

**Statement of James X. Dempsey\***  
**Policy Director**  
**Center for Democracy & Technology**

**on behalf of**

**the Markle Foundation Task Force on National Security in the Information Age**

**before the**

**President's Privacy and Civil Liberties Oversight Board**

**"Privacy and Information Sharing for Counterterrorism"**

**December 5, 2006**

Madame Chair, members of the Board, colleagues, good afternoon. Thank you for the opportunity to participate in this public panel. I am Policy Director of the Center for Democracy and Technology and I am here today to speak on behalf of the Markle Foundation Task Force on National Security in the Information Age. I submitted, through the staff, a statement for the record, consisting of excerpts from the Task Force's third report, which I will not read now, but instead I will address some key issues and then look forward to responding to your questions.

First of all, congratulations on holding this public meeting. It is part of a broader, very important process of dialogue as our nation strives for answers to some of the challenging questions posed by the war on terrorism. The Markle Task Force, in its third report, stated, "We urge our government to engage in a public debate, to the extent possible while maintaining national security, about the guidelines and rules that govern information sharing. This debate should also seek to clarify agency missions and address the requisite civil liberties and privacy protections." This debate, of course, will occur and should occur in multiple forums, this Board being one of them.

I will focus my comments today, as the Markle Task Force has done in its work, on the question of information sharing. Earlier this year, in its third report, the Task Force called for renewed commitment to the establishment of the Information Sharing Environment (ISE), which the Task Force recommended in its second report (2004) and which was mandated by the Intelligence Reform and Terrorism Prevention Act of 2004.

In recent weeks, two important steps have been taken in the development of the ISE. Those two steps were, first, the issuance last month of the Information Sharing

---

\* This is an edited and revised transcript of oral comments given to the President's Privacy and Civil Liberties Board.

Environment Implementation Plan and, second, the issuance just yesterday of initial privacy guidelines for the ISE. Primarily, I'm going to talk about the guidelines.

It is important at the outset to recognize what the ISE privacy guidelines do not address. First of all, they do not address collection standards. In particular, they do not address the standards and process for the initial collection of information. The Markle Task Force did not address this question in-depth either, but the Task Force did stress that there had to be a predicate for any collection of personally identifiable information.

The guidelines also do not address the question of agency roles and missions. This is an issue that the Markle Task Force did address, for the Task Force believed that the development of a process for better sharing terrorism-related information while also better protecting civil liberties required, among other things, a clarification of "authorized uses" of intelligence regarding individuals, which in turn requires careful consideration and definition of the appropriate roles and missions of agencies and offices engaged in counterterrorism. The question of roles and responsibilities is addressed neither in the Information Sharing and Implementation Plan nor in the Privacy Guidelines. Those questions include: Which agencies have which missions? Who is responsible for the collection of intelligence information, particularly inside the United States or against U.S. persons? What is the role of the military in domestic intelligence? What does domestic intelligence mean? Until those questions can be answered, they will be left to the assertions of individual agencies, with the risk not only of civil liberties intrusions but also duplication of effort and the expenditure of resources on non-productive forms of information gathering and analysis.

Also it is important to recognize the limitations of what was issued yesterday. The guidelines are appropriately described as a "framework." They focus more on process than on substance. To take just one relatively small example, the guidelines issued yesterday state that agencies shall, "Take appropriate steps when merging information about an individual from two or more sources to ensure that the information is about the same individual." Now, first of all, we would expect that the agencies are taking steps to improve their ability to match information about individuals. More fundamentally, however, the guidelines do not offer any guidance to the agencies about how to actually improve their practices. So the guidelines tell the TSA, for example, to be careful when matching Ted Kennedy on the terrorist watch list with Ted Kennedy on the flight to Massachusetts, but they did not begin to tell TSA or any other agency how to actually go about doing that.

To take another example, the guidelines appropriately say that each agency shall implement adequate review and audit mechanisms to ensure compliance with the guidelines. But the guidelines do not have any specificity as to what is an adequate audit, what agencies should be auditing for, who should be audited, or who should have access to the audits. The Markle Task Force, in its third report on pages 67 through 70, gave some concrete recommendations as to how auditing should be conducted, not only at the agency level but at the individual level and what are some of the technologies for carrying out auditing.

A third example: The guidelines call for redress mechanisms to be put in place to address complaints from persons regarding protected information about them that is under an agency's control. Again, however, the guidelines offer no further details on how to go about setting up a redress mechanism. In particular, they don't address the threshold problem, which is that a number of agencies won't even tell you in the first place whether they have information about you or not. How can you exercise a redress right if you don't know what information exists about you and what it says? For example, it has been revealed recently that the Department of Homeland Security through Customs and Border Protection Bureau is conducting risk assessments of all people entering and leaving the country, including citizens. The Privacy Act notice for those risk assessments specifically purports to exempt them from the Privacy Act's rule that a person has the right to see information about himself, a right upon which redress normally hinges. Of course, there will be circumstances in which the government cannot tell a person what it knows about him, but in those circumstances there has to be some alternative redress mechanism, and the guidelines offer no guidance on how to reconcile the tension between secrecy and redress.

