SAIS Review vol. XXIV no. 1 (Winter–Spring 2004)

Domestic Intelligence and Civil Liberties

Kate Martin

Since September 11, domestic intelligence authorities and technical capabilities have been expanded to fight terrorism. There are calls to substitute an "intelligence" paradigm for a "law enforcement" paradigm in domestic counterterrorism efforts and proposals to establish a new domestic intelligence agency. While better information and analysis is needed to fight terrorism, there is reason to fear that transforming domestic counterterrorism primarily into an intelligence matter is unlikely to appreciably increase security, but will seriously threaten civil liberties. This article outlines an alternative approach that will serve to obtain the intelligence necessary to prevent catastrophic attacks without compromising civil liberties.

The terrible attacks of September 11 have been described as the worst U.S. intelligence failure since Pearl Harbor.[1] In their wake Congress and the Bush administration have expanded domestic intelligence powers and shifted institutional responsibilities for intelligence gathering inside the United States. There are now calls for further changes, including proposals to create a new "domestic intelligence agency."

While there is a general consensus that better information and analysis is needed to fight terrorism, there is reason to fear that many of these changes—in particular, transforming domestic counterterrorism primarily into an intelligence matter and expanding the legal authorities for "domestic intelligence"—are unlikely to appreciably increase security, but instead will threaten civil liberties. An intelligence-centered approach ignores the continuing importance of law enforcement measures to disable potential terrorists, increases the potential for serious abuses of power, and does not address the real problems highlighted by the intelligence failures before September 11. This article will outline an alternative approach that would serve to obtain the intelligence necessary to prevent catastrophic attacks without compromising civil liberties.

Civil Liberties Risks Inherent in Domestic Intelligence

Domestic intelligence activities—the secret collection of information by a government on its own citizens and residents—have always posed a serious threat to individual liberty and to constitutional government. (On the other hand, intelligence gathering to assess the vulnerabilities of domestic infra-

---

Kate Martin, a civil liberties lawyer, has been the director of the Center for National Security Studies in Washington DC since 1992.

structures, one of the tasks of the new Department of Homeland Security, does not pose risks to civil liberties.) There is virtually no domestic intelligence agency, including MI5 in Great Britain, untainted by scandal, political spying and dirty tricks, activities that threaten not only individual rights, but the proper functioning of democratic government. In 1976, the Church Committee documented and catalogued the abuses committed by the FBI, CIA and other intelligence agencies against Americans: violations of and lack of regard for the law; overbroad domestic intelligence activity; excessive use of intrusive techniques; use of covert action to disrupt and discredit domestic groups; political abuse of intelligence information; inadequate controls on dissemination and retention of information about individuals; and deficiencies in control and accountability.[2]

Risks to civil liberties are inherent in the very nature of domestic intelligence. This is because intelligence necessarily operates in secret and, as a result, it is exceedingly difficult to subject intelligence activities to the checks and balances that the Framers of the Constitution understood as essential to prevent abuses of power. Secrecy operates to make congressional oversight less vigorous than usual, even though it is needed in this case to compensate for the lack of the usual forms of public scrutiny over government activity. In addition, the Executive Branch has been very successful in arguing that judicial review of intelligence activities should be extremely deferential and limited, even when constitutional rights are at stake.[3] Perhaps the greatest barrier to strong oversight and accountability is the always-present notion that the interest served by the intelligence agencies—national security—is of paramount concern and always outweighs other interests. While the overriding importance of national security may be true as a general proposition, what is required in any specific situation is an analysis of the competing interests at stake.

The "Wall" Between Law Enforcement and Intelligence

Since September 11, government officials have frequently cited the existence of a "wall" between law enforcement and intelligence as the main reason the CIA and FBI didn't find the September 11 hijackers. They claim that legal obstacles prevented law enforcement and intelligence agencies from sharing vital information about suspected terrorists. The Justice Department made this argument when it sought the repeal of key safeguards against abuse of surveillance authorities as part of the Patriot Act. But this "wall" metaphor is inaccurate and the existence of legal barriers to sharing information is highly exaggerated. Such talk is used to obscure bureaucratic failures of coordination and communication between the FBI and CIA, as well as inside each agency.

