Center for National Security Studies

Protecting civil liberties and human rights

Director
Kate Martin

KATE MARTIN

Kate Martin has been Director of the Center for National Security Studies, a non-profit human rights and civil liberties organization located in Washington, D.C, since 1992. Previously, she served as litigation director for the Center. From 1993 to 1999, Ms. Martin was also co-director of a project on Security Services in a Constitutional Democracy in 12 former communist countries in Europe.

Ms. Martin has taught Strategic Intelligence and Public Policy at Georgetown University Law School and also served as general counsel to the National Security Archive, a research library located at George Washington University from 1995 to 2001.

She has testified frequently before the United States Congress and has litigated cases involving the entire range of national security and civil liberties issues. Since September 11, 2001, she has filed an amicus brief challenging the illegal detentions of US citizens as "enemy combatants and serves as lead counsel in the lawsuit brought by more than 20 organizations challenging the secret arrests of 1200 people in the wake of September 11.

She participated in the drafting of the Johannesburg Principles on National Security and Freedom of Expression

Among her publications are: "*Intelligence, Terrorism and Civil Liberties,*" Human Rights, Winter 2002; *Civil Liberties and National Security on the Internet*, published in The Information Age Anthology, vol. II: National Security Implications of the Information Age (CCRP 2000): with Paul Hoffman *Safeguarding Liberty: National Security, Freedom of Expression and Access to Information: United States of America*, published in Secrecy and Liberty, ed. Coliver et al. (Martinus Nijhoff Publishers 1999); *Preventive Detention of Immigrants and Non-Citizens in the United States since September 11th*, published in Refuge, ed. Aiken et al. (Centre for Refugee Studies 2002); *Secret Arrests and Preventive Detention*, ed. Brown (New Press forthcoming Fall 2003).

Previously Ms Martin was a partner with the Washington, D.C. law firm of Nussbaum, Owen & Webster. She graduated from the University of Virginia Law School in 1977, where she was a member of the Law Review, and from Pomona College in 1973 with a B.A. in Philosophy.

1120 19th Street, N.W., Suite 800, Washington, D.C. 20036
tel: (202) 721-5650 fax: (202) 530-0128 kamartin@gwu.edu

Statement of Kate Martin
Director,
Center for National Security Studies

Before the Permanent Select Committee on Intelligence
of the House of Representatives

on

Securing Freedom and the Nation:
Collecting Intelligence Under the Law

Wednesday, April 9, 2003

Thank you, Mr. Chairman for the honor and opportunity to testify today on behalf of the Center for National Security Studies. The Center is a civil liberties organization, which for 30 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

We commend the Committee for holding this hearing on these extremely important issues. We urge you to hold additional hearings to examine how we can preserve our freedoms while defending against terrorism.

Today I want to focus my remarks on the question of how we can marshal our information and technology resources most effectively to fight terrorism, while protecting civil liberties. In the limited time available, I will focus on government data-mining and networking linked databases. In doing so, I want to outline the important questions that is facing this Committee and the Congress.

Intelligence—the collection and analysis of information—is frequently said to be key to fighting terrorism. Some uses of intelligence, while important for anti-terrorism efforts are outside the scope of my remarks today. They have limited implications for civil liberties at home, although some have important implications for the promotion of democracy and human rights overseas. One use of intelligence, which I will not address is that which has been assigned to the new Department of Homeland Security: to assess the vulnerabilities of various targets in the United States, from the cyber-infrastructure to water reservoirs. Nor will I discuss the traditional task of foreign intelligence overseas: to assess the capabilities and intentions of foreign actors, including for example, what governments might covertly provide assistance to Bin Laden and Al Qaeda. The appropriate means and necessary resources for these tasks are different than the means and resources necessary for the prevention of terrorist acts inside the United States. That task requires identifying, surveilling, and ultimately apprehending and prosecuting individuals planning terrorist activities in the U.S.[1] It is this use of intelligence—focused on individuals within our own country—that raises the most serious issues of protecting constitutional values.

