Using 911 Calls to Detect Terrorism Threats

by Kevin J. Strom, John Hollywood and Mark Pope

Terrorists frequently engage in surveillance activities when selecting a target and planning an attack.[1] Needless to say, when we are able to spot such surveillance activities, we stand a greater chance of preventing an attack. In 2007, for example, authorities thwarted a terrorist plot in Germany when they caught people surveying U.S. military facilities near Hanau.[2] In 2006, two men were charged with videotaping the U.S. Capitol building, the World Bank, a Masonic temple and a fuel depot in Washington, D.C., to send to overseas terrorist groups.[3] And in 2004, the U.S. Department of Homeland Security raised the terrorist threat level following reports of terrorist surveillance of key financial institutions in New York City, New Jersey and Washington, D.C.[4]

Pre-attack surveillance can include videotaping, photographing, or taking notes on or drawing sketches of a building's structural components or security defenses. Other activities might involve trespassing in secure areas, asking detailed questions about a target's occupants or defenses, or leaving suspicious packages or making bomb threats to study emergency response procedures. These behaviors — also known as "hostile surveillance" — require terrorists to temporarily expose themselves and reveal their true intentions.

Suspicious activity reports document behavior (including criminal and attempted criminal acts that may be related to terrorism) reported by citizens or observed by police.[5] Information in a SAR can come from unclassified sources — such as 911 calls for service, field interview reports, crime incident narrative reports and site security logs — or from classified sources, such as informant tips or law enforcement investigation reports.

Developing a comprehensive process for identifying and analyzing information from SARs could enable police to prevent or deter a terrorist attack. But in trying to pull this information quickly out of SARs, law enforcement agencies face two major challenges:

- **Identifying:** How to efficiently identify and prioritize cases of interest from the large volume of SARs.
- **Analyzing:** How to analyze SARs that often have dissimilar formats and that contain open-text comment fields that must be searched for key data.

Identifying cases of interest is not easy: Attempting to determine if suspicious behavior is truly indicative of something more sinister is like looking for the proverbial needle in the haystack. Potentially hostile surveillance is, of course, intended to appear innocuous to the casual observer. And as every law enforcement officer knows, behaviors can be misinterpreted by citizens, officers or security personnel, which, in turn, can result in "false-positive" reports.

Analyzing information from SARs is also inherently challenging. For example, only a small number of potential terrorist-related activities may be contained in a 911 call database of thousands of SARs. The large volume of data requires a filter process, a process to separate the merely suspicious from true terrorist surveillance activities. Most law enforcement agencies, however, have had limited guidance on analyzing, prioritizing and disseminating operationally relevant information from SAR data sources that often are in different formats and that contain comment fields not easily comparable.

In 2006, the National Institute of Justice funded RTI International to develop and test a process for analyzing and prioritizing data from one type of SAR: 911 calls for service.[6] As part of that project, RTI researchers (including the authors of this article), in collaboration with the Washington, D.C., Metropolitan Police Department, analyzed more than 1.3 million 911 MPD call records.

The main goal of our study was not to identify confirmed terrorist activity. Rather, we designed and tested a process for reducing a large volume of data to a smaller subset of incidents that could then be reviewed for follow-up investigation. Our study showed that simple analytic processes could produce operationally relevant findings from 911 calls. We documented this process so it could be implemented and refined in other jurisdictions.

