulls information from all participants in counterterrorism efforts, from local law enforcement officers to senior policy makers.
- SHARE is based on the concept of "write to share." Instead of the Cold War culture that placed the highest value on securing information through classification and distribution restrictions, SHARE uses an authorization system .to encourage reporting that contains the maximum possible amount of sharable information. Organizations that originate information would not exercise the kind of control over its dissemination they did in the past. "Write to share" nevertheless allows for tear lines to protect sources and methods.
- SHARE is a hybrid of technology and policy. The system would use currently available technology to share and protect the information that flows through it. And when paired with clear guidelines that would determine the collection, use and retention of information and who should have access to information, it can both empower and constrain intelligence officers, and provide effective oversight.

- SHARE allows for vertical and horizontal co-ordination and integration. Information would be able to flow not just up the chain of command, but also horizontally, to the edges of the system.
- SHARE enables analysts, law enforcement agents and other experts to find others with common concerns and objectives, to come together in "virtual," informal teams to exchange information and ideas.

Many of these principles are reflected in the information sharing recommendations of the 9/11 Commission report, which calls for the horizontal sharing of information across new networks that transcend individual agencies. The Commission summarized the decentralized network model at the core of the SHARE Network concept:

> "Agencies would still have their own databases, but those databases would be searchable across agency lines. In this system, secrets are protected through the design of the network and an 'information rights management' approach that controls access to the data, not access to the whole network. An outstanding conceptual framework for this kind of 'trusted information network' has been developed by a task force of leading professionals in national security, information technology, and law assembled by the Markle Foundation."

The tools for this kind of system are readily available. They include common interfaces; directories and pointers; federated search engines; information resource management technologies, anonymization tools, , auditing systems, and other technologies that facilitate sharing and collaboration. What is needed is the leadership to force adoption of these technologies and to guide their implementation in a way that respects privacy and due process. Under the structure recommended by of the 9/11 Commission, that should be an important responsibility of the new National Intelligence Director,.

Senators Collins and Lieberman have introduced S. 2701, the Homeland Security Interagency and Interjurisdictional Information Sharing Act of 2004, legislation that would create the SHARE Network, even using the name adopted by the Markle Task Force. The bill, in addition to providing resources to help first responders and preventers to purchase the interoperable communications equipment they need to execute effective emergency responses, would require the Secretary of Homeland Security, with intelligence and other federal agencies, to establish a SHARE Network to assist in the sharing of homeland security information among all levels of government.

Privacy and Due Process Guidelines

Government use and dissemination of personal information raises privacy and related due process issues. Appropriately, therefore, the 9/11 Commission recommended, "As the President determines the guidelines for information sharing among government

agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared."

The "wall" that previously separated law enforcement and intelligence agencies is down. No one is proposing re-constructing it. Foreign intelligence agencies and domestic law enforcement and intelligence agencies are sharing information. On the collection side, government agencies have expansive authority. Communications intercepts under the criminal wiretap law increase almost every year. There have been even more dramatic increases in recent years under the Foreign Intelligence Surveillance Act. In this information age, vast quantities of data are generated as we go about our daily lives – records about travel, store purchases, credit, financial and medical matters. Under current law, there are few restrictions on the government's ability to gain access to this kind of information for counterterrorism purposes. The Privacy Act and other privacy laws are not adequate for the modern digital data environment.

The government undeniably needs access to information to prevent terrorism. However, the Markle Task Force concluded that different considerations apply to the government's 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, 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. Therefore, the Task Force concluded, the government should not have routine access to personally identifiable information even if that information is widely available to the public. At a minimum, the Task Force concluded, that information should be collected by the government only if it is relevant to preventing, remedying, or punishing acts of terrorism and that this showing should be documented and subject to periodic audit. Markle Task Force, "Creating a Trusted Information Network for Homeland Security" (December 2003) at pp. 33-34.

Similarly, the Defense Secretary's TAPAC recommended that government access to personally identifiable information, wherever located, should be subject to clear rules and meaningful oversight. At a minimum, even access to "publicly available information" should be subject to written authorization and compliance audits. The approval process should specify, among other findings, the need for the data, that the data are necessary and appropriate fro the intended use, the consequences that will flow from use of the data, that the approach has been demonstrated to be effective, and that there is a system in place for dealing with false positives. For all other government data mining efforts involving personally identifiable data about U.S. persons, the TAPAC recommended that government access should be permitted only pursuant to a court order. TAPAC, Safeguarding Privacy in the Fight Against Terrorism (2004), at pp. 47-52.

In framing the guidelines recommended by the 9/11 Commission and the Markle Task Force, it should be made clear that the collection under counterterrorism authorities of personally identifiable information about U.S. persons or within the United States should be in accordance with priorities established nationally through a clear and politically accountable process, possibly by the new National Intelligence Director.) As a

minimum standard, the guidelines should specify that personally identifiable information regarding U.S. persons should be collected for counterterrorism purposes only if relevant to preventing, remedying, or punishing acts of terrorism. Compliance with this standard should be subject to audit, and collection should be conducted in such a way as to minimize the impact on privacy of persons not suspected of any involvement in terrorism.

The guidelines should implement these principles through oversight procedures and privacy-protective technologies, including:

- anonymization technologies that can minimize unnecessary disclosure of personal information not relevant to counterterrorism purposes;
- search and sharing techniques that can leave information with the originator and minimize unnecessary transfers of data to central repositories;
- strong data quality and corrective mechanisms, including automated mechanisms that can identify and correct errors in shared data that may cause harm to individuals;
- access control and permissioning technologies that can protect against improper access to personal information, including the ability to restrict access privileges so that data can be used only for a particular purpose, for a finite period of time, and by people with the necessary permissions;
- automated audit trails that can protect against misuse of data, improve security, and facilitate oversight; and
- oversight processes and redress mechanisms within each participating department and agency.

