

Real-time Data Sharing



What First Responders Really Need To Have

BY FRED JOHNSTON

Officer Jones was driving past the Eastwood Elementary School at around 12 PM. Recess was always around that time, and Officer Jones always made it a point, when he could, to simply drive past the school to make sure the kids were okay. A month ago, there had been an as yet unsolved abduction of a little girl from an elementary school on the other side of the county, and while his town had never experienced anything like that, he always tried to err on the safe side.

This morning, as he did his pass, he noticed an unfamiliar metallic gray Dodge pickup truck idling on the side of the street near the back fence gate where the children played. Officer Jones stopped his cruiser on the other side of the yard for a few minutes (out of sight of the truck), just to make sure the truck moved along. As recess was nearing its end, the truck still hadn't moved, so the officer decided to be on the safe side and pull up behind the truck to encourage him to move along and stop loitering.

As Officer Jones pulled up behind the truck, he flashed his lights a few times at the driver. The driver waved

cheerfully in acknowledgement to the officer, and began to pull away. Officer Jones was beginning to think he was being paranoid – that the truck had just stopped there briefly for some reason. But, again, on the safe side, he decided to run the plate through his real-time data sharing software on his mobile data computer (MDC).

As the truck began to pull away, Officer Jones input the plate number and vehicle description into his system, and within three seconds, got back some eye-opening information. While the plate/truck had never had any contact with his department, it had numerous contacts with other jurisdictions in the county. The latest of these contacts was only 20 minutes earlier, when another officer at a neighboring jurisdiction, Woodstown, had also noticed the same truck idling on a street behind a different elementary school. As Officer Jones quickly scanned down the list of other contacts, he found that the same truck had had similar seemingly innocuous contacts with at least three other jurisdictions a few weeks ago. Same truck, same MO, three different elementary schools.

Armed with this information, the officer, realizing this simple loitering truck could very well be something much more sinister, turned on his lights and siren and sped after the departing truck before it could leave. He approached the vehicle, questioned the driver – a 40-something white male – asking him if he had had any previous contacts with the police over the past few days. The driver, looking obviously nervous, lied and said he had not. During the conversation, the officer noticed a red book bag on the floor of the passenger side of the truck. He knew that reports regarding the unsolved abduction indicated that the little girl had a red book bag with her when she was taken. Based on this, the officer asked the man to exit the vehicle.

Officer Jones had just stopped a sexual predator on the prowl. The man had been thwarted earlier in the day in Woodstown, and was trying for some easier pickings in Eastwood. Most likely, this guy is also the one who abducted the little girl on the other side of the county. The frightening part is, without the ability to instantly see the prior contact with the other jurisdiction 20 min-



STÉPHANE BRUNET

Far left: A St. Johns hospital helicopter, from Springfield communicates with an engine from the Aurora fire dept. in Missouri. Data sharing between EMS units, like that of police agencies, can strengthen mutual aid operations and support public safety. Left: A police officer for the Sûreté du Québec contacts dispatch while on a call. By sharing data about crimes, suspects, and persons of interest between departments, officers are better armed with information and awareness when on even routine calls.

utes earlier, as well as the previous contact with other law enforcement groups, Officer Jones would have accepted that the seemingly innocent façade was the truth. He never would have stopped the truck, he never would have questioned the driver, and he never would have seen the red book bag. The predator had just cased the Woodstown School 20 minutes ago, had just cased the Eastwood School, and wouldn't have stopped until he got his prey. That didn't happen here, primarily because Officer Jones had access to real-time data sharing software from inside his mobile unit.

The real-time data sharing technology that Officer Jones used allows information entered locally into records management systems at linked agencies to be synched with a center-point data center and made accessible to first preventers in the field from other linked agencies within six seconds of it being entered at the local level. It is what allowed Officer Jones to run the plate in seconds, and get all the prior contacts from across the county (including the one only 20 minutes earlier) presented to him in his cruiser within six seconds of running the query.

While the above scenario is not science fiction, the unfortunate reality is that far too few jurisdictions across our country have access to such real-time cross-jurisdictional information. They rely solely on systems such as NCIC

(National Crime Information Center) and the like, or other less than real-time data sharing systems which, while valuable resources, do not reflect *all* the most current information that should be available to officers and agents in the field. Such sources are often hours, days, if not weeks behind reality, forcing field officers to rely on data that may or may not be current. Further, such high level sources are limited to actual reported crimes. So in this case, the simple police activity report (without citation) that occurred would never have been a blip on the radar. This "data-gap" is a clear and present issue facing police, and they deserve to have access to real-time information from any and all relevant sources.

Currently there is no standard for what should constitute real-time data sharing within the public safety sector. Systems that merely update data sources once an hour, a day, or even a week has become the accepted but dangerous industry norm, because many believe one of two false conclusions: (1) that real-time data-sharing is simply not possible yet; (2) that it is not necessary.