The term "wall" is shorthand for reforms adopted following the Church Committee revelations of intelligence abuses to implement fundamental principles limiting government surveillance of Americans. Those reforms proceeded from the recognition that there are important consequences for individuals depending on the government's purpose in initiating surveillance; in particular whether it intends to use the fruits of its

surveillance against the individual to prosecute and jail him. The reforms incorporated the teaching of the Fourth Amendment, which states that the best protection against abuse of surveillance powers is to require the government to have some indication of criminal activity before investigating an individual. This principle also reflects the understanding that the essence of liberty is to be left alone by one's government. Accordingly, the government is limited as to when it can act against its citizens, and therefore may only punish individuals for acts, not thoughts. Moreover, requiring some criminal predicate for government investigations helps protect citizens from being targeted based on dissent, religion, or ethnicity, and helps to ensure that surveillance and intelligence are not used for political purposes. Foreign intelligence gathering, the collection of information that policymakers need concerning the capabilities and intentions of foreign governments and groups, however, is not linked to a criminal predicate. The distinction between the two—investigating possible wrong-doing by individuals and spying on foreign powers—is the fundamental rationale for separating the functions of law enforcement and intelligence agencies.

Indeed, to protect civil liberties and guard against the creation of a Gestapo-like agency, the CIA's original charter, the 1947 National Security Act, prohibited the agency from exercising any "police, subpoena, law-enforcement powers, or internal security functions." But this early attempt to prevent the CIA from spying on Americans was not enforced through any law or oversight mechanism, and in fact the intelligences agencies did engage in widespread political spying. The Defense Department's description of how DOD intelligence and counterintelligence units came to spy on Americans in the 1960s and 1970s is instructive:

> What had occurred was a classic example of what we would today call "mission creep." What had begun as a simple requirement to provide basic intelligence to [military] commanders [in the United States] charged with assisting in the maintenance and restoration of order, had become a monumentally intrusive effort. This resulted in the monitoring of activities of innocent persons involved in the constitutionally protected expression of their views on civil rights or anti-war activities. The information collected on the persons targeted by Defense intelligence personnel was entered into a national data bank and made available to civilian law enforcement authorities. This produced a chilling effect on political expression by those who were legally working for political change in domestic and foreign policies.[4]

The reforms undertaken since the 1970s to prevent such abuses have been misunderstood as creating a so-called "wall" between law enforcement and intelligence. In particular, the rules governing surveillance and retention of data on Americans, along with the efforts to confine the CIA to intelligence-gathering overseas, have been faulted.

In fact, there were separate authorities written to govern law enforcement and foreign intelligence investigations in the United States, but those authorities did not erect a "wall" between the two. In particular, since 1978, wiretapping to investigate crimes has been governed by one federal stat-

ute, while the Foreign Intelligence Surveillance Act (FISA), governs wiretapping agents of a foreign power inside the United States for the purpose of gathering foreign intelligence. Similarly, the Attorney General's Guidelines governing FBI activities, written by Attorney General Levi in 1976 and since amended, provided one set of rules for criminal investigations and another for gathering foreign intelligence relating to espionage or international terrorism inside the United States. These authorities allowed the government much wider latitude in gathering information about Americans and keeping it secret for foreign intelligence purposes. This latitude is greater than that which is allowed for law enforcement purposes. They also provided much less judicial oversight in the gathering of information for foreign intelligence purposes than for criminal investigations.

The post-Church Committee reforms also attempted to enforce the original intent of the CIA's charter by severely limiting the agency's domestic operations. New regulations confined the CIA largely to gathering foreign intelligence abroad regarding the intentions and capabilities of foreign powers for policymakers. The FBI was given both law enforcement and intelligence responsibilities inside the United States, specifically for counter-espionage and international terrorism investigations using FISA and other authorities.

