

The Washington Post

Top Secret America: Local agencies help collect data on Americans

By Dana Priest and William M. Arkin - The Washington Post

Posted: 12/20/2010 MST

Nine years after the terrorist attacks of 2001, the United States is assembling a vast domestic intelligence apparatus to collect information about Americans, using the FBI, local police, state homeland security offices and military criminal investigators. The system, by far the largest and most technologically sophisticated in the nation's history, collects, stores and analyzes information about thousands of U.S. citizens and residents, many of whom have not been accused of any wrongdoing. The government's goal is to have every state and local law enforcement agency in the country feed information to Washington to buttress the work of the FBI, which is in charge of terrorism investigations in the United States.

Other Top-Secret America democracies — Britain and Israel, to name two — are well acquainted with such domestic security measures. But for the United States, the sum of these new activities represents a new level of governmental scrutiny. This localized intelligence apparatus is part of a larger Top Secret America created since the attacks. In July, The Washington Post described an alternative geography of the United States, one that has grown so large, unwieldy and secretive that no one knows how much money it costs, how many people it employs or how many programs exist within it.

Today's story, along with related material on The Post's website, examines how Top Secret America plays out at the local level. It describes a web of 4,058 federal, state and local organizations, each with its own counterterrorism responsibilities and jurisdictions. At least 935 of these organizations have been created since the 2001 attacks or became involved in counterterrorism for the first time after 9/11. The months-long investigation, based on nearly 100 interviews and 1,000 documents, found that:

- * Technologies and techniques honed for use on the battlefields of Iraq and Afghanistan have migrated into the hands of law enforcement agencies in America.
- * The FBI is building a database with the names and certain personal information, such as employment history, of thousands of U.S. citizens and residents whom a local police officer or a fellow citizen believed to be acting suspiciously. It is accessible to an increasing number of local law enforcement and military criminal investigators, increasing concerns that it could somehow end up in the public domain.
- * Seeking to learn more about Islam and terrorism, some law enforcement agencies have hired as trainers self-described experts whose extremist views on Islam and terrorism are considered inaccurate and counterproductive by the FBI and U.S. intelligence agencies.
- * The Department of Homeland Security sends its state and local partners intelligence reports with little meaningful guidance, and state reports have sometimes inappropriately reported on lawful meetings.

The need to identify U.S.-born or naturalized citizens who are planning violent attacks is more urgent than ever, U.S. intelligence officials say. This month's FBI sting operation involving a Baltimore construction worker who allegedly planned to bomb a Maryland military recruiting station is the latest example. It followed a similar arrest of a Somali-born naturalized U.S. citizen allegedly seeking to detonate a bomb near a Christmas tree lighting ceremony in Portland, Ore. There have been nearly two dozen other cases just this year.

"The old view that 'if we fight the terrorists abroad, we won't have to fight them here' is just that — the old view," Homeland Security Secretary Janet Napolitano told police and firefighters recently.

The Obama administration heralds this local approach as a much-needed evolution in the way the country confronts terrorism.

However, just as at the federal level, the effectiveness of these programs, as well as their cost, is difficult to determine. The Department of Homeland Security, for example, does not know how much money it spends each year on what are known as state fusion centers, which bring together and analyze information from various agencies within a state. The total cost of the localized system is also hard to gauge. The DHS has given \$31 billion in grants since 2003 to state and local governments for homeland security and to improve their ability to find and protect against terrorists, including \$3.8 billion in 2010. At least four other federal departments also contribute to local efforts. But the bulk of the spending every year comes from state and local budgets that are too disparately recorded to aggregate into an overall total. The Post findings paint a picture of a country at a crossroads, where long-standing privacy principles are under challenge by these new efforts to keep the nation safe.

The public face of this pivotal effort is Napolitano, the former governor of Arizona, which years ago built one of the strongest state intelligence organizations outside of New York to try to stop illegal immigration and drug importation. Napolitano has taken her "See Something, Say Something" campaign far beyond the traffic signs that ask drivers coming into the nation's capital for "Terror Tips" and to "Report Suspicious Activity." She recently enlisted the help of Wal-Mart, Amtrak, major sports leagues, hotel chains and metro riders. In her speeches, she compares the undertaking to the Cold War fight against communists.

