

Suspicious Activity Reporting

Terrorism

Author:

Stephen G Serrao

Date

December 2009

Suspicious Activity Reporting and Its Growing Prominence in Interdicting Criminal, Terrorist Plots

By Stephen G. Serrao, Captain, New Jersey State Police (ret.)

Prior to 9/11, police agencies generally referred to information coming in from the public as “Tips.” Often, these came from “800” tip lines, where citizens could call and leave information. Activities that might have some indication of criminal actions or that were observed by police officers also were referred to as Tips. Conversely, when police were investigating a specific crime and citizens reported information relative to that crime, then that was generally called lead information or “Leads.”

Tips and Leads were considered distinct categories of information in the day-to-day work of law enforcement professionals. Tips and Leads were handled by separate systems. Generally, there were no computerized systems whatsoever for tracking them.

That all changed with 9/11. Thousands of citizens reporting Tips and Leads flooded police departments across the country. The Federal Bureau of Investigation’s (FBI) own Rapid Start Lead Management program for terrorism-related tips was inundated with phone calls, e-mails and letters from the public. I remember my own agency in New Jersey received several thousand calls from citizens over the course of several days immediately following the World Trade Center collapse.

Evolution of Tips and Leads

It became apparent to large police agencies across the country and the new counter-terrorism units being formed, including the Department of Homeland Security, that there was a need for a centralized system for Tips and Leads – one where information could be captured, categorized, and catalogued. Otherwise, how could any of this seemingly disjointed tips and leads information be analyzed for specific patterns of crime, or crime in the making? Many forward-thinking law enforcement agencies built formal statewide systems for capturing and processing Tips and Leads.

Such systems became repositories for capturing, storing, analyzing, vetting and acting upon this type of information. For the most part, these tips and leads were fed into a central repository where they could be vetted to ascertain if there was any nexus to terrorism or other planned criminal activities. Among their daily activities, Fusion Centers became the clearinghouses for Tips and Leads, with trained officers examining

the data to potentially connect the “dots” to terrorism-related planning and other activities.

Local Tips and Leads related to terrorism were usually forwarded to the FBI – JTTF (Joint Terrorism Task Force), while others related to drug, organized crime and non-terrorism, for example, remained in local or municipal jurisdictions. At the federal level, the FBI established a new Tips and Leads program called Guardian for managing terrorism-related suspicious activity. Even then, the question of what constitutes true Tips and Leads was on the minds of commanders and officers at local, tribal and state agencies.

SAR Support and Implementation Project

About 18 months ago, officials from the Office of the Director of National Intelligence (ODNI), the Bureau of Justice Assistance, the Los Angeles Police Department, and several other large police agencies convened a working group called, “SAR Support and Implementation Project.” This group spearheaded an initiative to explore how best to standardize and share Tips and Leads data, and to further utilize the information in their Record Management Systems (RMS). These systems which record the activity of police interacting with thousands of citizens each day could provide very useful information to other law enforcement entities. Suspicious Activity Reporting (SAR) has become the new ‘catch-phrase’ for Tips and Leads in law enforcement circles. It is regarded as a more accurate term for citizen observations and police reporting.

But what is SAR, and how should one define it? One definition is the “official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention.”

Determining when non-suspect activity becomes suspect activity can be difficult to determine, as you might imagine. Many tourists in big cities take photos of infrastructure – buildings, roads, tunnels and bridges. They’re not necessarily breaking the law. Usually, no crime is being committed. They may never have seen such massive structures. How do you determine those who are doing this as pre-operational surveillance versus those who are interested in great shots for their family photo albums? It’s very difficult. But officers detailing these observations, coupled with other data that are then examined by trained analysts, can lead to developing “reasonable suspicion” of criminal activity. The same could be said for the neighbor who is storing 55-gallon drums in his garage. It looks suspicious to the person offering the tip, but is it really?

In the pre-SAR days, these types of Tips and Leads would get lost in the incident reports found in RMS or CAD (Computer Aided Dispatch) systems. Such information often never made it to a terrorist, gang or drug investigative unit because it got buried in an incident report. But now with computerized SAR systems and trained analysts, the information is being shared and is being vetted by trained personnel. These

professionals are then in a position to draw informed conclusions. For example, “x” number of diesel fuel drums and “y” amount of fertilizer in a person’s garage may be used for bomb-making. The analysis can then be shared with more specialized investigators and/or higher-level officials for further investigation.