Internal review and approval procedures ensure that agents are focusing on priority issues and promising leads, while clear rules empower agents to take actions without fear that they will be second-guessed. Such rules and procedures can both define clear limits and avoid irrationally tying the hands of investigators. These internal guidelines should be made public. Few *procedural* rules have national security implications requiring them to be classified, and public confidence and trust will grow with a full understanding of the policies in place to protect the public – both from a terrorist attack and from an overzealous intelligence agent.

Accountability and Internal Oversight

The Markle Task Force emphasized, "Guidelines must also address the question of how we assure compliance with the required polices and procedures and foster accountability." The 9/11 Commission has recommended the creation of a board within the executive branch to oversee adherence to the guidelines and the commitment the government makes to defend civil liberties. This may be desirable, but is probably not sufficient. As the Markle Task Force concluded in the context of use of private sector data, in a decentralized system, there is no single entity with the ability to monitor day-to-day decisions to acquire, retain or disseminate information. Therefore, the Task Force recommended a blended system. Government-wide rules will be necessary, and some agency must have overall supervisory responsibility to oversee the application of the

guidelines, including the training of personnel, the implementation of auditing procedures, and the imposition of consequences for failure to comply. At the same time, each agency has the responsibility to develop its own procedures to ensure compliance.

Several mechanisms are available. Congress, in creating the Department of Homeland Security, created a privacy officer and a civil rights and civil liberties officer. Earlier this year, I testified that, based on the short but significant record of the DHS Privacy Office, it is clear that a statutory Privacy Officer, participating in senior level policy deliberations and using the tools of the Privacy Act notices and Privacy Impact Assessments, can be an important mechanism for raising and mitigating privacy concerns surrounding the government's use of personal information. Legislation has passed the House to create a Privacy Officer for the Department of Justice and other legislation has been introduced to create a privacy officer at OMB and each cabinet agency.[3] The Inspectors General will also have a role to play. Inspectors General, in particular, provide a critical internal ability to identify civil liberties violations, and should regularly review agency actions to assess their privacy implications. Inspector General reports and other internal reviews should not only identify vulnerabilities and mistakes, but should also provide recommendations for avoiding them in the future. They should not only respond to public outcries; they should also regularly review agency effectiveness and safeguards to constantly improve operations and safeguards.

Technology can also be built into information systems to assure accountability and transparency. For example, personally identifiable information can be anonymized so that identity is not revealed. Auditing technology, too, can provide built-in recordation and documentation capabilities to track how information is used, and shared. Strong auditing capabilities could also allow individuals to make Privacy Act and FOIA requests to see what was done with data about them. Markle report, p. 35..

Another aspect of oversight is ensuring the accuracy of data brought into the system. Accuracy is vital not only to protect the privacy and civil liberties of individuals who can be harmed by inaccurate data, but also to ensure that information has real value to the counterterrorism effort. "False positives" that mistakenly suggest that an innocent person is somehow tied to terrorism can have significant adverse consequences for the individual involved. They can also waste scarce investigative resources. Technologies can help assure that information is up-to-date. Software can ensure that information is

---

[3] Section 305 of the Department of Justice Appropriations Bill (H.R. 3036) requires the Attorney General to appoint a Privacy Officer for the Department of Justice. The bill was passed by the House but has yet to be introduced in the Senate.

On May 20, Reps. Meek and Turner introduced the SHIELD Privacy Act (H.R. 4414), which would require the President to appoint a Chief Privacy Officer at OMB, the head of each federal and independent agency to appoint a privacy officer; and would establish a Commission on Privacy, Freedom, and Homeland Security to conduct a comprehensive study of U.S. efforts to further homeland security in a manner that protects privacy, civil liberties, and individual freedoms.

updated regularly and that it is unusable after a certain date if not refreshed. Other technology can permit users to track where information came from and who received it and alert users if the original data is subsequently disproved or corrected.

Finally, oversight includes redress – processes that allow individuals to respond when they are about to face adverse consequences based on information. This includes the right to challenge inaccurate information.

Oversight and accountability, done right, will benefit both national security and civil liberties. Not only will appropriate, well-implemented accountability mechanisms *not* impede intelligence operations, they will actually help to ensure that failures do not occur. Checks and balances result in clear lines of responsibility, well-allocated resources, protection against abuse, and the ability to evaluate and correct past mistakes.

Congressional Oversight

The 9/11 Commission calls for more effective Congressional oversight. Non-partisan Congressional oversight is one of the pillars of a system of checks and balances. The Markle Task Force has not explored this area in depth. The 9/11 Commission report leads to the conclusion, I believe, that the oversight committees should hold more public hearings and should conduct annual reviews and issue public reports on the impact of counterterrorism efforts on privacy and civil liberties. If the Intelligence Committees are to get more deeply into the details of intelligence operations, they need to assess the civil liberties implications of those operations as well. The Commission recommends the consolidation of oversight efforts but also expressly calls for the creation of a subcommittee dedicated specifically to oversight, freed from the consuming responsibility of working on the budget. Among the duties of this entity should be the monitoring of civil liberties issues.

CONCLUSION

We now have the possibility of achieving a major enhancement in our nation's security by development of an information sharing network based on write for release. An integral part of that revolution must be the establishment of checks and balances to preserve civil liberties. As policymakers seek to reform the Intelligence Community and enhance information sharing and analytical capabilities, they need not do so at the expense of civil liberties.