This difference in functions is important from the standpoint of civil liberties. The CIA acts overseas, in secret, and its mission includes violating the laws of the country in which it is operating when necessary. It is charged with collecting information overseas without regard to individual privacy, rights against self-incrimination, or requirements for admissibility of evidence. It is also tasked with carrying out covert actions to influence events by whatever means the President authorizes. The agency gives the highest priority to protection of its sources and methods. In contrast, the FBI's law enforcement efforts involve the collection of information for use as evidence at trial, and its methods and informants are quite likely to be publicly identified. Perhaps most significantly, law enforcement agencies, unlike intelligence agencies, must *always* operate within the law of whatever jurisdiction in which they are operating.

Similarly, there are important differences between government investigations for foreign intelligence purposes and those for law enforcement purposes. The constitutional concerns for Fourth Amendment due process and First Amendment rights of Americans and others located inside U.S. borders do not extend to aliens overseas and thus place fewer restrictions on government activity abroad than at home. (An intelligence agency collecting information overseas for use by policymakers has less opportunity to improperly use that information against individuals than does a police agency working with prosecutors.) While the task of foreign intelligence is to learn as much as possible to provide analyses to policymakers, deep-seated notions of privacy rooted in the Constitution limit the information the government may collect and keep about Americans. [5]

Recognizing the difference between law enforcement and intelligence objectives is especially important in terrorism investigations—both to pro-

tect civil liberties and to ensure effective investigations. Terrorism, unlike organized crime for example, raises problems concerning the intersection between protected First Amendment rights and alleged criminal activity. It is always difficult to investigate planned terrorist activity without targeting those who may share the religious or political beliefs or the ethnic backgrounds of the terrorists, but do not engage in criminal activity. It is easier for an agency to identify those who share the political goals or religious fanaticism of terrorists than to identify and locate those actually plotting harm. It is therefore crucial to structure bureaucratic rules and incentives to discourage investigations based on political and religious activities and to require focusing on finding actual terrorists. An important means for doing this is to require agencies to focus on criminal activity, which encompasses all terrorist plotting and financing, rather than authorizing an intelligence approach that absorbs all available information about thousands of individuals in the hope of finding something useful.

Recognizing the difference between law enforcement and intelligence objectives is especially important in terrorism investigations—both to protect civil liberties and to ensure effective investigations.

Indeed, for years before September 11, there was disagreement between civil libertarians and the Justice Department over whether its "intelligence" investigations of terrorism—of right-wing militias and anti-abortion groups, for example—ranged too far in targeting First Amendment-protected activity. Civil libertarians argued that rules that require investigations to be tied to some reasonable indication of planned terrorist activity not only serve to protect against government abuse of individual liberties, but also help to focus bureaucratic resources on true threats.[6]

While the pre-September 11 framework assumed differences between law enforcement and intelligence, everyone, including the civil liberties community, always recognized the necessity of effective coordination between the intelligence community and law enforcement to fight terrorism.[7] Indeed, for all the talk of a "wall," the pre-September 11 legal regime acknowledged that terrorism—like espionage, and to a lesser extent international narcotics trafficking—is both a law enforcement and intelligence matter. Much work had been done on the legal issues raised by the necessity of close coordination between agencies whose job is to collect critical intelligence by illegal spying abroad if necessary, and by agencies seeking to prosecute individuals within a system of law. The original drafters of the FISA in 1978 specifically provided for a situation in which foreign intelligence gathering uncovers evidence of a crime warranting prosecution. In addition, the long-standing concerns of the intelligence community about exposing sources and methods in criminal prosecutions were addressed by

crafting procedures to reconcile the need for secrecy and the constitutional requirements of public trials and disclosure of relevant evidence.[8] (The only prosecution derailed by these requirements in the Classified Information Procedures Act was one of a CIA officer charged with lying to Congress in the Iran Contra affair.[9])

Better Coordination or Substituting "Intelligence" for "Law Enforcement" ?

Despite the recognition of the need for coordination between law enforcement and intelligence, there have been many difficulties and failures of communication and planning among agencies. Some difficulties are bound to arise when more than one agency has counterterrorism responsibilities. Such expected difficulties were further compounded by bureaucratic rivalries and perhaps incompetencies.