"This represents a shift for our country," she told New York City police officers and firefighters on the eve of the 9/11 anniversary this fall. "In a sense, this harkens back to when we drew on the tradition of civil defense and preparedness that predated today's concerns."

On a recent night in Memphis, a patrol car rolled slowly through a parking lot in a run-down section of town. The military-grade infrared camera on its hood moved robotically from left to right, snapping digital images of one license plate after another and analyzing each almost instantly. Suddenly, a red light flashed on the car's screen along with the word "warrant." "Got a live one! Let's do it," an officer called out. The streets of Memphis are a world away from the streets of Kabul, yet these days, the same types of technologies and techniques are being used in both places to identify and collect information about suspected criminals and terrorists. The examples go far beyond Memphis.

Hand-held, wireless fingerprint scanners were carried by U.S. troops during the insurgency in Iraq to register residents of entire neighborhoods. L-1 Identity Solutions is selling the same type of equipment to police departments to check motorists' identities.

In Arizona, the Maricopa County Sheriff's Facial Recognition Unit, using a type of equipment prevalent in war zones, records 9,000 biometric digital mug shots a month.

U.S. Customs and Border Protection flies General Atomics' Predator drones along the Mexican and Canadian borders—the same kind of aircraft, equipped with real-time, full-motion video cameras, that has been used in wars in Kosovo, Iraq and Afghanistan to track the enemy. The special operations units deployed overseas to kill the al-Qaida leadership drove technological advances that are now expanding in use across the United States. On the front lines, those advances allowed the rapid fusing of biometric identification, captured computer records and cellphone numbers so troops could launch the next surprise raid. Here at home, it's the DHS that is enamored with collecting photos, video images and other personal information about U.S. residents in the hopes of teasing out terrorists. The DHS helped Memphis buy surveillance cameras that monitor residents near high-crime housing projects, problematic street corners, and bridges and other critical infrastructure. It helped pay for license plate readers and defrayed some of the cost of setting up Memphis's crime-analysis center. All together it has given Memphis \$11 million since 2003 in homeland security grants, most of which the city has used to fight crime.

"We have got things now we didn't have before," said Memphis Police Department Director Larry Godwin, who has produced record numbers of arrests using all this new analysis and technology. "Some of them we can talk about. Some

of them we can't."

One of the biggest advocates of Memphis's data revolution is John Harvey, the police department's technology specialist, whose computer systems are the civilian equivalent of the fancier special ops equipment used by the military. Harvey collects any information he can pry out of government and industry. When officers were wasting time knocking on the wrong doors to serve warrants, he persuaded the local utility company to give him a daily update of the names and addresses of customers. When he wanted more information about phones captured at crime scenes, he programmed a way to store all emergency 911 calls, which often include names and addresses to associate with phone numbers. He created another program to upload new crime reports every five minutes and mine them for the phone numbers of victims, suspects, witnesses and anyone else listed on them. Now, instead of having to decide which license plate numbers to type into a computer console in the patrol car, an officer can simply drive around, and the automatic license plate reader on his hood captures the numbers on every vehicle nearby. If the officer pulls over a driver, instead of having to wait 20 minutes for someone back at the office to manually check records, he can use a hand-held device to instantly call up a mug shot, a Social Security number, the status of the driver's license and any outstanding warrants. The computer in the cruiser can tell an officer even more about who owns the vehicle, the owner's name and address and criminal history, and who else with a criminal history might live at the same address.

Take a recent case of two officers with the hood-mounted camera equipment who stopped a man driving on a suspended license. One handcuffed him, and the other checked his own PDA. Based on the information that came up, the man was ordered downtown to pay a fine and released as the officers drove off to stop another car. That wasn't the end of it, though.