I believe that the most effective means of identifying such individuals and preventing terrorist attacks in the U.S. is also the means which carries the fewest risks to our civil liberties. Both logic and experience show that it is not true that the greater the sacrifice of individual privacy and liberty, the safer we become. There is no necessary relationship between the two. While some have cast the difficult situation we find ourselves in today as one in which we must decide what liberties we are willing to sacrifice for an increased measure of safety, I do not believe that is an accurate or helpful analysis. Before asking what trade-offs are constitutional, we must ask what gain in security is accomplished by restrictions on civil liberties.

[1] I will not talk about the separate task of locating individuals overseas who may be involved in planning attacks here. However, in thinking about an effective approach inside the United States, an obvious and crucial issue is coordinating these two tasks.

There are two fundamentally different approaches that can be used to identify and locate dangerous individuals in the United States and their sources of financing. The approach, which has generated the most discussion, interest, and apparently resources is different forms of data-mining, the "suspicionless surveillance" of large groups of people, whether through linking computerized databases, programs like Total Information Awareness, pattern analysis, the creation of a "terrorist profile," or surveillance of an entire group.

The alternative approach is also much less threatening to individual privacy and liberty: that is to follow the leads from the voluminous information the government possesses about actual terrorists. Today, the U.S. government knows the identity of hundreds or perhaps thousands of individuals associated with Al Qaeda.[2] (Indeed it knew the identities of many even before September 11, including at least two of the hijackers.) It has seized scores of documents, computer hard drives and other information from terrorists in Afghanistan, the United States and around the world. According to press accounts citing official sources, the government is obtaining important information from interrogating individuals being held in captivity. Effective anti-terrorism intelligence requires following every one of those leads, by tracing the associates and activities of each one of those individuals; identifying, locating and investigating all of their contacts, casual or otherwise, all of their financial transactions, and their travel records. It requires using all available databases and technological resources to follow the leads, including the most intrusive kinds of surveillance, where authorized. This is obviously an enormous job, requiring resources, patience, analysis and thoroughness. It is made more difficult and time consuming because much of the information is likely to be in a language other than English and located overseas.

Such an approach could also investigate all the individuals who traveled to Afghanistan before September 11 when the Taliban and Al Qaeda were running training camps there and following up on their associates and activities. It would require reading and analyzing the volumes of information seized from the first World Trade Center

[2] For example, the Attorney General has described "a database of thousands of known terrorists. The operations of the U.S. military in Afghanistan have allowed us to expand that database considerably... now we have a sizable database of fingerprints of known terrorists." Attorney General Prepared Remarks on the National Security Entry-Exit Registration System, June 6, 2002 http://www.usdoj.gov/ag/speeches/2002/060502agpreparedremarks.htm

bombers, reportedly untouched by the FBI before September 11. Using such an approach, the FBI would have followed up on the Phoenix memo by looking at students in flight schools before September 11, and discovered individuals engaged in the suspicious behavior of not being interested in learning to land a plane.

Such an approach of following leads based on individualized suspicion tied to a person's activities and contacts, likely would have uncovered at least in part the network of September 11 conspirators. The FBI and CIA knew that two individuals, who had attended a meeting of terrorists in Malaysia were in the United States and would have targeted and surveilled them to discover their intentions and associates.

Some of this is apparently now being done. But more and more resources are being poured into the other approach: building the capability for the government to electronically access massive data about the details of everyone's life and the resources to examine all this data looking for "potential terrorists." There is a push to create a comprehensive networked system that would include linked databases containing everything from a biometric identifier for all individuals to medical records. The intent is to assemble as much information on as many individuals as possible from both existing databases and new collection efforts and then to use computer software tools to generate lists of suspicious individuals. The Total Information Awareness program, an example of this approach would use some un-described algorithm to conduct pattern analysis to generate a list of potential terrorists.

