COMMENTARY

Guiding Lights: Intelligence Oversight and Control for the Challenge of Terrorism

JERRY BERMAN & LARA FLINT

Winning the war on terrorism requires clear guidelines for data collection, use, and dissemination. The failure of our law enforcement and intelligence agencies to predict and prevent the attacks of September 11, 2001, was powerful evidence of the need for reform of U.S. counterterrorism efforts. Unfortunately, in the government's reaction to September 11 central elements of developing policy have been both dangerous to civil liberties and unlikely to improve national security. In particular, the tendency by legislators and executive branch officials to loosen limits on domestic spying and to weaken oversight mechanisms fundamentally undermines the efficacy of Constitutional checks and balances. The hijackers did not evade detection because of rules intended to guide the efforts of intelligence and law enforcement agencies and to prevent the chilling of activities protected by the First Amendment, although some of these rules have been misunderstood and misapplied in perverse ways. As we seek to improve intelligence collection, sharing, and analysis, it is necessary to set reasonable guidelines for the FBI, the CIA, and the new Department of Homeland Security and to enforce them though judicial and Congressional oversight. Such guidelines are as important to the prevention of terrorism as they are to the protection of civil liberties.

One response to September 11 has been the loosening of rules on information collection through electronic and other means. But casting a wider net and collecting massive volumes of information without direction is not justified by what we know about government activity before September 11. The joint investigation into September 11 by the Congressional intelligence committees identified no pre-9/11/01 legal barriers that needed to be lifted for the government to collect the information necessary to prevent terrorism. Nor did an independent task force commissioned by the Markle Foundation identify such a need.[1] Instead, a primary lesson drawn by Congressional and other inquiries into the September 11 intelligence failure is that the government did not make good use of the information it had already collected and failed to utilize information-sharing authorities at its disposal. Granting the government broader authority to collect vastly greater volumes of information without particularized suspicion could exacerbate this problem. Collecting more information will not catch terrorists if the information is irrelevant because it has been acquired without deliberate targeting.

The war on terrorism will be aided, not hampered, by respect for core Constitutional values: the First Amendment rights to assembly, speech, and the exercise of religion; due process, especially the right to confront the charges and accusers against oneself in a court open to public scrutiny; and privacy. By "privacy," we mean fair information principles that not only protect personal dignity, but also ensure the accuracy of information as the government collects and draws inferences from the ocean of data produced by the digital revolution.

The Relationship Between Law Enforcement and Intelligence

Our nation has traditionally drawn distinctions between law enforcement and foreign intelligence, and between agencies operating domestically and those focused overseas. Sometimes these distinctions have been seen as creating a "wall" that has prevented the useful sharing of information and other forms of collaboration among various agencies. One theme of the Patriot Act—officially entitled the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act—was to break down the "wall" between law enforcement and intelligence.

Jerry Berman is President of the Center for Democracy and Technology and Lara Flint is a staff counsel there. CDT is a non-profit civil liberties organization focusing on policy challenges presented by digital communications and information technologies.

In fact, there was never just one wall. As the Congressional inquiry into September 11 found, there were really many walls, built between and within agencies over the past sixty years as a result of various legal, policy, institutional, and individual factors. Some walls were meant to protect individual rights. Others were meant to protect national security interests. Some walls meant to protect legitimate interests were bureaucratically misconstrued to the point that they served neither civil liberties nor national security. The Patriot Act, passed with record speed just forty-five days after the attacks of September 11, 2001, gave little attention to these distinctions. It broke down the walls indiscriminately, scarcely considering what purpose they served and never asking what should replace them to guide both law enforcement and intelligence agencies in the new collection and sharing of information. It gave intelligence agencies access to the power of domestic law enforcement tools—such as grand jury subpoenas—without asking how abuses of information would be prevented in the absence of the checks and balances that are available only in the criminal justice arena.

The Patriot Act also gave law enforcement officials access to intelligence tools, but in a way that freed law enforcement agencies from the procedural protections of the criminal justice system. The prime example of this was a provision in the Patriot Act that allowed the government to invoke the special wiretap provisions of the Foreign Intelligence Surveillance Act (FISA) even if the primary purpose of the surveillance was not the collection of foreign intelligence. A special court of appeals ruled last fall that this change allowed prosecutors and criminal investigators to use FISA for the purpose of conducting criminal investigations. But Congress and the court of review left behind key elements of the adversarial process normally associated with criminal investigations. When information collected under FISA is introduced in criminal trials, the defendant never obtains the information necessary to challenge the basis for the surveillance and never obtains the full transcript of the intercepts to use to defend himself. If intelligence procedures are to be used in criminal prosecutions, they should be subject to judicial controls. The Classified Information Procedures Act (CIPA) was adopted in 1980 precisely to protect national security while also protecting individual rights in criminal cases. It offers workable procedures that should apply when FISA evidence ends up in court. But in the rush to break down the wall, Congress did not apply CIPA to the use of FISA evidence in criminal cases.