A record of that stop—and the details of every other arrest made that night, and every summons written—was automatically transferred to the Memphis Real Time Crime Center, with three walls of streaming surveillance video and analysis capabilities that rival those of an Army command center. There, the information would be geocoded on a map to produce a visual rendering of crime patterns. This information would help the crime intelligence analysts predict trends so the department could figure out what neighborhoods to swarm with officers and surveillance cameras. But that was still not the end of it, because the fingerprints from the crime records would also go to the FBI's data campus in Clarksburg, W.Va. There, fingerprints from across the United States are stored, along with others collected by American authorities from prisoners in Saudi Arabia and Yemen, Iraq and Afghanistan.

There are 96 million sets of fingerprints in Clarksburg, a volume that government officials view not as daunting but as an opportunity. This year for the first time, the FBI, the DHS and the Defense Department are able to search each other's fingerprint databases, said Myra Gray, head of the Defense Department's Biometrics Identity Management Agency, speaking to an industry group recently. "Hopefully in the not-too-distant future," she said, "our relationship with these federal agencies—along with state and local agencies—will be completely symbiotic." At the same time that the FBI is expanding its West Virginia database, it is building a vast repository controlled by people who work in a top-secret vault on the fourth floor of the J. Edgar Hoover FBI Building in Washington. This one stores the profiles of tens of thousands of Americans and legal residents who are not accused of any crime. What they have done is appear to be acting suspiciously to a town sheriff, a traffic cop or even a neighbor.

If the new Nationwide Suspicious Activity Reporting Initiative, or SAR, works as intended, the Guardian database may someday hold files forwarded by all police departments across the country in America's continuing search for terrorists within its borders. The effectiveness of this database depends, in fact, on collecting the identities of people who are not known criminals or terrorists—and on being able to quickly compile in-depth profiles of them.

"If we want to get to the point where we connect the dots, the dots have to be there," said Richard A. McFeely, special agent in charge of the FBI's Baltimore office. In response to concerns that information in the database could be improperly used or released, FBI officials say anyone with access has been trained in privacy rules and the penalties for breaking them. But not everyone is convinced. "It opens a door for all kinds of abuses," said Michael German, a former FBI agent who now leads the American Civil Liberties Union's campaign on national security and privacy matters. "How do we know there are enough controls?"

The government defines a suspicious activity as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity" related to terrorism. State intelligence analysts and FBI investigators use the reports to determine whether a person is buying fertilizer to make a bomb or to plant tomatoes; whether she is plotting to poison a city's drinking water or studying for a metallurgy test; whether, as happened on a Sunday morning in late September, the man snapping a picture of a ferry in the Newport Beach harbor in Southern California simply liked the way it looked or was plotting to blow it up.

Suspicious Activity Report N03821 says a local law enforcement officer observed "a suspicious subject . . . taking photographs of the Orange County Sheriff Department Fire Boat and the Balboa Ferry with a cellular phone camera." The confidential report, marked "For Official Use Only," noted that the subject next made a phone call, walked to his car and returned five minutes later to take more pictures. He was then met by another person, both of whom stood and "observed the boat traffic in the harbor." Next another adult with two small children joined them, and then they all boarded the ferry and crossed the channel. All of this information was forwarded to the Los Angeles fusion center for further investigation after the local officer ran information about the vehicle and its owner through several crime databases and found nothing. Authorities would not say what happened to it from there, but there are several paths a suspicious activity report can take:

At the fusion center, an officer would decide to either dismiss the suspicious activity as harmless or forward the report to the nearest FBI terrorism unit for further investigation.

At that unit, it would immediately be entered into the Guardian database, at which point one of three things could happen:

The FBI could collect more information, find no connection to terrorism and mark the file closed, though leaving it in the database.

It could find a possible connection and turn it into a full-fledged case.

Or, as most often happens, it could make no specific determination, which would mean that Suspicious Activity Report N03821 would sit in limbo for as long as five years, during which time many other pieces of information about the man photographing a boat on a Sunday morning could be added to his file: employment, financial and residential histories; multiple phone numbers; audio files; video from the dashboard-mounted camera in the police cruiser at the harbor where he took pictures; and anything else in government or commercial databases "that adds value," as the FBI agent in charge of the database described it. That could soon include biometric data, if it existed; the FBI is working on a way to attach such information to files. Meanwhile, the bureau will also soon have software that allows local agencies to map all suspicious incidents in their jurisdiction.