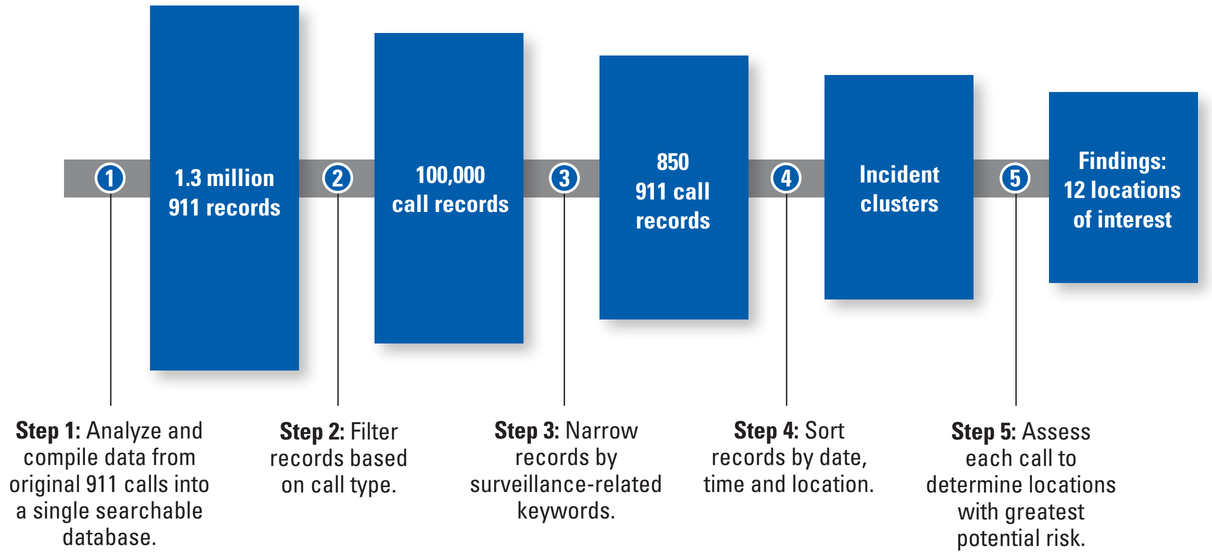
Our study showed that simple analytic processes could produce operationally relevant findings from 911 calls.

Analyzing 911 Calls

There are several advantages to being able to use 911 call records to detect potential terrorist activities. First, in one sense, data have already been "filtered" through the citizen's perception: that is, before a person makes a 911 call, the suspicious behavior has already risen to a certain level of seriousness in his or her mind. Second, 911 calls constitute public information that can be analyzed without infringing on individual privacy rights (unlike analyses of personal data from credit card transactions and phone records, for example, which have come under heavy criticism for violating privacy).[7] Perhaps most importantly, 911 calls include behaviors underreported in other police data sources. For instance, if police respond to a suspicious activity call and the suspect is no longer at the scene, a formal incident report may not be completed.

The process we developed to analyze 911 calls has five major steps (see, "Identifying Potential Terrorist Behavior Using 911 Calls: A Five-Step Process," page 26). These steps can be easily replicated and do not require extensive technical training or software. Once refined and tested in additional jurisdictions, this process could be implemented more widely to monitor suspicious activity as part of a police department's homeland security and crime prevention efforts.

Identifying Potential Terrorist Behavior Using 911 Calls: A Five-Step Process



Step 1: Analyze and compile data from original 911 calls into a single searchable database.

Step 2: Filter records based on call type.

Step 3: Narrow records by surveillance-related keywords.

Step 4: Sort records by date, time and location.

Step 5: Assess each call to determine locations with greatest potential risk.

Step 1: We started with more than 1.3 million electronic 911 call records that spanned a 20-month period. There were two types of records: one with consistent data fields and one with text of the conversation between the 911 operator and the caller. In this step, we compiled data into a single searchable database, including call location (for example, geospatial coordinates, cross streets or addresses); call date and time; type of call (for example, bomb threats or suspicious persons, vehicles or packages); and comments entered by the 911 operator.

Step 2: We filtered the records based on their call type: "suspicious persons," "suspicious vehicles," "suspicious packages," "bomb threats," "investigate the trouble" and "other." This narrowed the data to about 100,000 records.

Step 3: We searched the 100,000 records for surveillance-related keywords: video, photography, taking notes and using visual aids. This narrowed the records search to approximately 1,200, which we then manually reviewed. Our manual review reduced the pool of potential hostile surveillance or probing records to about 850.

Step 4: We sorted the 850 records by location, time and type of activity to identify clusters of incidents in time and space. "Space" refers to the same address or addresses that are close by. "Time" refers to clusters in a particular space that occurred within a few months or, in some cases,

Surveillance-Related Keywords

Type of Surveillance	Keywords Used in the 911 Call
Photography	Photo, Camera, Picture
Video	Video, Taping, Film, Camcorder
Note-taking	Note, Write, Typing
Visual Aids	Binocular, Telescope, Lens

Assessing Potential Preoperational Surveillance Incidents

Location of Interest	Evidence Indicating Possible Terrorist Surveillance	Evidence Mitigating Against Possible Terrorist Surveillance
Highway bridges and overpasses	• 16 incidents in 6 clusters. • 3 additional calls (not in the 6 clusters) for trespassing in bridge infrastructure. • Disruption to this area would have major consequences.	• Stopped cars and people on highways are more likely to be noticed. • Site provides scenic views for tourists.
Highway tunnels and exits	• 9 incidents. • 5 of these 9 incidents were similar calls for a man taking pictures of traffic.	• Stopped cars and people are more likely to be noticed. • Cluster is comparatively old (calls occurred in 2005).
Military facilities	• 9 incidents, most concerned people taking pictures of the facilities from a highway or a bridge.	• Stopped cars and people on highways are more likely to be noticed. • Sites provide scenic views for tourists.
Hospital	• 2 calls about a woman taking photos; 1 involved a chemical facility.	• Cluster is comparatively old (calls occurred in 2005).
Power plant	• 3 calls for taking photos of a power plant.	• Cluster is comparatively old (calls occurred in 2005).

days. Incident locations were plotted using geographic software to find geographic clusters. We also looked for spikes in potential surveillance incidents across similar types of locations, such as hotels, hospitals and other types of landmarks and infrastructure.

Step 5: We assessed the risk of each call to identify locations of greatest potential risk. In consultation with MPD, we developed a risk-assessment framework that assigned a score to the potential preoperational surveillance incidents based on a 10-point scale. We used four main factors to assess risk:

- Is the incident atypical, or can it be easily explained by tourist activities, albeit somewhat unusual activities, such as taking pictures of a bridge?
- Is the location attractive for an attack? For example, is it a well-known landmark? Could an attack result in significant casualties?
- Is the call part of a larger cluster for the same target?
- Was a police report filed?

Looking at the scores, we identified 12 locations that had multiple incidents and were assessed to be at moderate risk or higher; these became our "locations of interest." We searched for additional evidence that the locations of interest were, in fact, being targeted. We queried the database for all calls that involved suspicious activity at these locations, even calls that had been previously filtered out. We reviewed every incident at those locations for any additional incident potentially related to surveillance or probing.

What Was Identified?

This five-step process reduced the amount of information to a manageable level for a human analyst. Out of the more than 1.3 million calls that initially went into the

This five-step process reduced the amount of information to a manageable level for a human analyst. Out of the more than 1.3 million calls that initially went into the database, 175 calls for 12 locations were identified as potentially related to preoperational terrorist activities.

database, 175 calls for 12 locations were identified as potentially related to preoperational terrorist activities.

We looked at the evidence indicating possible terrorist surveillance for each location and the evidence mitigating against it being terrorist related. Evidence that locations of interest were potentially being targeted included having a cluster of recognized incidents within a small defined area. Evidence that mitigated against a location being a target included other likely explanations for the behavior.

Based on the evidence, we identified five areas from the 12 locations of interest that warranted further investigation (see "Assessing Potential Preoperational Surveillance Incidents," page 27). MPD staff determined that some of the incidents could be explained by routine tourist behavior. For example, it was likely that most of the highway and bridge incidents were tourists taking photos, despite some personal risk from traffic. However, cases of trespassing within a bridge infrastructure (underneath the bridge or within the bridge support structure) were cause for concern.

What Are the Next Steps?

The Office of the Director of National Intelligence is working toward establishing a nationwide capacity to gather, analyze and share terrorism-related suspicious activity reports. This evolving process also seeks to ensure that privacy is protected and civil liberties are guarded.[8]

Developing a systematic approach for monitoring 911 calls for suspicious activity is important for our nation's homeland security. We cannot rely solely on an alert patrol officer or 911 dispatcher to identify relevant cases; rather, we need an automated process for filtering calls related to potential terrorist activity from the large volume of 911 calls. Recently, important steps have been taken in outlining the basic processes for standardizing the gathering, processing and analysis of suspicious activity by law enforcement agencies.[9] Our study addressed two aspects of these processes: As described above, we first developed and tested a method for filtering 911 call data to isolate those records most likely associated with potential terrorist-related activities; then we used a straightforward analytic process that does not require specialized software.

Plans are under way to continue to refine this method by automating some of the data-processing steps and testing it in additional U.S. jurisdictions. As our study demonstrated, analyzing 911 call data can reveal previously unknown information or shed light on existing information to help identify high-risk locations within and across cities. More broadly, information identified from 911 data and other sources can be used to establish a baseline level of suspicious activity in a jurisdiction that can be monitored over time.

