MARKLE FOUNDATION

United States Senate Committee on the Judiciary
Written Testimony Zoë Baird[1] and Slade Gorton[2]
Markle Foundation Task Force on National Security in the Information Age
January 20, 2010

We would like to thank Chairman Leahy and Ranking Member Sessions for holding this hearing and dedicating their time and energy to the critical issue of improving information sharing. Since 2002, the Markle Foundation Task Force on National Security in the Information Age has pursued a "virtual reorganization of government" that uses the best technology to connect the dots and the best management know-how to get people working across agency lines to understand the meaning of fragments of information. We are submitting this testimony as follow-up to our April 21, 2009 testimony before the Terrorism and Homeland Security Subcommittee at their hearing entitled "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing."

In the wake of the attempted Christmas Day attack on Flight 253, it is essential to distinguish between amassing dots and connecting them. Information sharing is a means, not an end. The end goal is production of actionable intelligence derived from a form of collaboration that leads to insight and action. The information the Director of National Intelligence reports to the President in his daily briefing is only as good as the information sharing that underlies it.

[1] President of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies to address critical public needs, particularly in the areas of health care and national security.

[2] Senator Gorton served in the United States Senate for 18 years representing Washington state and currently practices law at K&L Gates LLP. He has served on the Markle Task Force since its inception and was a member of the 9/11 Commission.

The President and Congress need to hold a small number of top officials accountable for improving the knowledge he receives from information across the entire government.

As President Obama recognized in his speech on January 7th, the key to achieving this is leadership on a continuing basis. In that respect, this Committee has an important role to play. The Markle Task Force has **five concrete recommendations** to address the cultural, institutional, and technological obstacles that prevented the government from taking full advantage of information that could have helped prevent Umar Farouk Abdulmutallab from boarding a Detroit bound flight with explosives. These recommendations build on the Markle Task Force's past work, which was embraced by the 9/11 Commission and the Weapons of Mass Destruction Commission and was enacted in the intelligence reform laws passed since the September 11th attacks. Our Task Force, composed of national security policy makers from every administration since the Carter Administration, civil liberties advocates and information technology experts, has released four reports and has worked closely with Congress, the Obama administration, and the previous administration. The five recommendations outlined below are detailed in the Task Force's March 2009 report, which we would like to submit for the record.

First, strong sustained leadership from Congress and the President is required. Urgency has been lacking. The Task Force takes heart from the President's leadership on this issue and the fact that you are holding this hearing to reaffirm information sharing as a top priority. Congressional oversight will be critical to ensure that government-wide efforts are being coordinated effectively.

We further believe that it is imperative that there be an official within the Executive Office of the President ("EOP") with adequate horsepower to drive interagency coordination at a senior level. Senior leadership from within the EOP will provide government-wide authority to coordinate information sharing policies and the White House backing to overcome the bureaucratic resistance that persists today. This official would benefit from budget certification authority.

Second, while it is important to immediately address the gaps exposed by the most recent attack, the larger goal should be transformation of how government does business. The Markle Task Force envisions information sharing as a means to change the way government does business by creating a distributed network across all agencies, not just the Intelligence Community, that allows teams working on a problem to form quickly and discover relevant information. The failure President Obama identified to "connect and understand" the intelligence that we already had can only be corrected through an information sharing framework that enables collaboration.

Too often information sharing has become simply passing dots to another agency where they are amassed and not properly analyzed. The problem is not the failure to share, but the failure to take responsibility for learning what others know when critical information is discovered. We need to eliminate the belief that the job is done once the information has been shared with the National Counterterrorism Center ("NCTC") or another agency.

More follow-up is required to avoid this type of "systemic failure" in the future. The information sharing framework should facilitate such follow-up. For example, when new information comes into NCTC on a person who is already in the centralized TIDE database on terrorist identities, NCTC should alert the agency that originally submitted the data that caused the person to be in TIDE that a second agency has now submitted related information.

Consistent with the President's January 7, 2010 Directive, there should be some responsibility on those two agencies to work together to "run down the lead," but first they have to know that they are interested in the same person or topic. Such real-time, virtual collaboration promotes agile decision making by eliminating the seams between departments and agencies that are often exploited by our enemies. Technology exists to facilitate this critical collaboration.