The September 11 attacks dramatically highlighted these problems. But since then, there has been inadequate consideration of how to increase the necessary cooperation United States and collaboration between agencies operating overseas and those operating in the and between foreign intelligence gathering and criminal prosecutions. Instead, both Congress and the Bush Administration have resorted to a rhetorical demand for more "intelligence" and blamed the "wall" for whatever agency failures contributed to the attacks. But the most serious pre-September 11 failures—the CIA's lack of a timely warning to the FBI that two known associates of Al Qaeda were in the United States, the FBI's lack of follow-up to the Phoenix memo, as well as other mistakes—were not caused by any of the safeguards imposed after the 1970s on national security surveillance.[10] Nothing in the pre-September 11 law prevented the CIA from informing the FBI that the suspected terrorists had entered the United States, and nothing would have prevented the FBI from pursuing them.

Instead of focusing on this truly difficult, yet essential task of coordination, many have simply argued that there needs to be a shift from a law enforcement paradigm to an intelligence paradigm with a focus on preventing rather than solving crimes. This formulation, however, is based on faulty assumptions, and substitutes rhetoric for analysis. As the FBI points out, it has always been in the business of preventing terrorist attacks and it had some notable successes before September 11, such as the foiled plot to blow up the Holland Tunnel in New York in 1993. Rather than pose a falsely rigid dichotomy between law enforcement and intelligence, it is necessary to examine how intelligence information is actually used in counterterrorism.

The first use of "intelligence" information is to identify and locate individuals involved in planning terrorist acts. This information must then be used to prevent the attack, in ways that are legally permissible (for the purposes of this discussion) inside the United States. Potential terrorists found in the United States may be placed under intensive surveillance. They may be apprehended if there is probable cause that they are engaged in criminal activity, have been in the past, or are in the United States in violation of the immigration laws. They may be arrested not only for plotting

terrorism, including attempt or conspiracy, but for any crime or visa violation. The government may also attempt to turn them into informants on their associates (with or without arresting them). Ultimately, in order to disable individuals from future terrorist activity, they have to be arrested and prosecuted. Such "prevention" through prosecution has remained one of the government's major anti-terrorism tools even since September 11. Such an approach focuses on individuals involved in planning criminal activities and ultimately relies on law enforcement authorities.[11]

The talk of re-focusing domestic anti-terrorism efforts as an "intelligence" activity, rather than a law enforcement effort using intelligence information, raises the disturbing specter of a different approach to prevention. The methods used by the CIA and foreign intelligence agencies to "disable" terrorists—predator drones shooting missiles at a car crossing the desert; turning individuals over without any legal proceedings to intelligence services infamous for coercive interrogations; or indefinitely detaining individuals incommunicado without any legal process—have never been deemed constitutional or appropriate to use against individuals in the United States. Even absent military hostilities, overseas intelligence methods include disruption of groups and harassment of individuals using agent provocateurs, blackmail or other means, which would be illegal in the United States.

While the morality and legality of employing such methods overseas was debated before September 11 and depends in part on the particular circumstances, (such as the existence of an armed conflict) no reasonable voices advocated their use domestically.[12] But since September 11, the rhetoric of intelligence and prevention has already been invoked to justify measures that were virtually unthinkable before. The President ordered the military detention of two U.S. citizens and one non-citizen arrested in the United States without charge or trial as "enemy combatants." They are being denied access to legal counsel and held incommunicado, on the grounds that it is necessary to do so in order to interrogate them for "intelligence" purposes. One of the key justifications for the President's November 13, 2001 order authorizing secret military detention and trial of suspected "terrorist" aliens is the need to protect intelligence sources and methods. The Justice Department defended its refusal to release the names of hundreds of individuals who were jailed after the attacks but were never charged with terrorism by claiming the names were part of a larger intelligence "mosaic."[13] There is every reason to fear that the Administration's insistence on describing the domestic counterterrorism task as an "intelligence" one is a back door effort to construct a new approach that would allow the use of "intelligence" and military methods against individuals, including citizens, found in the United States and fully protected by the Constitution.