The Defense Department is also interested in the database. It recently transferred 100 reports of suspicious behavior into the Guardian system, and over time it expects to add thousands more as it connects 8,000 military law enforcement personnel to an FBI portal that will allow them to send and review reports about people suspected of casing U.S. bases or targeting American personnel. And the DHS has created a separate way for state and local authorities, private citizens, and businesses to submit suspicious activity reports to the FBI and to the department for analysis.

As of December, there were 161,948 suspicious activity files in the classified Guardian database, mostly leads from FBI headquarters and state field offices. Two years ago, the bureau set up an unclassified section of the database so state and local agencies could send in suspicious incident reports and review those submitted by their counterparts in other states. Some 890 state and local agencies have sent in 7,197 reports so far. Of those, 103 have become full investigations that have resulted in at least five arrests, the FBI said. There have been no convictions yet. An additional 365 reports have added information to ongoing cases. But most remain in the uncertain middle, which is why within the FBI and other intelligence agencies there is much debate about the effectiveness of the bottom-up SAR approach, as well as concern over the privacy implications of retaining so much information on U.S. citizens and residents who have not been charged with anything.

The vast majority of terrorism leads in the United States originate from confidential FBI sources and from the bureau's collaboration with federal intelligence agencies, which mainly work overseas. Occasionally a stop by a local police officer has sparked an investigation. Evidence comes from targeted FBI surveillance and undercover operations, not from information and analysis generated by state fusion centers about people acting suspiciously.

"It's really resource-inefficient," said Philip Mudd, a 20-year CIA counterterrorism expert and a top FBI national security official until he retired nine months ago. "If I were to have a dialogue with the country about this . . . it would be about not only how we chase the unknowns, but do you want to do suspicious activity reports across the country? . . . Anyone who is not at least suspected of doing something criminal should not be in a database."

Charles Allen, a longtime senior CIA official who then led the DHS's intelligence office until 2009, said some senior people in the intelligence community are skeptical that SARs are an effective way to find terrorists. "It's more likely that other kinds of more focused efforts by local police will gain you the information that you need about extremist activities," he said.

The DHS can point to some successes: Last year the Colorado fusion center turned up information on Najibullah Zazi, an Afghan-born U.S. resident planning to bomb the New York subway system. In 2007, a Florida fusion center provided the vehicle ownership history used to identify and arrest an Egyptian student who later pleaded guilty to providing material support to terrorism, in this case transporting explosives. "Ninety-nine percent doesn't pan out or lead to anything" said Richard Lambert Jr., the special agent in charge of the FBI's Knoxville office. "But we're happy to wade through these things." Ramon Montijo has taught classes on terrorism and Islam to law enforcement officers all over the country. "Alabama, Colorado, Vermont," said Montijo, a former Army Special Forces sergeant and Los Angeles Police Department investigator who is now a private security consultant. "California, Texas and Missouri," he continued.

What he tells them is always the same, he said: Most Muslims in the United States want to impose sharia law here. "They want to make this world Islamic. The Islamic flag will fly over the White House—not on my watch!" he said. "My job is to wake up the public, and first, the first responders."

With so many local agencies around the country being asked to help catch terrorists, it often falls to sheriffs or state troopers to try to understand the world of terrorism. They aren't FBI agents, who have years of on-the-job and classroom training. Instead, they are often people like Lacy Craig, who was a police dispatcher before she became an intelligence analyst at Idaho's fusion center, or the detectives in Minnesota, Michigan and Arkansas who can talk at length about the lineage of gangs or the signs of a crystal meth addict. Now each of them is a go-to person on terrorism as well. "The CIA used to train analysts forever before they graduated to be a real analyst," said Allen, the former top CIA and DHS official. "Today we take former law enforcement officers and we call them intelligence officers, and that's not right, because they have not received any training on intelligence analysis."

