Center for National Security Studies
Protecting civil liberties and human rights

Advisory Board Chair
Morton H. Halperin

Director
Kate Martin

Statement for the Record

Kate Martin
Director, Center for National Security Studies

Before the Senate Select Committee on Intelligence
Hearing on Reauthorization of the USA Patriot Act

April 19, 2005

Sections 203 and 905 concerning Information Sharing

While effective counterterrorism and counterintelligence require that agencies share relevant information, sections 203 and 905 of the USA Patriot Act fail to address the real difficulties in such sharing: How to determine what information is useful for counterterrorism and counterintelligence; how to determine what information would be useful if shared; how to identify whom it would be useful to share it with; and how to ensure that useful and relevant information is timely recognized and acted upon. To the contrary, the approach of the Patriot Act – which can fairly be summarized as share everything with everyone – can be counted on to obscure and make more difficult the real challenge of information sharing.

Widespread and indiscriminate warehousing of information about individuals violates basic privacy principles. Amending the Patriot Act to require targeted rather than indiscriminate information sharing would restore at least minimal privacy protections and substantially increase the likelihood that the government could identify and obtain the specific information needed to prevent terrorist acts.

Section 203 of the USA Patriot Act allows unrestricted sharing of sensitive information gathered by law enforcement agencies with the CIA, the NSA, immigration authorities, the Secret Service, and White House officials. Such sharing is not limited to officials with responsibility for terrorism matters, nor are there any safeguards regarding the subsequent use or dissemination of such information by such officials (so long as the use is within the official duties of the recipient). Section 203 allows the sharing of all information that is in any way related to any American's contacts with or activities involving any foreign government, group, or individual. (Section 203 allows the sharing of "foreign intelligence information," "foreign intelligence" and "counterintelligence." The definition of "foreign intelligence information" included in section 203 is tied to threats and potential threats of terrorism, sabotage and clandestine intelligence-gathering, the national defense and foreign affairs, § 203(a)(1)(iv), 203(b)(2)(C), and 203(d)(2). However, the definitions of "foreign intelligence" and "counterintelligence" are not even that limited.) Section 203 applies to all intercepts of

telephone conversations. It applies to all confidential information obtained by a grand jury, which has the power to subpoena virtually any records or testimony from any person merely at the request of a prosecutor.

Section 905 overlaps with section 203, but makes such sharing *mandatory*. It requires the Attorney General and the head of any other law enforcement agency to "expeditiously disclose" to the Director of Central Intelligence (and now the new Director of National Intelligence) all "foreign intelligence" acquired during a law enforcement investigation. The Attorney General may exempt only those classes of foreign intelligence whose disclosure "would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests." Section 905 suffers from the same defects as section 203: it covers the most sensitive grand jury information and wiretap intercepts regardless of relevance, and contains no limits on the use or redisclosure of the information by intelligence agency staff. "Foreign intelligence" includes anything related to any American's contacts with a foreign government, group or person.

The Act sets no standards or safeguards for use of this information. While it requires the Attorney General to issue rules, those rules simply require that information concerning citizens and legal permanent residents be marked as such. Existing intelligence agency protocols are so broad as to allow intelligence agencies to keep all information obtained under section 203 or 905. *See* EO 12333 section 2.3.

Two and a half years after the passage of the Patriot Act, the 9/11 Commission staff confirmed that "there is no national strategy for sharing information to counter terrorism." The Department of Justice has yet to explain how these Patriot Act provisions will focus the bureaucracies on identifying what information is useful to locate actual terrorists, analyzing that information, and determining what actions to take based on the information. To the contrary, the provisions essentially direct agencies simply to dump massive volumes of unanalyzed information on other agencies. They facilitate the construction of a vast intelligence database on Americans. And they effect an extraordinary change in the capability and authority of the foreign intelligence agencies, including the CIA, to keep information on Americans.

Congress should amend both sections 203 and 905 to provide some simple privacy safeguards, which will also ensure that information sharing is done in a more effective way.

Current law offers no protections against abuse. Too much information may be turned over to the CIA and others, including virtually all information about any American's contacts with any foreigner or foreign group, including humanitarian organizations, for example. Existing rules provide virtually no protection against authorized government compilation of dossiers on millions of Americans and use of those dossiers in intelligence operations.

Congress could provide some modest protections. The amendments proposed below – limiting shared information to information relating to terrorism or counterintelligence, limiting its dissemination to officials working on those matters, requiring judicial approval, and requiring marking to prevent redissemination – would not interfere with the needs of counterterrorism or counterintelligence.

While the Justice Department claims that any modifications to the information-sharing provisions would mean that agencies "would be required to identify proper legal authority prior to sharing or disseminating information outside of the collecting agency or community," such objection misses the point. *See* Justice Department, USA Patriot Act: Sunsets Report, April 2005. The proposed amendments would not change the legal authorities for sharing information, they would simply help ensure that information is actually analyzed and determined to be useful to counterterrorism and counterintelligence. None of the uses of information outlined by the Justice Department in its Patriot Act report would be prohibited because all of them relate to terrorism.

But Congress should act to ensure that those agencies which first obtain information and are best positioned to understand its context do the work necessary to determine whether the information may be useful or relevant to other agencies. When in doubt, they should of course err on the side of transferring the information, but they should exercise some judgment in doing so. Ideally, they should describe the potential usefulness of the information when distributing it to other agencies. We note that intelligence officials are already reporting that under the current regime there is too much indiscriminate sharing of useless information.

Specifically Congress should consider the following modifications.

1. When information is gathered pursuant to judicial power, the court's approval should be required before transferring the information to intelligence agencies, White House personnel, or other law enforcement agencies in order to ensure that there is some real need for more widely distributing the information. Accordingly, court approval for sharing criminal wiretap intercepts of conversations and e-mail and secret grand jury information should be obtained, except when there is no time to obtain such approval in order to prevent an imminent terrorist act or the flight of a suspect.

2. The information that should be shared with the intelligence agencies, the White House, etc., should be limited to information relevant to terrorism or counterintelligence, rather than all information concerning any foreign contacts, the vast majority of which have nothing to do with terrorism. If the information transferred by law enforcement to the intelligence community were limited to "foreign intelligence information" as that term is defined in the Foreign Intelligence Surveillance Act, it would offer some protection against the CIA and others constructing a database on the domestic activities of Americans. This safeguard was included in the Patriot Act, HR 2975 (107 Cong.), as approved by the House Committee on the Judiciary in October 2001.[1]

3. The information should be shared only with those officials who are directly involved in terrorism or counterintelligence.

4. There should be procedures for marking and safeguarding the shared information so these limits can be enforced and to protect against the redissemination of the information beyond

[1] See, H.R. REP. No. 236, 107th Cong., 1st Sess., pt. 1 (2001), at 8, available at http://judiciary.house.gov/legacy/107-236p1.pdf.

these limits, much as classified information is marked and stored. Confidential grand jury information should be marked as such and intercepts of Americans' conversations and e-mails should be marked to prohibit indiscriminate circulation.

Conclusion:

One of the most basic protections against government abuses has been the principle that a government agency should only collect information about individuals that it needs for a specific and articulated purpose, should use it only for the purposes for which it was collected, should not keep it any longer than necessary, and should not share it with other government agencies except for very good reasons. The Patriot Act violates that principle by adopting the approach that myriad government agencies should collect, share and maintain forever as much information on as many people as possible. Requiring the minimal protection that the government articulate why specific information could be useful for counterterrorism or counterintelligence before widely distributing it would help keep the government focused on the information needed to locate the next attackers, instead of warehousing personal information about millions of Americans.