The U.S. Patriot Act and Other Surveillance Measures

The push to expand domestic intelligence authorities began within days of the September 11 attacks, long before any examination of whether insufficient surveillance powers had played any part in the pre-September 11

failures. In the Patriot Act, Congress and the Bush administration first repealed the most important check against abuse of FISA surveillance, and then required wholesale sharing of information on Americans with the CIA with virtually no safeguards.

In seeking the Patriot Act, the administration complained that FISA barred the sharing of information with prosecutors and law enforcement investigators. They asked Congress to repeal its fundamental requirement that FISA's secret and extraordinary procedures be used only when the government's primary purpose is to collect foreign intelligence. Before September 11, it was understood that if the government started out with the primary purpose of making a criminal case against an individual, it must use the criminal surveillance authorities, not FISA.[14] In the Patriot Act, the administration sought to allow the use of FISA's extraordinary powers when the government targets an individual for criminal prosecution or otherwise.

Contrary to the administration's assertion, however, there was no statutory prohibition on sharing information prior to September 11, and FISA information had been used in many criminal cases. To the extent that the administration believed that legal rather than bureaucratic obstacles existed to sharing information, Congress could have adequately addressed the problem simply by providing that FISA information could be shared with law enforcement personnel, a provision proposed by Senator Leahy and included in the final Act (section 505). But Congress went much further and acceded to the administration's request to repeal the requirement that foreign intelligence gathering be the primary purpose when initiating FISA surveillance.

In doing so, Congress simply ignored that FISA authorizes broader surveillance on less probable cause of criminal activity than is authorized by the Fourth Amendment in criminal investigations. Moreover, FISA contains many fewer safeguards against abuse because there is no post surveillance check on either the legality of the initial warrant or on how the surveillance was conducted. Americans targeted by FISA wiretaps or searches of their homes are never told of those searches unless they are subsequently criminally indicted and the government tries to use the fruits of the searches against them. Even then, unlike with a criminal warrant, there is no opportunity for an adversarial judicial review of the adequacy and legality of the search, because the original application for a FISA warrant, unlike a criminal warrant application, is always withheld from the target.[15]

The Patriot Act also increases the domestic intelligence authority of the CIA. It gives the Director of Central Intelligence a role in identifying which Americans to target for FISA wiretaps and secret searches. It requires that vast amounts of information gathered on Americans by criminal investigators be turned over to intelligence agencies, but fails to enact any safeguards on the use or dissemination of this information. In particular, the Patriot Act requires the Attorney General to turn over to the Director of Central Intelligence all "foreign intelligence information" obtained in any criminal investigation, including the most sensitive grand jury information and wiretap intercepts. Over the objections of civil liberties groups

and some Democratic senators, the administration refused to limit this mandatory sharing to information related to international terrorism or to intelligence officials with counterterrorism responsibilities. Instead, the Act requires the Justice Department to give the CIA *all* information relating to any American's contacts or activities involving any foreign government, organization, or individual, and sets no standards or safeguards for use of this information. Such an approach will be counter-productive in identifying useful information for counterterrorism purposes. Its only purpose would seem to be to facilitate the construction of a vast intelligence database on Americans.

Following the Patriot Act, in May 2002, the Attorney General amended the guidelines governing FBI criminal investigations inside the United States to eliminate the requirement that the FBI must be investigating a past or planned crime or criminal conspiracy before it may collect information on the lawful political or religious activities of Americans. (This requirement had not applied to FBI "foreign intelligence" investigations.) Thus, the FBI is now authorized to go into mosques and churches without identifying themselves, and collect information on Americans worshipping there. On the slightest hint of a connection to a foreign church or government, the FBI is required to share that information with the CIA, which is free to include it in any secret databases.

The FBI is now authorized to go into mosques and churches without identifying themselves, and collect information on Americans worshipping there.

Total Information Awareness: Data-Mining as Counterterrorism

In addition to changes in the law since September 11, massive efforts are underway to increase government data-mining capabilities. These efforts are also rooted in an intelligence paradigm rather than a law enforcement one.