State fusion center officials say their analysts are getting better with time. "There was a time when law enforcement didn't know much about drugs. This is no different," said Steven W. Hewitt, who runs the Tennessee fusion center, considered one of the best in the country. "Are we experts at the level of (the National Counterterrorism Center)? No. Are we developing an expertise? Absolutely." But how they do that is usually left up to the local police departments themselves. In their desire to learn more about terrorism, many departments are hiring their own trainers. Some are self-described experts whose extremist views are considered inaccurate and harmful by the FBI and others in the intelligence community.

Like Montijo, Walid Shoebat, a onetime Muslim who converted to Christianity, also lectures to local police. He too believes that most Muslims seek to impose sharia law in the United States. To prevent this, he said in an interview, he warns officers that "you need to look at the entire pool of Muslims in a community." When Shoebat spoke to the first annual South Dakota Fusion Center Conference in Sioux Falls this June, he told them to monitor Muslim student groups and local mosques and, if possible, tap their phones. "You can find out a lot of information that way," he said.

A book expanding on what Shoebat and Montijo believe has just been published by the Center for Security Policy, a Washington-based neoconservative think tank. "Shariah: The Threat to America" describes what its authors call a "stealth jihad" that must be thwarted before it's too late. The book's co-authors include such notables as former CIA director R. James Woolsey and former deputy undersecretary of defense for intelligence Lt. Gen. William G. Boykin, along with the center's director, a longtime activist. They write that most mosques in the United States already have been radicalized, that most Muslim social organizations are fronts for violent jihadists and that Muslims who practice sharia law seek to impose it in this country. Frank Gaffney Jr., director of the center, said his team has spoken widely, including to many law enforcement forums. "Members of our team have been involved in training programs for several years now, many of which have been focused on local law enforcement intelligence, homeland security, state police, National Guard units and the like," Gaffney said. "We're seeing a considerable ramping-up of interest in getting this kind of training."

Government terrorism experts call the views expressed in the center's book inaccurate and counterproductive. They say the DHS should increase its training of local police, using teachers who have evidence-based viewpoints. DHS spokeswoman Amy Kudwa said the department does not maintain a list of terrorism experts but is working on guidelines for local authorities wrestling with the topic. So far, the department has trained 1,391 local law enforcement officers in analyzing public information and 400 in analytic thinking and writing skills. Kudwa said the department also offers counterterrorism training through the Federal Emergency Management Agency, which this year enrolled 94 people in a course called "Advanced Criminal Intelligence Analysis to Prevent Terrorism." The DHS also provides local agencies a daily flow of information bulletins.

These reports are meant to inform agencies about possible terror threats. But some officials say they deliver a never-ending stream of information that is vague, alarmist and often useless. "It's like a garage in your house you keep throwing junk into until you can't park your car in it," says Michael Downing, deputy chief of counterterrorism and special operations for the Los Angeles Police Department. A review of nearly 1,000 DHS reports dating back to 2003 and labeled "For Official Use Only" underscores Downing's description. Typical is one from May 24, 2010, titled "Infrastructure Protection Note: Evolving Threats to the Homeland." It tells officials to operate "under the premise that other operatives are in the country and could advance plotting with little or no warning." Its list of vulnerable facilities seems to include just about everything: "Commercial Facilities, Government Facilities, Banking and Financial and Transportation . . ."

Bart R. Johnson, who heads the DHS's intelligence and analysis office, defended such reports, saying that threat reporting has "grown and matured and become more focused." The bulletins can't be more specific, he said, because they must be written at the unclassified level. Recently, the International Association of Chiefs of Police agreed that the information they were receiving had become "more timely and relevant" over the past year. Downing, however, said the reports would be more helpful if they at least assessed threats within a specific state's boundaries. States have tried to do that on their own, but with mixed, and at times problematic, results.

In 2009, for instance, after the DHS and the FBI sent out several ambiguous reports about threats to mass-transit systems and sports and entertainment venues, the New Jersey Regional Operations Intelligence Center's Threat Analysis Program added its own information. "New Jersey has a large mass-transit infrastructure," its report warned, and "an NFL stadium and NHL/NBA arenas, a soccer stadium, and several concert venues that attract large crowds."