In sum, the guidelines have little to say about what agencies should be doing differently than they are doing now. We have to look at the guidelines as the beginning of a process and the challenge, really, is to put some meat on these bones. I see the need for a process that would take each one of the hard issues -- data accuracy, entity resolution or watch list fidelity, auditing -- and develop more detailed guidance, leading to a set of appendices or attachments to the guidelines. In its third report, the Markle Task Force stressed that guidelines such as these will have to be developed incrementally. Specifically, the Task Force said,

“In an area this complex and dynamic and so affected by evolving threats and rapidly changing technologies, the guidelines should be revisited at regular intervals to determine what is working, what is not, what needs to be changed or improved. There inevitably will be ambiguities or unanswered questions. These should be addressed explicitly, not ignored or exploited to avoid the laws' requirements. We recommend an annual or biannual review of guidelines by the DNI or other senior Executive Branch official charged with overseeing their implementation.”

Speaking for CDT, I look forward to contributing to that process and I know that other members of the Markle Task Force also remain committed to working to resolve the hard issues. Representatives of the Privacy Officer at the DNI have already called me to say that they want to convene such a meeting, which I will be pleased to attend, and I think really should be seen as the first in a series of meetings and a process to put some meat on these bones.

I would like to address another aspect of the Markle Task Force's third report and that is our recommendation on “U.S. persons” data, which is one of the hardest issues facing information sharing initiatives. The Task Force recommended the development of an

“authorized use” standard for sharing and accessing information lawfully collected by or available to the U.S. Government. That is, once the government has information about U.S. persons, how can it be shared? We did not recommend abandonment of the concept that U.S. persons are entitled to special protection in the collection or processing of data. We did not recommend lowering standards on collection of U.S. person data and we did not recommend the expansion of agency missions to permit targeting of U.S. persons, for example, by agencies traditionally focused overseas. Consistent with those positions, the guidelines that were issued yesterday were premised upon the principle that U.S. person data merits special treatment.

What the Markle Task Force said is that authorized uses are mission or threat-based permissions to access or share information for a particular purpose that the government, through an appropriate process, has determined beforehand, is lawfully permissible for a particular employee or a particular unit or a particular component, a particular agency. The guidelines issued yesterday talk about purpose specification but they say that each agency shall adopt internal policies and procedures requiring it to ensure that the agencies’ access to and protected use of information available through the ISE is consistent “with the authorized purpose of the ISE.” But the ISE has the very broad purpose of promoting the sharing of information relevant to terrorism. What the rules should really say is that agencies must ensure that the receipt of information or the sharing of information is consistent with the authorized purpose and mission *of the receiving (or requesting) agency*.

In the Markle Task Force report, we provided some examples of how an authorized purposes standard would work. For example, the CIA is generally prohibited from collecting intelligence inside the United States. However, if some U.S. person data collected by another agency is relevant to some overseas activity of the CIA, such as the tracing of terrorist financing overseas, then under our proposed authorized purposes standard it would be appropriate to share that U.S. person related data with the CIA, not for the purpose of the CIA operating domestically but for the CIA to use in its mission to investigate terrorist financing overseas.

I want to highlight what I think is one potentially very important element of the guidelines issued yesterday, Section 4, on page 3, which requires each agency to identify its data holdings that contain U.S. person data that might be shared through the ISE and to identify specifically the rules within the agency that govern the use and sharing of that information. This catalogue of information will be very helpful, not only to the agency privacy officers, not only to this Board, not only to the program manager for the ISE but also to the agencies themselves, so they can get a sense of what they their counterpart agencies hold as well as to the DNI and to Congress.

The Markle Task Force called for careful monitoring and oversight of the implementation and actual uses of the Information Sharing Environment. The guidelines, of course, are only a day old and they were issued, I think, with the understanding that they would be re-examined and improved, now that they are out there in the public light. The Markle Task Force had urged that the guidelines be issued for public comment before they were

finalized, and they would have benefited from such input, but I understand to some extent the sort of Executive Branch issues at stake in drafting documents internally, but now that we have these guidelines, let's all engage with them and take them to the next level. Obviously, there is a need for ongoing oversight by this board and others and for much greater detail than we see in the guidelines issued yesterday. We welcome them as an important step but only as an initial step. With that, Madame Chair and Members of the Board, I look forward to your questions.