This method for analyzing 911 calls might also be used in traditional ("predictive

About the Authors

Kevin J. Strom, Ph.D., is a senior scientist in RTI International's Crime, Violence and Justice Program. His research has focused on law enforcement responses to community violence and interagency coordination in response to terrorism.

John Hollywood, Ph.D., is an operations researcher in RTI International's Crime, Violence and Justice Program. He has more than 10 years of experience in justice, counterterrorism, counterinsurgency and intelligence research, including developing concepts for counterterrorism intelligence analysis.

Mark Pope is a research analyst in RTI International's Crime, Violence and Justice Program. He has more than eight years of experience in criminal justice research, including using information technology to develop data-driven responses to crime.

policing") crime prevention. Many 911 calls about suspicious or criminal activity — for example, calls about drug activity, disorderly conduct and suspicious activity related to criminal activities (casing locations or victims) — do not result in formal police reports. This means that important information is lost, leaving analysts only with crime incident and arrest data that may be insufficient for analyzing local crime trends and predicting emerging patterns in crime. By analyzing 911 calls-for-service data and identifying normal levels of activity, it may be possible to identify and predict small-area upswings in crime. Such analysis could also enhance our understanding of which types of suspicious and criminal activity are precursors to violent crime.

Ultimately, the systematic use of this data could help law enforcement agencies take more complete advantage of citizen reporting, both in terms of counterterrorism and crime prevention.

NCJ 226874

For More Information

- Hollywood, J., K. Strom, and M. Pope, *Developing and Testing a Method for Using 911 Calls for Identifying Potential Pre-Planning Terrorist Surveillance Activities,* final report submitted to the National Institute of Justice, U.S. Department of Justice, Washington, DC: May 2008 (NCJ 222911), available at www.ncjrs.gov/pdffiles1/nij/grants/222911.pdf.
- Hollywood, J.S., K.J. Strom, and M. Pope, "Using 9-1-1 Calls for Service to Identify Potential Instances of Terrorist Surveillance," *Police Chief* 75 (10) (October 2008): 160, 163, 165, available at http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1651&issue_id=102008.
- Information Sharing Environment, "Nationwide Suspicious Activities Reporting (SAR) Initiative," Washington, DC: Information Sharing Environment, available at www.ise.gov/pages/sar-initiative.html.
- U.S. Department of Justice, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project,* Washington, DC: U.S. Department of Justice, June 2008, available at http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.

Notes

1. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report,* Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004, available at http://govinfo.library.unt.edu/911/report/911Report.pdf.
2. Landler, M., "German Police Arrest 3 in Terror Plot," *New York Times,* September 6, 2007, available at www.nytimes.com/2007/09/06/world/europe/06germany.html?_r=1.
3. Associated Press, "Prosecutors Allege Suspects Shot 'Casing Video,'" MSNBC, April 28, 2006, available at www.msnbc.msn.com/id/12539510.
4. Office of the Press Secretary, "Remarks by Secretary of Homeland Security Tom Ridge Regarding Recent Threat Reports," press release from the U.S. Department of Homeland Security, August 1, 2004, available at www.dhs.gov/xnews/releases/press_release_0471.shtm.
5. U.S. Department of Justice, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project,* Washington, DC: U.S. Department of Justice, June 2008, available at http://online.wsj.com/public/resources/documents/mccarecommendation-06132008.pdf.
6. Hollywood, J., K. Strom, and M. Pope, *Developing and Testing a Method for Using 911 Calls for Identifying Potential Pre-Planning Terrorist Surveillance Activities,* final report submitted to the National Institute of Justice, U.S. Department of Justice, Washington, DC: May 2008 (NCJ 222911), available at www.ncjrs.gov/pdffiles1/nij/grants/222911.pdf.
7. O'Harrow, R., "Centers Tap Into Personal Databases: State Groups Were Formed After 9/11," *Washington Post,* April 2, 2008, available at www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html.
8. Information Sharing Environment, "Nationwide Suspicious Activities Reporting (SAR) Initiative," Washington, DC: Information Sharing Environment, available at www.ise.gov/pages/sar-initiative.html.
9. O'Harrow, "Centers Tap Into Personal Databases."