In addition to attempting to recruit informants in terrorist groups, there are two fundamentally different strategies that can be used to identify and locate dangerous individuals in the United States and their sources of financing. One approach, based on an "intelligence" paradigm, is data-mining: the "suspicion-less investigation" of large groups of people, through the use of linked computerized databases, pattern analysis software like the Total Information Awareness program, and the creation of a "terrorist profile."

The alternative approach, based on a "law enforcement" paradigm, is both more effective and much less threatening to individual privacy and liberty. It involves following the leads from the voluminous information the government possesses about actual terrorists. Today, the U.S. government knows the identity of thousands of individuals associated with al

Qaeda.[16] (Indeed, it knew the identities of many of them 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 and around the world. According to press accounts citing official sources, the government is obtaining important information from interrogating individuals held in captivity. Effective counterterrorism requires following every one of those leads, by tracing the associates, contacts, and activities of each one of those individuals, as well as 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 located overseas, in a language other than English. Nonetheless, it is likely to be the most effective means of preventing terrorist attacks.

Such an approach could be used to investigate all the individuals who traveled to Afghanistan before September 11, when the Taliban and al Qaeda were running training camps there, and to follow up on their associates and activities. It would require reading and analyzing the volumes of information seized from the first World Trade Center bombers, reportedly untouched by the FBI before September 11.

Following leads based on individualized suspicion tied to a person's activities and contacts would likely have uncovered, at least in part, the network of September 11 conspirators. Using such an approach before September 11, the FBI could have followed up on the infamous Phoenix memo by looking at various students in flight schools, investigating their backgrounds and associations, and probing their connections with legitimate airlines. Before September 11, the FBI and CIA knew two of the hijackers as suspected terrorists who had attended an al Qaeda meeting in Malaysia. The CIA knew that those individuals successfully entered the United States and the agency eventually informed the FBI. Neither agency put out an all-points bulletin to locate the men.

But the current effort to increase technological capabilities to electronically access data about the details of everyone's life, and to examine all this data looking for "potential terrorists," is tied to an intelligence rather than law enforcement approach. There is a push to create a comprehensive networked system that would include linked databases containing a biometric identifier for all individuals and virtually all available information about them. The Defense Department's controversial Total Information Awareness program, renamed Terrorist Information Awareness (TIA) is typical; it views entire communities rather than specific individuals as potentially suspect.[17]

In fact, the government, and in particular the intelligence community, already has access to vast amounts of information that could be included in any such database. The Patriot Act gave the FBI the authority to secretly subpoena any private database on individuals simply on the assertion that such database is needed "to protect against international terrorism or clan-

destine intelligence activities."[18] This was followed in May 2002, by an order from the Attorney General authorizing the FBI to use commercial data mining services to access commercial databases, which contain myriad details on hundreds of millions of Americans, including credit histories.[19] Apparently the FBI does so regularly.[20] In 2002, Congress also required airlines to provide the government with departure and arrival manifests for all passengers, including U.S. citizens, information that can now be used to create a permanent database of all overseas travel by Americans.[21] Moreover, in the course of several programs to interview non-citizens from Middle Eastern countries, the Department of Justice has collected the names and addresses of all those in the United States in contact with the interviewees, including their American family and friends, even when there is no suspicion of any terrorist link.[22] That information can now be used to create a database of Americans' contacts with non-citizens.

Having accessed and linked all these databases, intelligence agencies will then be able to use some anonymous algorithm in a program like TIA to conduct pattern analysis to generate a list of "potential terrorists." It is not known whether the algorithm would use religion or ethnicity, or names or national origin as a proxy for religion, as criteria to generate lists of suspicious individuals meriting further scrutiny. It is not known whether the algorithm would use the neighborhood in which known terrorists lived as a criterion in the same way that the FBI did when it arrested an individual who applied for a drivers' license at the same office as one of the hijackers.[23]

It is useful to contrast how this data-mining approach might have been employed before September 11 with the more targeted "law enforcement" approach. 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 United States. Even if it were 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. As we have seen, 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.[24]

While the data-mining paradigm is unlikely to yield useful information, its costs are enormous.