A similar lack of groundrules applies to the concept of domestic intelligence. The FBI has been our domestic intelligence agency, investigating domestic groups under criminal investigation rules and foreign groups under either law enforcement rules or foreign intelligence rules. Many commentators are calling for a new concept of domestic intelligence, but so far these calls have not defined who would be targeted, what information would be collected, and how it would be used any differently from the past.

Datamining

Contrary to popular impression, the Patriot Act did not give the government *carte blanche* to conduct wiretaps or read email. Although it created some new and potentially broad exceptions to judicial review, and expanded the scope of certain electronic monitoring provisions that reduce judges to mere rubber stamps, the Patriot Act did not upset the constitutionally mandated requirement that government officials must normally obtain a judicial order to intercept the content of voice or data communications.

"Datamining," however, is a technique to which traditional Fourth Amendment concepts do not apply. Datamining involves the scanning of billions of bits of data in search of hints of terrorist activities. It has the potential to encompass all the records that exist about us in the hands of third parties—medical, financial, credit card, travel, education, employment, housing, shopping, Internet browsing, even library borrowing records. Unlike the wiretap authorities, there are literally no legal constraints on government datamining. Because the data being collected typically are held by businesses that collect it in the course of ordinary transactions, the data are not protected by the Fourth Amendment. Access to this information turns the presumption of innocence upside down and overturns the Fourth Amendment prohibition against blanket searches. Rather than seeking information on a specific individual who is suspected of wrongdoing, datamining scans information about everyone's legal activity in an effort to identify suspicious behavior.

The Patriot Act gave a huge boost to this datamining technique by vastly expanding the ability of the FBI to compel disclosure of entire databases of records. The FBI need only claim that databases are sought for an authorized intelligence investigation. In other words, a court order is still required to obtain these business records, but the standard for obtaining that order is incredibly low. In addition, the statute does not constrain government officials with respect to the scope of records they can demand. Rather than being required to request the records of a specific person, the government now can insist that a business turn over its entire database.

The mining of vast and diverse commercial and government databases containing personal information about innocent Americans, with no basis for suspicion, is being explored by numerous agencies. The Attorney General has encouraged the FBI to engage in datamining. The Homeland Security Act authorizes the new Department of Homeland Security to utilize datamining. The Transportation Security Administration is developing a new passenger profiling system that relies on datamining technology. And the Department of Defense has launched a "Total Information Awareness" (TIA) datamining program (although Congress has recently taken steps to curtail the deployment of any TIA technology).

Yet none of these agencies has guidelines to control the use of this powerful tool. They have no standards for accuracy and reliability, no rules on how inferences should be drawn from such data, no limits on the actions that may be taken based on such commercial data, no guidance on warehousing or sharing of such information, and no time limits on retention. Datamining technology has the potential to watch all of us, all of the time. What is needed is a comprehensive set of stan-

dards to govern all agencies.

Monitoring Political Activity

First Amendment issues are among the most difficult confronting anti-terrorism agencies. Terrorism is, after all, ideologically motivated violence, so religious or political ideology is not entirely irrelevant to terrorism investigations. Yet merely following a certain religion or holding a particular political viewpoint is obviously an inadequate basis for casting suspicion on someone. Too often in the past, security agencies, especially the FBI, used ideology as a guide and found their investigations to be fruitless.

In March 2002, Attorney General Ashcroft authorized FBI agents to visit religious institutions and monitor political events where there has been no indication that illegal activities are being planned. The Attorney General argued that the FBI should be able to attend meetings on the same basis as a member of the public. But a member of the public can go to a meeting on a whim or out of animosity. Was the Attorney General suggesting that FBI agents could target religious or political groups on the same basis? If not, then how are FBI agents to decide how to prioritize their efforts? Was the Attorney General really suggesting that there is no difference in the value of intelligence to be gathered by monitoring a mosque suspected of serving as a center for planning terrorist activity and monitoring one where there is no indication of wrongdoing? The Attorney General's guidelines fail to answer these questions. They leave agents in the field wondering about how to implement their expanded powers and how to handle the information they obtain. The Attorney General's guidelines provide poor guidance on what can be recorded at those meetings and no time limits on the retention of data acquired. The new guidelines decrease the internal supervision and coordination at various stages of investigation, in particular by expanding the scope and duration of "preliminary" inquiries. These are inquiries that do *not* involve a reasonable indication of criminal or terrorist conduct, yet under the new guidelines the FBI can conduct a preliminary investigation for up to a year—without producing results and without internal review or independent scrutiny.

