Domestic Intelligence System Grows without Controls

March 18, 2009

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

Without a definitive decision to do so, and without adequate guidelines or limits, government agencies at the federal, state and local level are creating a vast domestic intelligence apparatus. The concerns long posed by domestic spying are magnified by the digital revolution, which makes it easier than ever to collect, store, exchange and retrieve personally identifiable information, making it available far removed from the context in which it was collected and creating a high risk that information will be misinterpreted and used to the detriment of innocent persons.

---

1) Vast Domestic Intelligence System Grows without Adequate Civil Liberties Protections

Without a definitive decision to do so, and without adequate guidelines or limits, government agencies at the federal, state and local level are creating a vast domestic intelligence apparatus. The concerns long posed by domestic spying are magnified by the digital revolution, which makes it easier than ever to collect, store, exchange and retrieve personally identifiable information, making it available far removed from the context in which it was collected and creating a high risk that information will be misinterpreted and used to the detriment of innocent persons.

Homeland security intelligence, as it is sometimes called, is not statutorily defined, but the loosely structured system that is being created does not distinguish between information regarding foreign terrorist organizations and information regarding domestic terrorist groups. It includes information collected under criminal investigative powers, "foreign intelligence" or counterintelligence collected under the national security powers, and information collected under regulatory or administrative authorities or from open sources. Indeed, there is a new effort to collect information with no real predicate at all, based solely on a broadly defined notion of "suspicious activity." The system includes information collected by federal agencies and information collected by state and local governments.

To some degree, counter-terrorism intelligence gathering and dissemination must be broad in scope, since one of the reasons why the planning of the 9/11 attacks went undetected is that agencies observed various artificial distinctions that prevented information sharing and collaboration. However, with such an all-encompassing definition, the cycle of collecting, sharing and using homeland security intelligence clearly poses risks to constitutional values of privacy, free expression, free association and democratic participation.

There are also questions of effectiveness: the security "bang per byte" of information gathered may be diminishing. While "stove piping" was yesterday's problem, tomorrow's problem may be "pipe clogging," as huge amounts of information are being gathered without apparent focus.

CDT Testimony on Homeland Security Intelligence: [1] (March 18, 2009)

2) Nationwide Information Sharing Networks Magnify Risks to Privacy

Multiple agencies at the federal level collect and analyze information that fits under the homeland security intelligence umbrella. Within the Department of Homeland Security alone, there is a departmental Office of Intelligence and Analysis and there are intelligence units within several of the Department's components as well, including the U.S. Citizenship and Immigration Service, the Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration. Outside the DHS, federal agencies collecting or analyzing homeland security intelligence include the FBI, the CIA, the Drug Enforcement Administration, the Department of Energy, the Treasury Department, and entities within the Department of Defense, including the National Security Agency and the National Reconnaissance Office, whose satellites are available for domestic collection.

Outside of the federal government, state, local, and tribal police forces of varying sizes also engage in the collection of homeland security intelligence. The level of sophistication of these efforts varies widely. For example, the New York City Police Department has a sophisticated intelligence operation, which operates with little public oversight. Likewise, the Los Angeles Police Department has a very sophisticated intelligence gathering and integration program.

Until recently, collection, analysis and dissemination efforts have been disjointed and uncoordinated, which may have offered some comfort to civil libertarians. Now, a variety of efforts are underway to integrate the information that is being collected and to share it more widely. They include:

- Information Sharing Environment: The ISE, created by Congress and housed in the Office of the Director of National Intelligence, is intended to facilitate sharing of terrorism, law enforcement and homeland security information across federal agencies and among state, local and tribal police forces. The ISE is scheduled to go operational this summer.
- National Counterterrorism Center: The NCTC employs more than 500 people, drawn from 16 federal departments and agencies, to integrate and analyze counterterrorism intelligence, much of which fits under the homeland security intelligence umbrella. The NCTC has access to more than 30 intelligence, military and law enforcement networks; it also takes in copies of data from other agencies, creating its own depository of data that is analyzed and shared. Among other functions, the NCTC maintains the repository of information about terrorists from which is derived the watchlist used to screen airline passengers.
- E-Guardian: E-Guardian is an FBI system for sharing unclassified information relating to terrorism with 18,000 entities, including state and local law enforcement entities. According to a DOJ Inspector General's report, a related system, Guardian, which contains terrorism tips and reports by federal agencies, suffers from numerous data integrity failures.
- Fusion Centers: State and local governments have created at least 58 fusion centers. Each fusion center is different, but there continue to be questions about their mission and effectiveness and they face significant challenges.
- Joint Terrorism Task Forces: JTTFs are comprised of federal, state and local law enforcement officers and specialists. The JTTF concept pre-dated 9/11 by several decades but was expanded after 9/11 and there are now 100 JTTFs, including one in each of the FBI's 56 field offices nationwide. Sixteen other federal law enforcement and intelligence agencies are involved in one or more JTTFs.