It is useful to contrast the two approaches using a concrete hypothetical inquiry. Various government officials have spoken about following the pattern of financial transactions by the September 11 hijackers to identify additional suspects. The data-mining approach would presumably look at money transfers from various countries in the Middle East to individuals in the U.S. Even if limited to transfers through particular banks, or perhaps through Germany, the analysis would undoubtedly generate thousands of hits, most of which, upon further scrutiny, would turn out to involve innocent people making innocent transfers. The other approach based on individualized suspicion would require looking at the particular individuals and accounts used to fund the hijackers and the accounts of those who knew the hijackers. It would mean following every lead and using all available data analysis techniques on the data that would be gathered in this

way. While perhaps harder in certain respects, the likelihood of generating useful information is much greater than in the case of the more general data-mining, pattern analysis approach.

While the data-mining paradigm is unlikely to yield useful information, its costs are enormous. It requires scarce federal budget dollars, even more scarce human resources, including limited but crucial translation capabilities. Spending such limited resources for such limited benefits increases the risk of missing the real terrorists, all the while data-mining all Americans or immigrants or Arabs and Muslims.

The costs to individual privacy will be immeasurable. The importance of this issue to Americans was vividly demonstrated by the spontaneous public outcry and rejection of the concept of Total Information Awareness. Building this kind of technological capability will fundamentally alter the relationship between Americans and their government. And it is very difficult, if not impossible, to enact laws or build oversight mechanisms strong enough to protect against abuses.

As Senator Sam Ervin recognized in 1974:

> Government has an insatiable appetite for power, and it will not stop usurping power unless it is restrained by laws they cannot repeal or nullify. There are mighty few laws they cannot nullify. [...]
>
> Each time we give up a bit of information about ourselves to the government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. [...]
>
> One of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information without any subjective concern for human emotion and fallibility.[3]

We respectfully suggest that this is a subject that requires intense scrutiny and work by this Committee and the Congress as a whole. Close scrutiny of the effectiveness of current anti-terrorism efforts is needed. Oversight of the implementation of the Patriot Act is crucial, along with oversight of the other steps taken by the government outside of

[3] Introductory Remarks of Senator Sam J. Ervin on S. 3418, Legislative History of the Privacy Act of 1974 S. 3418. (Public Law 93-579), Committee on Government Operations United States Senate and the Committee on Government Operations House of Representatives Subcommittee on Government Information and Individual Rights, May 1, 1974.

those authorities. On the subject of data-mining and the creation of linked databases, key information about the government's current efforts and plans needs to be made available immediately for public scrutiny and discussion. Such capabilities should not be built until and unless there has been a public airing and congressional authorization for such systems.

What is already underway?

While resources are being poured into data mining efforts in many government agencies, and some have urged that it is now time to talk about guidelines, important fundamental questions have been overlooked. There has been insufficient discussion of how such programs would actually work.

1. While there is talk of finding "potential terrorists," it is unclear what that means. Nor is there agreement on a definition of terrorism for data-mining purposes. Some definitions are so broad as to cover Father Berrigan taking a sledgehammer to a nuclear missile, in what is clearly an illegal, but symbolic form of protest. On the other hand, the definition of terrorism in the Foreign Intelligence Surveillance Act is tied to actual activities by individuals, which can reasonably be seen as a step towards planning and carrying out criminal acts.[4] But many of the recent anti-terrorism measures by the Department of Justice and FBI seem based on the assumption that all those who share the ethnic background or religion of the terrorists should be considered "potential terrorists." Is religion or ethnicity the criteria that will be used in the algorithm to generate lists of suspicious individuals? Or will the algorithm use names or national origin as a proxy for religion? Will the algorithm use the neighborhood that known terrorists lived in, in the same way that the FBI arrested the individual who applied for a drivers' license at the same office as one of the hijackers?[5] There are also disturbing indications that the FBI and Justice Department are not focusing on identifying those actually engaged in planning terrorist acts, but is seeking to learn and record individuals' political sympathies, thoughts and ideas.[6]

---

[4]. The FISA definition is 50 USC sec 1801 (b (2) (c) and (d).

[5] See "A Deliberate Strategy of Disruption; Massive, Secretive Detention Effort Aimed Mainly at Preventing More Terror," The Washington Post, November 4, 2001.

[6] There are repeated reports of FBI agents asking individuals about their political and religious views.

2. A comprehensive examination is also needed of currently existing and planned databases What kinds of linking technology are being considered or are already being used? Perhaps most importantly, what are the effects of linking them? This Committee needs to examine carefully how that will be done and to what end.

In examining the implications of government access to this information, it is important to begin with the individual databases. Many of them considered alone raise questions about their purpose and appropriate use and the adequacy of any existing safeguards, depending on the sensitivity of the information in the database. Collecting information about an individual's religion or lawful political activities and filing such information electronically raises serious First Amendment concerns as well as privacy concerns. Electronically storing information about one's race or ethnic background or national origin raises equal protection and discrimination concerns. The collection and retention of other information may raise serious privacy concerns either because of the intrusiveness of the methods used to obtain the information, or because the information itself is highly personal, like medical records. Finally, of course, there is information about individuals, like addresses and telephone numbers that is generally publicly available. Of course, we have always recognized that there are circumstances when the collection and retention of all of these kinds of information are appropriate, but only with adequate criteria for collection, use and retention, as well as safeguards against abuse. But most difficult questions regarding government collection of information have always arisen in the context of intelligence and law enforcement in part because of the necessary secrecy surrounding the actual data and in part because while the government's needs are important, the risk to civil liberties is also great.

Following is a partial list of existing databases accessible to intelligence and law enforcement officials, which need to be examined.

Commercial databases. These contain myriad details on hundreds of millions of Americans, including credit histories. Some, such as ChoicePoint put together databases from both public and private sources, like motor vehicle records, land records, and military personnel records all keyed to an individual's Social Security number. On May 30, 2002, the Attorney General revised the guidelines that govern FBI investigations to "authorize the FBI to use commercial data mining services to detect and prevent terrorist

attacks, independent of particular criminal investigations."[7] Apparently the FBI regularly does so.[8]

Medical records databases. The Department of Defense established the Electronic Surveillance System for Early Notification of Community-based Epidemics (ESSENCE) in 1999 to monitor military personnel, and recently expanded the system to include civilians. The system gathers personally identifiable information from emergency rooms, health plans, clinical laboratories, 911 calls, pharmacies, work absenteeism, and veterinary clinics, to search for unusual or suspicious symptoms and events. After the controversy over the Total Information Awareness program – which Essence strongly resembles—the program was moved out of the DOD and into the Homeland Security Department.

National Bioterrorism Syndromic Surveillance Demonstration Program-- The Centers for Disease Control is developing an integrated electronic network of public health alert and surveillance systems to be operated in at least 10 states initially. The systems will gather information from health plans, hospitals, emergency rooms, laboratories, and pharmacies.

Overseas travel records. The Border Security and Visa Entry Reform Act of 2002 required the submission of departure and arrival manifests by aircraft and sea vessels, of all passengers including citizens, lawful permanent residents and others. There does not appear to be any requirement to destroy the information after arriving passengers have been checked and it is likely to be entered into a permanent database of all overseas travel by Americans.[9]

Airline travel database. For the past 10 years, all airlines in the USA were required to pass passenger data from their reservation systems through a government-run Computer Assisted Passenger Screening (CAPS I) system each time a passenger checked in, which designated individuals for additional security screening. The government

[7] Fact Sheet on Attorney General's Guidelines: Detecting and Preventing Terrorist Attacks, May 30, 2002.
[8] Simpson, Glenn, "Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint—U.S. Agencies' Growing Use of Outside Data Suppliers Raises Privacy Concerns," *The Wall Street Journal*, April 13, 2002.
[9] Federal Register, Vol. 68, No. 2, January 3, 2003, Proposed Rule to implement section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. 107-173).