While the data-mining paradigm is unlikely to yield useful information, its costs are enormous. It requires scarce federal budget dollars and 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, at the same time that it generates massive amounts of information about all Americans or all immigrants, particularly Arabs and Muslims. 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.[25]

At the time the Framers wrote the Fourth Amendment, individual privacy was protected by the law and by the technological limitations on the part of the government to know what was said in the privacy of the home or to retain and catalogue information. When the government comes to possess unlimited capabilities to gather and process information on everyone, the law is a thin reed to protect our privacy and to resist the enormous pressure within the government to misuse the information for political or other purposes.

A New Domestic Counter-Intelligence Agency: The Right Solution?

These questions of law enforcement versus intelligence lie at the heart of another proposal: as part of its mandate to examine the causes of the September 11 attacks, Congress has charged the National Commission on Terrorist Attacks to consider the wisdom of creating a new domestic intelligence agency without law enforcement responsibilities. Many argue that a new agency is needed because of the concern that the FBI cannot be adequately reformed to meet future terrorist threats.

The institutional weaknesses of the FBI are outside the scope of this article. But it is clear that instead of increasing security, a domestic intelligence agency as currently proposed is likely to pose significant dangers to open government, individual privacy, and civil liberties. A new intelligence agency will not address the existing "hand-off" problems of sharing information collected overseas and information collected domestically and will

only exacerbate the difficulty of coordination between intelligence and law enforcement. Information collected by the CIA will still have to be shared in a timely manner with the new domestic agency and those responsible for prosecuting terrorists in the United States. In addition, the FBI and the Justice Department will now have to deal with a new agency collecting information to be used in such prosecutions. Such coordination is crucial because, even though the Bush administration claims dangerous new powers to indefinitely detain individuals outside the criminal justice system, most of the successes claimed by the Justice Department in its war against terrorism have consisted of criminal prosecutions of alleged terrorists.

If a new agency is needed, a better model would begin with the recognition that law enforcement authorities ultimately must be used against terrorists found in the United States. Thus, any new agency should be constructed primarily as a law enforcement rather than intelligence agency, devoted solely to—and ultimately responsible for—counterterrorism. The agency should be authorized to use existing domestic intelligence authorities, grounded in the law, like FISA, and to obtain all other relevant intelligence information from other agencies, including information collected overseas. An agency constructed on this model could bridge the overseas/domestic divide by operating both abroad and at home, and would eliminate the "hand-off" problem between intelligence and law enforcement. Such an agency could appropriately be housed in the Department of Justice, but not in an intelligence agency or under the Director of Central Intelligence.

If a new agency is established, it should assume all of the FBI's current counterterrorism responsibilities and perhaps certain responsibilities now resident in other domestic agencies as well. The transfer of responsibilities from the CIA and other overseas intelligence agencies would be more complicated, but should be based on the premise that efforts to apprehend individual terrorists (outside the field of active military operations) should presumptively be carried out within the framework of the criminal law and thus be transferred to the new agency. The new agency, because it has extensive law enforcement responsibilities, should not be permitted to act illegally. Overseas covert actions, on the other hand, which are by definition illegal where carried out, would still need to be solely the province of the CIA and other intelligence agencies.

The creation of a new agency would of course involve many difficulties, not the least of which is the likelihood that, for political reasons, the FBI would never be forced to surrender its counterterrorism responsibilities. In the end, such a proposal may not be better than leaving counterterrorism with the FBI. The crucial point is to insist that anti-terrorism efforts in the United States be focused on identifying and apprehending individuals planning and financing terrorist acts against Americans. The alternative approach, building an intelligence capability directed at all Americans and divorced from law enforcement, is a less effective way to fight terrorism, and a grave danger to civil liberties.

Notes

[1] Following an investigation by the intelligence committees of the Congress, " Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001," Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence (December 2002) "Joint Inquiry Report", <www.gpoaccess.gov/serialset/creports/911.html>, Congress established the National Commission on Terrorist Attacks upon the United States to investigate the circumstances surrounding the attacks, and make recommendations. Its report is currently due in May 2004. See <www.9-11commission.gov>.

[2] See The Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate (Church Committee), Book II: Intelligence Activities and the Rights of Americans, <www.aarclibrary.org/publib/church/reports/book2/contents.htm>.

[3] See for example: *Snepp v. United States*, 444 U.S. 507 (1980); *CIA v. Sims*, 471 U.S. 159 (1985); compare *New York Times Co. v. United States*, 403 U.S. 713 (1971) and *Webster v. Doe*, 486 U.S. 592 (1988).

[4] U.S. Department of Defense web site, Office of the Assistant to the Secretary of Defense (Intelligence Oversight) <www.dtic.mil/atsdio/mission.html>.

[5] But the effort to blur the distinction between law enforcement and intelligence responsibilities began before September 11. In 1996, Congress amended the 1947 National Security Act to assign the CIA law enforcement responsibilities for the first time, authorizing the CIA to undertake the illegal collection of information overseas for the sole purpose of making a criminal case against a foreigner in a U.S. court.

[6] When Congress first criminalized material support of terrorism, it prohibited the initiation of investigations of such crimes based solely on First Amendment-protected activity. This protection was repealed in the 1996 Anti-Terrorism and Effective Death Penalty Act, leaving the FBI free since then to open investigations based purely on protected speech and religious activities.

[7] See, for example, Kate Martin's 24 September 2001 testimony before the Senate Select Committee on Intelligence on the Legislative Proposals in the Wake of September 11, 2001 Attacks, including the Intelligence to Prevent Terrorism Act of 2001, available at <www.cnss.org/kmtestimony0924.pdf>.

[8] See for example, the 1980 Classified Information Procedures Act and the Joint Task Force on Intelligence and Law Enforcement Report to the Attorney General and Director of Central Intelligence (Richards/Rindskopf Report) May, 1995.

[9] See *United States v. Fernandez,* 913 F.2d 148 (4th Cir. 1990).

[10] See the Joint Inquiry Report.

[11] Counterterrorism investigations, unlike foreign intelligence efforts focused on the legal activities of foreign governments in the United States, are always concerned with crimes, because all planning and involvement in terrorist activities is criminal.

[12] While international human rights law provides many of the protections recognized in the Bill of Rights and is not limited by national borders, its applicability to intelligence activities in times of emergency or war is less developed and outside the scope of this discussion.

[13] See *Center for National Security Studies v. Department of Justice,* 331 7.3d 918 (D.C. Cir), cert. pending (2003).

[14] But see *In re: Sealed Case No. 02-001*, Foreign Intelligence Surveillance Court of Review, 18 November 2002, <http://www.cnss.org/FISCR_opinion.pdf>.

[15] The Patriot Act and subsequent legislation also expanded the scope of personal information, which the government could seize in secret. See for example, section 215 authorizing secret seizures of library records and commercial databases.

[16] 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, 6 June 2002. <www.usdoj.gov/ag/speeches/2002/060502agpreparedremarks.htm>.

[17] While Congress voted to cut off funds for the original TIA program, the data-mining software and research tools were simply transferred to different, undisclosed agencies. "Washington in Brief," *The Washington Post*, 26 September 2003.

[18] Section 215 added this authority to the FISA; it is best known for authorizing the secret seizure of library records.

[19] See Fact Sheet on Attorney General's Guidelines: Detecting and Preventing Terrorist Attacks, 30 May 2002.

[20] Glenn Simpson, "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*, 13 April 2002.

[21] Federal Register, Vol. 68, No. 2, 3 January 2003, Proposed Rule to implement section 402 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Pub. L. 107-173).

[22] 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, 9 November 2001. 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 United States a U.S. Department of Justice Special Registration Worksheet.

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

[24] Of course, at some point, the two approaches—one focused on collecting information relevant to criminal activity and one seeking to collect all information and looking for suspicious patterns—overlap.

[25] 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, 1 May 1974.