MORE ABOUT SUSPICIOUS ACTIVITY REPORTING

Law enforcement agencies have long collected information about their routine interactions with members of the public. Sometimes called "field interrogation reports" or "stop and frisk" records, this documentation, on the one hand, provides a measure of accountability over police activity. But it also creates an opportunity for police to collect the personal data of innocent people and put it into criminal intelligence files with little or no evidence of wrongdoing. As police records increasingly become automated, law enforcement and intelligence agencies are increasingly seeking to mine this routine contact information and distribute it broadly, as if it is criminal intelligence information. With new intelligence sharing systems like fusion centers, Joint Terrorism Task Forces and the Director of National Intelligence (DNI) Information Sharing Environment (ISE), information collected by local police in any city or small town in America can now quickly end up in federal intelligence databases.

SARs and the Reasonable Suspicion Standard. The Supreme Court established "reasonable suspicion" as the standard for police stops in *Terry v. Ohio* in 1968. This standard required suspicion supported by articulable facts suggesting criminal activity was afoot before a policeman could stop a person for investigative purposes. Likewise, the Department of Justice established a reasonable suspicion standard for the inclusion of personally identifiable information into criminal intelligence systems. Title 28, Part 23 of the Code of Federal Regulations states that law enforcement agencies receiving federal funds:

> "shall collect and maintain criminal intelligence information concerning an individual *only if there is reasonable suspicion that the individual is involved in criminal conduct or activity* and the information is relevant to that criminal conduct or activity [emphasis added]."

SAR programs threaten this reasonable, time-tested law enforcement standard by encouraging the police and the public to report behaviors that do not give rise to reasonable suspicion of criminal or terrorist behavior.

In January 2008 the DNI ISE Program Manager published functional standards for state and local law enforcement officers to report 'suspicious' activities to fusion centers and to the federal intelligence community through the ISE. The behaviors it described as inherently suspicious included such innocuous activities as photography, acquisition of expertise, and eliciting information. The following March the Los Angeles Police Department (LAPD) initiated its own SAR program to "gather, record, and analyze information of a criminal *or non-criminal nature*, that could indicate activity or intentions related to either foreign or domestic terrorism," and included a list of 65 behaviors LAPD officers "shall" report, which included taking pictures or video footage, taking notes, drawing diagrams and espousing extreme views. In June 2008, long before either of these programs could be evaluated, the Departments of Justice and Homeland Security teamed up with the Major City Chiefs Association to issue a report recommending expanding the SAR program to other U.S. cities. (Indeed, in April 2009 the LAPD admitted its SAR program had not foiled any terrorist threats during its first year in operation.) The FBI began its own SAR collection program called eGuardian in 2008, and in 2010 the military announced it would implement a SAR program through eGuardian.

Criticism and Response. The ACLU released a report criticizing these SAR programs in July 2008. In response, ISE program manager Thomas E. McNamara and his office worked with the ACLU and other privacy and civil liberties groups, as well as the LAPD and other federal, state and local law enforcement agencies, to revise the ISE SAR functional standard to address privacy and civil liberties concerns.

The revised ISE standard for suspicious activity reporting, issued in May 2009, indicates that a reasonable connection to terrorism or other criminal activity is required before law enforcement officers may collect Americans' personal information and share it within the ISE. It includes language affirming that all constitutional standards applicable to ordinary criminal investigations, such as the *Terry* reasonable suspicion test for whether a law enforcement officer can stop and question an individual, also apply to officers conducting SAR inquiries (see page 7). The revised ISE functional standard also makes clear that behaviors such as photography and eliciting information are protected under the First Amendment, and require additional facts and circumstances giving reason to believe the behavior is related to crime or terrorism before reporting is appropriate (see page 29). These changes to the standard, which include reiterating that race, ethnicity and religion cannot be used as factors that create suspicion (see page 7 and 29), led us to believe that law enforcement would have the authority it needs while ensuring greater respect for individuals' privacy and civil liberties. We applauded the willingness of the ISE Program Manager to engage constructively with the civil liberties community and to make modifications to the functional standard to address the concerns presented.