In Virginia, the state's fusion center published a terrorism threat assessment in 2009 naming historically black colleges as potential hubs for terrorism. From 2005 to 2007, the Maryland State Police went even further, infiltrating and labeling as terrorists local groups devoted to human rights, antiwar causes and bike lanes. And in Pennsylvania this year, a local contractor hired to write intelligence bulletins filled them with information about lawful meetings as varied as Pennsylvania Tea Party Patriots Coalition gatherings, antiwar protests and an event at which environmental activists dressed up as Santa Claus and handed out coal-filled stockings. Even if the information were better, it might not make a difference for the simplest of reasons: In many cities and towns across the country, there is just not enough terrorism-

related work to do. In Utah on one recent day, one of five intelligence analysts in the state's fusion center was writing a report about the rise in teenage overdoses of an over-the-counter drug. Another was making sure the visiting president of Senegal had a safe trip. Another had just helped a small town track down two people who were selling magazine subscriptions and pocketing the money themselves. In the Colorado Information Analysis Center, some investigators were following terrorism leads. Others were looking into illegal Craigslist postings and online "World of Warcraft" gamers. The vast majority of fusion centers across the country have transformed themselves into analytical hubs for all crimes and are using federal grants, handed out in the name of homeland security, to combat everyday offenses.

This is happening because, after 9/11, local law enforcement groups did what every agency and private company did in Top Secret America: They followed the money. The DHS helped the Memphis Police Department, for example, purchase 90 surveillance cameras, including 13 that monitor bridges and a causeway. It helped buy the fancy screens on the walls of the Real Time Crime Center, as well as radios, robotic surveillance equipment, a mobile command center and three bomb-sniffing dogs. All came in the name of port security and protection to critical infrastructure. Since there hasn't been a solid terrorism case in Memphis yet, the equipment's greatest value has been to help drive down city crime. Where the mobile surveillance cameras are set up, criminals scatter, said Lt. Mark Rewalt, who, on a recent Saturday night, scanned the city from an altitude of 1,000 feet. Flying in a police helicopter, Rewalt pointed out some of the cameras the DHS has funded. They are all over the city, in mall parking lots, in housing projects, at popular street hang-outs. "Cameras are what's happening now," he marveled.

Meanwhile, another post-9/11 unit in Tennessee has had even less terrorism-related work to do. The Tennessee National Guard 45th Weapons of Mass Destruction Civil Support Team, one of at least 50 such units around the country, was created to respond to what officials still believe is the inevitable release of chemical, biological or radiological material by terrorists. The unit's 22 hazardous-materials personnel have the best emergency equipment in the state. A fleet of navy-blue vehicles—command, response, detection and tactical operations trucks—is kept polished and ready to roll in a garage at the armory in Smyrna. The unit practices WMD scenarios constantly. But in real life, the crew uses the equipment very little: twice a year at NASCAR races in nearby Bristol to patrol for suspicious packages. Other than that, said Capt. Matt Hayes, several times a year they respond to hoaxes. The fact that there has not been much terrorism to worry about is not evident on the Tennessee fusion center's Web site. Click on the incident map, and the state appears to be under attack.

Red icons of explosions dot Tennessee, along with blinking exclamation marks and flashing skulls. The map is labeled: "Terrorism Events and Other Suspicious Activity. But if you roll over the icons, the explanations that pop up have nothing to do with major terrorist plots: "Johnson City police are investigating three 'bottle bombs' found at homes over the past three days," one description read recently. "... The explosives were made from plastic bottles with something inside that reacted chemically and caused the bottles to burst." Another told a similar story: "The Scott County Courthouse is currently under evacuation after a bomb threat was called in Friday morning. Update: Authorities completed their sweep . . . and have called off the evacuation."

Nine years after 9/11, this map is part of the alternative geography that is Top Secret America, where millions of people are assigned to help stop terrorism. Memphis Police Director Godwin is one of them, and he has his own version of what that means in a city where there have been 86 murders so far this year. "We have our own terrorists, and they are taking lives every day," Godwin said. "No, we don't have suicide bombers—not yet. But you need to remain vigilant and realize how vulnerable you can be if you let up."