Thus, the FBI, which is already overwhelmed by the oceans of information it collects, will be receiving even more information. And the information gathered under its new authorities need not be based on any suspicion of criminal conduct—so that it is likely to be irrelevant. Such "guidelines" do not make the FBI more effective in preventing terrorism.

State and Local Authorities

Guidelines are also being loosened (or in some cases never existed) for the state and local authorities that have a crucial but still poorly defined role in the fight against terrorism. Better cooperation among federal, state, and local authorities is highly desirable. But state and local law enforcement officials will be effective partners in the fight against terrorism only if they are trained to do it well, and if they are given rules to follow to ensure that their efforts are focused and do not infringe on civil liberties. State and local officials need clear standards governing the kind of information they are expected to collect, the standards under which they can collect it, how they can use it, and to whom they can disseminate it. They need guidelines explaining when it is permissible to monitor political activities and when it is not.

In the past, including the recent past, a number of police departments engaged in broad monitoring of political groups. The practice intimidated political activists but rarely produced information useful in preventing violence. Some of these police departments were brought under court decrees meant to protect First Amendment rights. Generally, such guidelines limited the collection of information about political groups and political activities of individuals unless there was some indication that criminal conduct was being planned. It is simply misleading to claim, as has the Justice Department, that these decrees prevented agencies from gathering information about organizations and individuals that might have been engaged in terrorist activities or other criminal wrongdoing. If criminal conduct of any kind was suspected, the decrees permitted full monitoring of political or religious groups. Nevertheless, since September 11, some officials have renewed complaints that the guidelines were too rigid, adding the argument that guidelines crafted in the 1970s or 1980s are unsuited to the international terrorism challenges of today.

The Justice Department, rather than seeking to assist its state and local partners in developing guidelines that are responsive to the newly appreciated threat, is instead supporting efforts to eliminate the rules completely. Under the Justice Department's latest legislative proposal, consent decrees and court orders governing the conduct of state or local police surveillance activities would be terminated, to be replaced with nothing. Future court orders could address only "ongoing" violations of the rights of "particular" plaintiffs. This would mean that courts could not act to stop unproductive but chilling political surveillance so long as the government said that it stopped the unconstitutional conduct yesterday with respect to the named plaintiffs, even if it admitted to doing the same thing with respect to others and refused to promise not to resume it tomorrow with respect to the named plaintiffs.

Where would this leave local authorities? Would Congress, in nullifying these orders, be advising state and local police to revert to the broad political surveillance of the past? To be sure, judicial micro-management of local investigations is undesirable. But if judges are barred from setting down guidelines, to where do local police turn? It would be good were the Justice Department to have rules to replace the supposedly outdated decrees. But the Justice Department's own guidelines, as we noted above, are insufficient and the Department does not want to replace these consent decrees with other guidance; it simply seeks to abolish them, setting state and local authorities adrift. In large and diverse cities, with vibrant and sometimes noisome grassroots political groups, where do police turn if they do not focus on criminal conduct? Do they monitor critics of police brutality, as they have in the past? Do they surveil demonstrators? What good

is monitoring all mosques if, as FBI investigators told the Congressional intelligence committees' staff, al-Qaeda members avoid other radicals and stay clear of mosques as part of their tradecraft? Unguided discretion for law enforcement authorities would likely result in the collection of irrelevant information, serving neither the war on terrorism nor the preservation of civil liberties.

Conclusion

Too often since September 11, the American public has been presented with a false trade-off: surrender personal freedoms and curtail democratic accountability in exchange for additional security. Setting law enforcement and intelligence officers adrift, without standards and oversight mechanisms, will certainly result in losses of privacy, due process, and other civil liberties, but it will probably not result in greater security. Law enforcement and intelligence officials operating in the field need guidance on how to prevent terrorism *and* on how not to infringe on civil rights. Clear rules that take into account the legitimate needs of law enforcement and intelligence communities as well as civil liberties concerns will result in more effective investigations and a higher degree of protection for civil rights.

From the Patriot Act to the revised Attorney General's "guidelines" to the latest Justice Department legislative proposals, the executive branch is seeking to free itself from rules and oversight. But to protect both our national security and our civil liberties, we need more, not fewer, guidelines and greater, not lesser, oversight and accountability for law enforcement and intelligence agencies.

NOTE

[1] Markle Foundation Task Force, *Protecting America's Freedom in the Information Age* (October 2002) <http://www.markletaskforce.org/> (3/20/2003).