Third, we recommend that all information within this distributed environment be made "discoverable" to facilitate quickly piecing information together. The information sharing framework envisioned by the Markle Task Force would allow "data to find data" so that opportunities for action are not missed. At the moment something is learned an opportunity exists to make sense of what this new piece of data means and respond appropriately, but the sheer volume of data makes it impossible for humans to piece every new bit of information together by hand. This process can be automated using existing technology so that a notification is sent to users when new information reveals a connection that may warrant action. The Task Force's concept of discoverability allows an arriving piece of data to be placed automatically so that insight will emerge from the system for the analyst's use. Using such a decentralized system of discoverability simultaneously improves security and minimizes privacy risks by avoiding bulk transfers of data. To achieve this, data should be tagged with standardized information that can be indexed and searched.

When the December 25th bomber was added to the TIDE database, it was instantly knowable that this individual had been approved for a U.S. multiple-entry visa, but no mechanism was in place to trigger reconsideration of the previously granted visa as a result of changes in TIDE. Such a mechanism could be implemented if TIDE were enhanced to allow for "persistent queries." A persistent query requires TIDE (or other databases) to remember the questions it has been asked in the past (*e.g.* the State Department checking the database as part of reviewing a visa application), so that if something changes in TIDE, a trigger notifies the person who asked about that individual weeks or months ago. Such triggers can help manage the mountains of dots collected by the U.S. government by highlighting new information for select individuals who have previously expressed interest in a topic, like Amazon.com recommending a new book based on the user's order history. This system of discoverability allows new information to be put in context with what we already know. Without context at the point of decision making, critical information may seem of interest, but not worthy of action.

Fourth, discoverability should be combined with a standard of Authorized Use. Authorized Use provides a standard to determine whether a user is authorized to see what has been discovered. Like a library card catalogue that offers information on books, but not the books themselves, discoverability offers users the ability to "discover" data without gaining access until it is authorized. This Authorized Use standard would overcome obstacles in the present system of classification and permit an agency or its employees to obtain information based on their role, mission, and a predicated purpose.

Congress requested a study of the feasibility of this standard in the Implementing Recommendations of the 9/11 Commission Act of 2007.[3] The Program Manager for the Information Sharing Environment discussed what he viewed as potential obstacles to implementation of an authorized use standard in his 2008 Feasibility Report. We believe this assessment should be revisited.

Fifth, government-wide privacy and civil liberties policies for information sharing must be developed to match increased technological capabilities to collect, store, and analyze data. Consistent policies are needed, but, today, each agency or department has been

[3] 6 U.S.C. § 485(j)(C) (calling for a "standard that would allow mission-based or threat-based permission to access or share information . . . for a particular purpose . . . (commonly known as an 'authorized use' standard)").

tasked to write their own policies on privacy. We must avoid the next failure that is based on an agency saying they weren't authorized to use information on U.S. persons, for example. The new government-wide policies should be clear, detailed, transparent, and consistent while allowing agencies the flexibility that their different missions and authorities require. They must provide direction on hard issues, rather than simply stating that agencies must comply with the Privacy Act without explaining how to do so. Such policies are necessary both for the American people to have confidence that their government is protecting their civil liberties and to empower the participants in the information sharing framework so they have confidence that their work is lawful and appropriate.

The President and Congress should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs.

Finally, the information sharing framework should take advantage of technological tools to build new and more powerful privacy protections into the system and minimize the risk of unintended disclosure of personally identifiable information. There are now a number of commercially available technologies, including anonymization, strong encryption, and digital rights management, that can enhance both privacy and security simultaneously.

***

Our enemies will continue to adapt. The next attack may not come from the air. Improved information sharing is a long-term strategic tool that will allow the U.S. to stay one step ahead of its enemies whether they are attempting to attack our critical infrastructure in cyberspace, deploy biological weapons, or smuggle explosives through airport security.

This Committee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing. We commend this Committee for its leadership on these issues, but much more needs to be done.

The Task Force is committed to continuing to work with Congress and the Obama administration to find practical solutions to this critical national security challenge.