It has become clear, however, that the Program Manager does not interpret the Functional Standard consistently with its plain language, or with our understanding at the time the standard was issued that it required reasonable suspicion of criminal activity. In fact, the Program Manager has expressly acknowledged that the Functional Standard requires "less than the ‘reasonable suspicion' standard." *See* PM-ISE, Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations–Nationwide Suspicious Activity Reporting Initiative at 12 (draft May 2010). That increases the likelihood that "intelligence" will be gathered about innocuous or constitutionally protected activity.

Competing Standards and Proliferation of Reports. The FBI has adopted a separate, even less stringent standard for suspicious activity reporting: "observed behavior that *may be indicative* of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention." As is the case with the ISE Functional Standard, the FBI standard does not require reasonable suspicion of criminal activity. These competing standards not only have resulted in confusion over whether specific conduct meets the standard for suspicious activity reporting, but they also have too often led to inappropriate law enforcement contact with completely innocent Americans. These inappropriate contacts include stops and arrests based on nothing more than First Amendment-protected activities and the unwarranted collection of personally identifiable information. For example, a 2010 government evaluation of the ISE SAR program reveals that the Virginia Fusion Center processed 347 SARs, only 7 of which met the ISE SAR standard, while the Florida Department of Law Enforcement processed a whopping 5,727 SARs, with only 12 meeting the ISE SAR standard (see page 32).

Due to the disparity in the SAR programs across the country, law enforcement officers on the beat are still being encouraged to collect information about people engaged in commonplace behaviors. This overbroad reporting mandate is not just constitutionally questionable; it's also counterproductive. These orders, if taken seriously by local law enforcement, can yield only one outcome: an ocean of data about innocent individuals that will overwhelm the investigative resources of the authorities. In attempting to put the intelligence community's failure to pursue investigative leads regarding the attempted bombing of an airplane over Detroit on December 25, 2009 into context, National Counterterrorism Center (NCTC) Director Michael Leiter complained that the NCTC receives "literally thousands" of pieces of intelligence every day. Adding innocuous information about the everyday activities of Americans will only increase this burden on intelligence resources. The police should instead focus their efforts and resources by collecting information only where there is a reasonable factual basis for suspecting misconduct.

Rather than tightening SAR collection standards, however, many federal, state and local law enforcement agencies are expanding them by encouraging not just police but the general public to report suspicious activity. The FBI, DHS and the Colorado fusion center teamed to produce a fear-inducing video that describes photography, using binoculars and even soliciting donations for charity as precursors to terrorism. The Michigan State Police have a similar video, the LAPD has a program called iWatch, and the Arizona fusion center has a website encouraging the public to report these same behaviors, as do many other state and local law enforcement agencies.

These programs are eerily similar to former Attorney General John Ashcroft's TIPS program, which encouraged meter-readers and postmen to spy on their neighbors until Congress ended it in late 2002 due to civil liberties concerns. And these SAR programs don't have the same limiting language—which has apparently been ignored—that was added to the ISE functional standard, making it even more likely that both the police and the public will continue over-reporting the commonplace behavior of their neighbors.

The George Washington University Homeland Security Policy Institute published a survey of fusion center employees in September 2012, which characterized suspicious activity reports as "white noise" that impeded effective intelligence analysis.

Racial Disparities in Stop and Frisk Data. Adopting and maintaining a reasonable suspicion standard for law enforcement stops and for the collection, retention and dissemination of personally identifiable information is a necessary, though not a sufficient methodology for protecting the rights and privacy of innocent people. Oversight and effective enforcement of the standard are critical to ensuring law enforcement authorities are not abused. For instance, the New York Civil Liberties Union obtained "stop and frisk" data from the New York Police Department which revealed that almost nine out of ten of the nearly three million people it stopped since 2004 were non-white. And though the NYPD should have been using the reasonable suspicion standard required under *Terry*, only about 10 percent of those stopped by the NYPD actually received summonses or were arrested. Yet the NYPD collected and retained the personal information of the innocent people it stopped as well as the guilty. In effect, NYPD is creating a massive database of innocent people of color in New York City. Such racial disparities in stop and frisk data should be a warning to police departments implementing SAR programs.

SAR Abuse Focusing on Photography Photographers appear to be among the most frequent targets of SAR and SAR-like information collection efforts. Whether lawfully photographing scenic railroad stations, government-commissioned art displays outside federal buildings or national landmarks, citizens, artists and journalists have been systematically harassed or detained by federal, state, and local law enforcement. In some instances, the ensuing confrontation with police escalates to the point where the photographer is arrested and their photos erased or cameras confiscated with no reasonable indication that criminal activity is involved. A Los Angeles Sheriff's Deputy even threatened to put a subway photographer on the Terrorist Watchlist.

Comedian Stephen Colbert had a light-hearted take on the story of a man arrested by Amtrak police for photographing an Amtrak train for an Amtrak photography contest, but illegal arrests of innocent Americans exercising their right to photograph in public (like this and this and this) are happening too often to be just a laughing matter. Congress held hearings into the harassment of photographers at Washington, D.C.'s Union Station and at the U.S. Department of Transportation. Several government agencies, including the New York Police Department (NYPD), the San Francisco Municipal Transit Authority (MUNI), the Department of Transportation, and Amtrak have had to send out memos to their police officers and security personnel reiterating that photography is not a crime. Given the contradictory messages sent by SAR programs, however, it is not surprising there is confusion among the officers on the street.

There is also evidence that some law enforcement officers are using SAR or SAR-like criteria to abuse their power. Many SAR programs describe photography of security personnel or facilities as a precursor to terrorism and a growing number of cases, such as those in Maryland, Washington, Tennessee, New Jersey, Boston, and Miami, involve police harassment, demands for identification, and even arrests of photographers for taking pictures or video documenting law enforcement officers in the performance of their duties. None of these incidents involved any reasonable links to terrorism or other threats to security. SAR criteria have also been used as a pretext for local law enforcement to check immigration status, and played a precipitating role in the arrest of a political activist in Connecticut.

Lack of Evidence That SAR Policing is Effective in Combating Terrorism. For all the potential impact on the rights and privacy of innocent people, there is little objective evidence that SAR programs are effective in identifying and interdicting acts of terrorism. A 2010 ISE SAR evaluation report indicated that few of the participating SAR programs studied were able to fully implement the ISE SAR process and share data; several of the SAR programs studied had difficulty in providing statistics on the SARs it received; and the majority of SAR programs could not calculate the number of arrests and investigations resulting from SARs (pages 31-32).

Moreover, other government studies question whether there is any scientific basis for believing that a behavioral detection program can be effective in countering terrorism. A 2008 National Academies of Science National Research Council study funded by DHS found that there is no consensus in the scientific community that behavioral detection systems to identify terrorists could be scientifically validated. Likewise, a 2010 Government Accountability Office review of the Transportation Security Agency's behavioral detection system called Screening of

Passengers by Observation Techniques (SPOT), in which Behavioral Detection Officers are purportedly trained to identify threats to aviation by looking for suspicious behavior and appearance, confirmed that no large-scale security screening program based on behavioral indicators has ever been scientifically validated (page 14). GAO noted that while Behavioral Detection Officers had sent over 150,000 travelers to secondary screening there is no evidence the program ever identified a terrorist or other threat to aviation (page 46). Meanwhile, at least 16 individuals suspected of involvement in terrorist plots traveled 23 times through 8 SPOT airports undetected (pages 46-47). Behavioral detection programs like SAR and SPOT, which pose significant threats to civil rights and privacy, must be proven effective before they are implemented or they will simply waste security resources.

Related Issues: Privacy and Surveillance, National Security