The goal, of course, is laudable: to collect and connect the dots that might reveal a terrorist scheme.

However, there is no overall theme to this collection and sharing effort, no guiding principles.

DOJ Inspector General's report [2]

---

3) Abuses Have Already Occurred

Despite the secrecy surrounding domestic intelligence activities, instances have been uncovered where homeland intelligence efforts classified legitimate political activity as "terrorism" and monitored peaceful activists. Example include.

- Undercover Maryland State Police officers conducted surveillance on war protesters and death penalty opponents from March 2005 until May 2006. The state police classified 53 nonviolent activists as terrorists and entered their names in state and federal terrorism databases.
- At least as of 2006, the Intelligence Branch of the Federal Protective Service in DHS was compiling a "Protective Intelligence Bulletin," mainly by using a "media reporting service" available on the Internet. The 17-page, March 3, 2006 bulletin, lists dozens of events such as a "Three Years Is Too Many Demonstration" by the Central Vermont Peace and Justice Center to be held at 1400 hours on the sidewalk in front of Main Street Park in Rutland.

Also, there is a trend toward the collection of huge quantities of information with little or no predicate, through "Suspicious Activity Reports." State, local, tribal and federal entities are collaborating to develop a nationwide SARs system that is just getting off the ground. So far, the standards for the program suggest that much innocent activity will be tracked. For example, photographing bridges is described as a suspicious activity, even though such sites are regularly photographed by tourists, journalists and photography buffs.

DHS ICE "Civil Activists and Extremists Action Calendar" bulletin [3] (March 3, 2006)

---

4) Closer Oversight, More Detailed and Stringent Guidelines Needed

Remarkably, there does not seem to be a set of intelligence guidelines for the Department of Homeland Security or for any of its intelligence-collecting components. Moreover, the guidelines that have been issued so far fail to provide adequate guidance. Guidelines for the FBI, issued by the Attorney General last year, permit intelligence collection without any suspicion of wrong-doing. Guidelines issued for the ISE provide generic, unhelpful guidance, stating that "all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders."

In a recent report, the Markle Foundation Task Force on National Security in the Information Age called on the President and Congress to develop government-wide privacy policies for information sharing to match the increased technological capabilities to collect, store and analyze information. The Task Force, which senior CDT staff participate in, stressed that these policies must be detailed and must address the hard questions not answered by current law -- who gets what information for what purpose, under what standard of justification.

In our March 18, 2009 testimony, CDT recommended a number of additional steps that should be taken to focus domestic intelligence operations:

- Require DHS entities to follow the principles of fair information practice (FIPs), including the minimization principle. The well-known FIPs are not perfect, but they provide probably the best framework available for designing a focused and limited information system.
- Adhere to the criminal predicate where appropriate. Probably the single most effective civil liberties protection that could be imposed on the collection and sharing of homeland security intelligence that includes personally identifiable information would be to require criminal predication. This means that information, unless it pertains to a terrorist, spy or another agent of a foreign power and was collected under the Foreign Service Intelligence Act, is collected or shared only because it has some degree of relevance to a potential violation of the law.
- Conduct comprehensive oversight of homeland security intelligence collection. Congress, in exercising its oversight role, should sample intelligence products developed by DHS components to more fully ascertain what is being collected, how it is used, and whether it is useful in preventing terrorism. Oversight Committees should consider whether more targeted collection efforts would be more effective. Also, they should review the training materials that DHS entities use.
- Conduct an independent assessment of the value of SARs reporting. SARs reporting may or may not be the best way to collect the "dots" that need to be connected to head off terrorist attacks; whether it is or is not should be tested. This may involve commissioning a GAO study or conducting an independent staff level assessment.

CDT's analysis of the Attorney General Guidelines: [4] (Oct. 29, 2008)

Our analysis of the ISE guidelines: http://www.cdt.org/security/20070205iseanalysis.pdf [5] (Feb. 2, 2007)

Markle Task Force report, Nation at Risk [6] (March 2009)

Source URL: https://cdt.org/policy/domestic-intelligence-system-grows-without-controls

Links:
[1] http://www.cdt.org/testimony/20090318nojeim.pdf /
[2] http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf /
[3] http://www.defendingdissent.org/ICECalendar.pdf/
[4] http://cdt.org/publications/policyposts/2008/16/
[5] http://www.cdt.org/security/20070205iseanalysis.pdf/
[6] http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf/