

Testimony of Joseph Onek
Senior Policy Analyst, Open Society Institute
House Committee on Homeland Security,
Subcommittee on Intelligence, Information Sharing,
and Terrorism Risk Assessment

Hearing on “Using Open-Source Information Effectively”

June 21st, 2005

Mr. Chairman, Ranking Member Lofgren and members of the Subcommittee. Thank you for giving me the opportunity to testify this morning on issues related to the government's access to open-source information.

As the Subcommittee well knows, since 9/11 Congress has enacted many provisions-- in the Patriot Act, the Homeland Security Act and the Intelligence Reform legislation -- authorizing or requiring federal agencies to collect and share more information about Americans. At the same time, new technologies are making it easier for government agencies to gather, store and analyze information. These developments have raised a variety of concerns.

Many Americans, I believe, have a visceral unease about the fact that the government has the capacity to gather so much information about them. That unease explains the powerful opposition to the Defense Department's Total Information Awareness Program. It also explains the opposition to section 215 of the Patriot Act -- the so-called library records provision. I myself agree that section 215 should be amended as proposed in the SAFE Act to prevent fishing expeditions by government officials and keep their focus properly on information relating to agents of a foreign power. I also believe that the government must do a better job of explaining its information collecting and sharing practices. Recently, for example, the Department of Homeland proposed to exempt one of its systems of records from the requirements of the Privacy Act. Its notices explaining the request were so opaque that it was difficult to understand what records were involved and why the exemption was appropriate.

Another development that, according to public opinion polls, is raising concerns about privacy is the proposal to authorize administrative subpoenas in national security investigations. The Senate Select Committee on Intelligence has reported out legislation granting the government administrative subpoena power under the Foreign Intelligence Surveillance Act (FISA). Administrative subpoenas are now used in many types of investigations, and the government asks why they shouldn't also be used by the FBI in the fight against terrorism. But, as I testified before the Senate Intelligence Committee, the government ignores some very crucial facts.

First, administrative subpoenas are typically used for discrete purposes and to obtain limited types of records. But here the subpoenas would be seeking records relating to foreign intelligence and terrorism. The range of activities that relate foreign intelligence and terrorism is enormous and, therefore, there is virtually no limit to the type of records the FBI will be able to subpoena. The FBI will seek financial records, employment records, transportation records, medical records and yes, sometimes, library records. The collection of this massive array of records creates special problems. Inevitably, FBI investigations will sweep up sensitive information about innocent, law-abiding people. How do we assure this information is not abused? The FBI will also sweep up information about people who have nothing whatsoever to do with terrorism, but who may have committed other infractions, both minor and major. What will the FBI do with this information? These are not problems that arise with the ordinary use of administrative subpoenas.

There is a second crucial difference between the ordinary use of administrative subpoenas and the new proposal. In the proposed legislation, the FBI's subpoenas must be kept completely

secret whenever the FBI says that national security requires non-disclosure. This means that a record holder who receives a subpoena that is overbroad or impinges on first amendment rights will not be able to complain to the press, Congress or the public.

This is not an insignificant disadvantage. Just last year, a federal prosecutor in Iowa served grand jury subpoenas on Drake University and members of the university community in connection with a peaceful antiwar forum. The university community protested loudly, the press took up the controversy, and the subpoenas were promptly withdrawn. This cannot happen when the subpoenas are secret.

If subpoenas covering a vast array of records are going to be served in secret, there must be additional safeguards. The most obvious safeguard is prior judicial approval, such as is provided, however inadequately, in Section 215 of the Patriot Act. We should not permit, for the first time in our history, the massive use of secret subpoenas that have not been approved by a judge.

I recognize that the proposed legislation provides record holders with the opportunity to challenge any subpoena in federal court. But this opportunity is no substitute for prior judicial approval. Third party record holders will generally have no incentive to undertake the burdens of a federal court challenge, and the secrecy provisions further reduce the likelihood of a challenge. If, for example, a hospital receives a subpoena for a massive number of medical records and the subpoena is made public, the medical staff and patient groups might pressure the hospital to file a challenge. There will be no such pressure with a secret subpoena. Thus, there will be little judicial supervision of the FBI's use of secret subpoenas.