retained the reservation data, whether or not it fit the profile, creating a massive—and little known—set of dossiers on individual travelers. [10]

The government has now established a second screening system, CAPPS II, which will use data-mining to conduct security checks. It will collect and comb passengers' information for patterns and associations that could be labeled as potential terrorist activity. Screened information will included credit reports, travel reservations, family connections and even housing information. CAPPS II will combine and scan multiple databases from both the FBI and INS as well as from commercial sources.[11]

No-fly Lists. The TSA maintains a list of individuals based on information supplied by the FBI and perhaps other agencies, who are subjected to extensive searching before boarding a plane. Individuals have been unable to discover the basis for their inclusion in the list or how to get their name removed.

Database of Americans' contacts with non-citizens. Since November 2001, the Department of Justice has interviewed thousands of men from Middle East and South Asian countries. While the announced purpose was to find information about terrorism, the questions appeared aimed at creating a database, on as many Americans and immigrants as possible. The interviews asked for the names and addresses of all those in the U.S. with whom the non-citizen had had contact, including American family and friends, even when there was no suspicion of any terrorist link[12]

In late 2002 and 2003, as part of the National Security Entrance and Exit Registration System, non-citizens were also required to give the names and contact information of individuals they knew in the U.S., which names are presumably being entered into a database.

FBI Databases. On April 11, 2002, the Attorney General ordered the inclusion of information on "known or suspected terrorists" to the NCIC without any accompanying

---

[10] See Final Report to President Clinton." White House Commission on Aviation Safety and Security. February 17, 1997. Available at: http://www.airportnet.org/depts/regulatory/gorecom.htm.
O'Harrow, Robert, Jr. "Intricate Screening Of Fliers In Works Database Raises Privacy Concerns." *Washington Post*. February 1, 2002. Page A01.

[11] Robert O'Harrow, Air Security Focusing on Flier Screening, Complex Profiling Network Months Behind Schedule, Washington Post, Sept. 4, 2002

[12] Memorandum for All United States Attorneys, All Members of the Anti-Terrorism Task Force from the Deputy Attorney General re: Guidelines for the Interviews Regarding International Terrorism, November 9, 2001.

guidelines to clarify either of those terms.[13] Not even minimal guidance was provided for the designation of "suspected" terrorist, nor were any instructions provided for what to do with the information for the over 650,000 local police officers who have access to the database.

The Attorney General's order also applied to the Department of State's TIPOFF System and the Customs Service's IBIS database.

The Department of Justice has recently lifted the accuracy requirement for the NCIC established by the Privacy Act of 1974. In the Federal Register, the DOJ argued that "in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete."[14] A further justification for the exemption from the Privacy Act requirements was that it is "administratively impossible" to ensure the accuracy of the information because it comes from many sources.

INS databases (now at the Homeland Security Department). The INS databases are famously inaccurate and unreliable, containing contain information about legal permanent residents and citizens as well as visitors to the U.S. [15]

CIA Databases. Very little is known concerning how many Americans, other than agency employees are listed in CIA databases or the criteria for doing so.

3. Current Anti-Terrorism Intelligence Efforts.

In addition to a comprehensive and detailed description of existing databases, a searching examination is needed of how these resources are presently being used for anti-terrorism purposes. There is extensive evidence that since September 11, major anti-terrorism resources have been used to identify, intimidate and deport thousands of immigrants and undocumented workers in the U.S.[16] It appears that no more than a

---

[13] The "known terrorists" designation was reserved for "individuals against whom sufficient evidence exists to justify such a determination." (April 11, 2002 Memorandum on Coordination of Information Relating to Terrorism, From Attorney General Ashcroft).