As a result of the SAR Project, LAPD and others have added check-off boxes to their RMS systems, enabling street level officers to “code in” certain observations or citizen complaints that don’t quite add up, or are more than what they appear on the surface. In the case of LA, this is the first step in developing SAR data which is then routed to, and further explored by, the analysts at the Los Angeles Joint Regional Intelligence Center.

Protecting Privacy Rights and Civil Liberties

How do civil liberties factor into police activity and SAR? For decades, police and other government agencies have documented their interactions with citizens. A secondary and often overlooked use for all of this information has been extracting suspicious activity indicators from this data.

Traditionally, police have been lawfully permitted, in fact mandated, to collect data and share such information with other law enforcement officials while being judicious about revealing details that could jeopardize a criminal investigation.

It wasn’t until the computerization of police record keeping, however, that privacy concerns among civil libertarians and privacy groups arose to a much greater extent. Law enforcement officials can now search and retrieve information much easier and faster with CAD and RMS systems supported by powerful, sophisticated software. The speed and accuracy with which police can now search repositories of information on criminals, suspects and victims, however, is disagreeable to some groups because they fear innocent people may, inadvertently or through unprofessional police practice, become objects of suspicion.

Yet as has been demonstrated time and time again in the post-9/11 world, sharing data between law enforcement officials provides the ability to detect patterns. The more information that police officers have to discern patterns of activity, the more likely they are to interdict, prevent and solve crimes that occur in their jurisdictions. From my perspective, there is nothing but positives that can come out of sharing and accessing information across jurisdictional boundaries.

Through automation, information can be searched in a way that mitigates personal bias. In some circles, police work is deemed successful because of the relationships between law enforcement officials in different areas. But officer-to-officer relationships can introduce personal biases, which can infringe on privacy rights.

The objective access to data, however – coupled with a valid, logical and competent police investigation – is the best practice for solving crimes. Investigations should never come down to personal relationships. SAR can be pursued without compromising civil liberties, and a national SAR standard will bring uniformity to these efforts.

National SAR Standard and ISE

In 2005, the ODNI was created to oversee all intelligence agencies in the U.S. The Office of the Program Manager, Information Sharing Environment (PM-ISE) also was formed. The ISE hopes to become a national network of interconnected computer systems, where SAR information can reside in repositories, allowing law enforcement agencies across jurisdictional boundaries to share and query SAR under a national standard.

The ISE joins the list of other national information-sharing programs, such as NCIC (National Criminal Information Center) for criminal histories, wanted persons, missing children, stolen cars, etc.; RISS (Regional Information Sharing Systems) for intelligence; and N-DEX (National Data Exchange) for incident-based data. Although SAR is not a subset of N-DEX, much of the data may have some cross-over.

Recommendations for Working with ISE

Having the capability of participating in, and sharing data through, the Information Sharing Environment (ISE) is something to which every law enforcement agency should aspire. Here are three suggestions:

- 1.** Deploy a SAR capability that is manageable, interoperable and compliant with ISE's SAR information sharing program. Your IT officials should ensure that your RMS/CAD technology can easily capture SAR and push the right information to ISE. The ability to move incident reports with SAR relevance into your SAR system should be transparent.
- 2.** Consider creating check-off boxes on your existing incident reports for easy transfer to your SAR system. You don't necessarily want limited analytical resources routinely looking at every incident as a SAR. This literally amounts to them looking at the entire haystack. You want them examining a "subset" that has been marked as "suspicious" and then using proven analytical methods for conducting higher level and more meaningful analysis.
- 3.** Work with a technology provider that has intelligence capabilities and is building systems to capture SAR, not just integrating RMS systems. This capability is very important today in light of discerning the terrorist pre-cursor or criminal activity from the routine criminal activity.

The rightly coded SAR in the hands of properly trained staff at well-equipped Fusion Centers and Intelligence Centers can best prevent important information from falling through the cracks. The resulting analysis can go a long way toward preventing the next terrorist plot or bank robbery.

Captain Stephen G. Serrao is a former New Jersey State Police Counterterrorism Bureau Chief, and now helps shape the direction of intelligence management software as Director of Product Management, Americas Region for Memex, Inc., a worldwide provider of intelligence management, data integration, search and analysis solutions (www.memex.com). Serrao can be reached at steve.serrao@memex.com.

Contact Us

Memex Technologies Ltd and Memex, Inc

UK and International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland
Telephone: +44 (0)1355 233804
Fax: +44 (0)1355 239676

America

Memex, Inc.
22636 Davis Drive, Suite 130
Sterling, VA 20164, USA
Telephone: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
Fax: +1 703 556 4282

Copyright ©

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of Memex.

More Information

For the latest information about our product and services, please visit

<http://www.memex.com>