The FBI should be required to obtain a court order when it seeks access to business records. As already noted, I believe the current standards for issuing such orders, as set forth in Section 215 of the Patriot Act, should be tightened along the lines suggested by the SAFE Act. But in any event there must be a requirement for judicial approval. Such a requirement imposes a salutary discipline on the government. It forces the government to think through and describe, in the words of Deputy Attorney General Comey, the "meaningful, logical connection between the record sought and the subject of the investigation." If the government believes that obtaining a court order is too slow in certain circumstances, it should propose special procedures for emergency situations.

In addition to the general unease about increased government collection of information, there are some highly specific concerns. Civil libertarians are worried that the government might misuse the information it gathers to attack and intimidate critics and opponents. The memory of J. Edgar Hoover's efforts to destroy the reputation of Martin Luther King lives on. And, just recently, there have been allegations that the White House leaked information about a CIA agent in order to punish her husband for criticizing certain policies of the Administration.

These privacy and civil liberties concerns deserve serious attention. But this morning I would like to focus on another concern-- the danger that the government will use the information it gathers and shares in ways that unfairly discriminate against Muslim Americans.

Although only a miniscule number of Muslim Americans are involved in any form of terrorism, it is obvious that the government's expanded information gathering and data-mining systems will focus on Muslim Americans. Even if such systems do not single out Muslims Americans by name or religious affiliation, Muslims will appear disproportionately on the government's computer screens because they are the people most likely (naturally and innocently) to visit, telephone and send money to places like Pakistan and Iraq. Inevitably, government officials will learn more about Muslim Americans than about other Americans. Many Americans, for example, employ undocumented workers in their homes and businesses. Many "harbor" out of status immigrants (often close relatives) by giving them a place to stay or finding them an apartment. Many do not fully report their earnings from tips to the IRS. But the Americans who will be caught doing these things, and subjected to prosecution, will disproportionately be Muslim.

Similarly, there are millions of persons in the U.S. who are violating the immigration laws. Their offenses range from illegal entry to failing to notify authorities of an address change. Again, Muslim violators will be caught and subjected to deportation in far greater percentages than other violators.

At first blush, there may seem to be no problem with prosecuting or deporting persons who have violated the law. But our nation's legal and moral values require equal application of the laws. When, for example, there are stretches of highway where virtually everyone exceeds the speed limit, it is not permissible for the police to stop and ticket only (or primarily) those speeders who are black. The new information gathering and data-mining systems will often deliberately focus on persons who are likely to be Muslims, and therefore it is necessary to address the unequal application of the laws that will inevitably follow.

I propose, therefore, that information gathered for anti-terrorist purposes not be used against individuals except in proceedings that directly relate to terrorism or to other violent crimes. Unless this restriction is imposed, criminal and immigration laws will be disproportionately applied against Muslim Americans. This unfairness will breed discontent in the Muslim community and undermine the fight against terrorism. It is important both that our country is seen by the world as fair to Muslim Americans and that it enlist the full cooperation of the American Muslim community in anti-terrorist efforts. These objectives can only be met if Muslims in this country believe the government is treating them fairly.

This proposal does not mean that anyone will be granted immunity for criminal activity or amnesty for immigration violations. The government remains free to bring criminal or immigration cases against Muslim Americans, provided that it does not use information generated by anti-terrorist data-mining systems in cases not involving terrorism or violent crime. This limitation will require some segregation of information and impose some burdens on the government. But these burdens are a small price to pay to ensure fairness to all Americans and strengthen the fight against terrorism.

Interestingly enough, the federal government is currently implementing a somewhat similar immunity program in accordance with the Homeland Security Act of 2002. Section 214 of the Act provides that companies such as nuclear power plants that voluntarily disclose to the

government critical infrastructure information concerning their vulnerabilities to terrorism are guaranteed that the government will not use that information against them in any civil action. This is so even though the disclosed information may indicate that the company is not complying with various laws regulating safety or the environment and is thus subject to severe civil penalties. Congress made the determination in the Homeland Security Act that granting companies this limited use immunity served important national security interests. As I have argued, national security interests are also served by providing limited use immunity to people caught up in our anti-terrorism data-mining efforts.

Whether or not you agree with my analysis, I am sure you do agree that the government's increasing authority and capacity to gather information about Americans requires congressional attention. Recently, the President named his nominees and appointees to the new Privacy and Civil Liberties Oversight Board, and I hope the Board will soon address the questions I have raised this morning. But, in the end, it is up to Congress to assure that the government obtains the intelligence it needs without violating the civil liberties and civil rights of the American people. Thank you.