[14] Federal Register Volume 68, Number 56

[15] See GAO REPORT: Homeland Security: INS can not locate aliens because it lacks reliable address information, November 2002. "When aliens do comply with the requirement, INS lacks adequate processing controls and procedures to ensure that the alien address information it receives is recorded in all automated databases"

[16] These efforts are separate from the new procedures and restrictions on foreign citizens seeking to enter the U.S., which raise fewer constitutional and civil liberties issues.

handful of them had any connection to terrorism. Whether such an approach is sound immigration or economic policy is debatable. As anti-terrorism policy, it is simply counter-productive. It uses scarce anti-terrorism resources to target individuals who have nothing to do with terrorism. And it discourages the very individuals whom the Justice Department is hoping will cooperate, from speaking to FBI agents out of justified fear that they or their relatives or friends will be handcuffed, arrested and jailed on civil immigration charges or minor criminal ones. For 20 years before September 11, the Justice Department and local police recognized the importance of the principle that FBI and police officers should not enforce civil immigration law for this reason. Underlying the new policy is an approach which views entire groups as under suspicion and uses scarce resources to target everyone, instead of concentrating on finding the dangerous individuals. It is poor anti-terrorism policy and undermines fundamental American values.

4. Legal Authorities. Finally, we need to know the Administration's view about what, if any, legal restrictions or safeguards exist on the creation and use of such databases and in particular on linking them together. It seems clear that there are few existing safeguards and that they are especially weak with regard to data on Americans collected or used for law enforcement and intelligence purposes. Perhaps the best example of this is the recent announcement that the FBI has decided to exempt its NCIC database from the fundamental requirement of the Privacy Act that information be accurate.

There have been many calls for congressional oversight and new guidelines regulating these new government capabilities. While the Center has spent 30 years drafting and working on such efforts, we are extremely concerned about the adequacy of any such guidelines and oversight to adequately deal with these new capabilities. At the time the Framers wrote the Fourth Amendment, individual privacy was protected by the law and by the lack of technological capability on the part of the government to know what was said in the privacy of the home. When the government comes to possess unlimited technological capability to gather and process information on everyone, the law is a thin reed to protect our privacy and to resist the enormous pressure that the government will exert to use the information, always in the name of benevolent purposes.

Many of the principles that have informed the laws and guidelines written in the past either have already been abandoned or will be impossible to apply to such capabilities. The basic privacy principle underlying the Computer Matching and Privacy Protection Act of 1988—that information collected for one purpose should not be used for a different purpose without the individual's consent—has already been jettisoned. Nor is access to such information likely to be restricted to a small number of government employees. To the contrary, there are good reasons to try and increase information sharing among the literally hundreds of thousands of law enforcement officers now charged with anti-terrorism responsibilities. Nor will use of the information databases and data mining capabilities be restricted to anti-terrorism efforts; it has already been extended to multiple other uses, beyond even enforcing the criminal law. Adequate accuracy and notice requirements do not seam likely. The FBI has already exempted one of its major databases from any requirement of accuracy, and other databases are not even covered by such a requirement. While some have suggested that individuals should be given notice of their inclusion in a database and an opportunity to challenge the basis therefor. It will not be possible to provide notice or an opportunity to challenge information designated intelligence in a government database. It does not appear that anyone has yet been able to learn how to get their name removed from the so-called "no-fly listy" much less the basis for being listed. Finally, the suggestion has been made that a system of permissions and accountability for uses could provide adequate safeguards. While theoretically possible, current law has already abandoned such requirements. When the Congress provided for the unlimited sharing of sensitive grand jury and wiretap intercepts with an enormous number of government officials in the USA Patriot Act, it refused to require a limited system of permissions and accountability, whereby a court would grant permission for such sharing and the information would be marked so that its use and re-dissemination could be tracked.

Conclusion. Much more information and analysis is needed before data-mining is adopted as a technique to be used against Americans. This Committee can supply the public record needed for the important debate on this issue. In the meantime, I urge the Committee to insist that anti-terrorism efforts in the United States be focused and directed on identifying and apprehending individuals involved in, planning, and

financing terrorist acts against Americans. Building an intelligence capability directed at all Americans is not the means to accomplish that task. The first approach will protect our liberty and our security, the second jeopardizes both.