Fueling this belief is the knowledge that in public safety and homeland security agencies across the United States, there are hundreds of different vendors' systems, data warehouses, database languages, etc. All of these variables can make it difficult for agencies to easily, quickly, and securely share their data and

provide actionable information to first preventers. It is this seemingly insurmountable concoction of obstacles that has conspired to foster a general falsehood in the industry that leads to the two wrong conclusions set forth above.

Real-time in the world of data-sharing has long been thought of as a myth, something to shoot for but never really hope to achieve. In actuality, real-time data sharing is not a myth, it is a field-proven reality. Technology is now so far advanced that real time is no longer merely a buzzword without substance; it can now be clearly defined and demanded by agencies. Real time means that as data is entered at the local level, regardless of RMS vendor, *within six seconds* it is made available to other agencies' users, at the desktop and/or in the field, again regardless of what RMS vendor these disparate agencies choose to use. This is real-time data sharing and it's what first preventers and responders should have to be keenly aware of any situation they face. In the scenario above, it was the difference that stopped a sexual predator from hurting more children.

Close to 10 years ago, the need for a solution that would overcome the obstacles presented by the above variables – a solution that would enable agencies, regardless of the systems they use or what database their data resides in to share their data with each other, and provide real-time, tactically critical data

to first preventers as well as analysis to detectives/analysts – was uncovered. The solution born of that need was an integrated software suite that has provided real-time tactical data sharing to first preventers and network-wide data, mapping, COMPSTAT, and multi-tiered visual analysis to investigators since 1998.

FOUR STEPS TO REAL-TIME TACTICAL DATA SHARING:

To achieve the goal of real-time tactical data sharing, and provide the type of prevention that averted the tragedy in the scenario above, a four-step process is used. The overall theme is real-time data fusion and sharing to the edge of the public safety network – to officers and agents in the field using MDCs, handhelds, tablet PCs, smartphones, etc. Such operatives are known as first preventers due to their unique position to avert, rather than respond to a major event.

Note, to avoid confusion, when I use the term real time in this article, I mean *six seconds* – six seconds from when information is entered at the local level

to when it is available by query to first preventers from all agencies connected to the data-sharing network. Literally, from the time a user at Agency 1 enters data into his local RMS system, it **MUST** be available to users from all other connected agencies (regardless of the RMS they use) within six seconds.

Real-time translation and transmission is accomplished through an on-the-fly universal data source translator (UDST). As data is entered/updated in any connected agency RMS system, the UDST translates it into a common format and transmits the new or changed data within seconds to an insulated data silo reserved for that agency in a centrally managed server (or server farm depending upon the consortium's size). Once in the agency's silo, it is available to all users in all participating agencies. More on these phases are explained below.

TRANSLATION

The first step to data fusion and sharing is linking with pre-existing RMS systems throughout the jurisdictions within a data-sharing network and

translating data into a common language in order to transmit it in real time from each connected participating agency's record management systems (regardless of vendor) to the agency's data silo in the central data center. This is absolutely essential to any data sharing project. The ability to quickly, efficiently, and easily connect to a local vendor's RMS in place at a local agency and synch this data in real-time for first preventers is truly the lynchpin of any successful initiative.

KEEP CURRENT RMS (REGARDLESS OF VENDOR)

The key to a UDST's success in enabling real-time data sharing for a consortium of agencies is its ability to link up in real time with each agency's pre-existing local RMS using a reusable synch template for that RMS vendor's system, and translate data in real time, as it is entered into the local RMS, into a common format for synchronization to an agency's data silo on the centralized server. Within this there are two distinct but equally important elements: (1) the ability to synch with *any* RMS vendor's system; and (2) the ability to achieve this synch in *real time*. A UDST should support interoperability with NIEM/GJXDM, and provide the capability for any connected local agency to support conformance with NIEM. Further, a UDST should be able to leverage and reuse the same synch template for each instance of the same vendor's RMS system, so that the same work does not need to be done (or paid for) multiple times.

TRANSMISSION

As mentioned in the translation section above, after data is translated from a local agency's RMS, it must be transmitted to the agency's data silo in the centralized server in real time. Anything less is to be avoided in order to provide actionable information to first preventers. As data is entered or updated in an agency's local RMS database, the UDST translates it and transmits it within seconds to the agency's data silo. The system only pushes *precisely what has been changed, not the whole record and/or all related records*. Put simply, if all that was changed in a person's record stored in the agency's RMS database is the person's middle name, then that is all that is

(continued on page 40)

that gives the data-sharing system its overall real-time speed. But more importantly it allows the system to provide individual, agency-level control over every aspect of their involvement in the consortium. This "silo approach" allows for full agency control over its own data silo, as well as access thereto, to ensure that privacy, criminal history and other such concerns are met.

SHARING

The three previous stages are necessary but not sufficient without the ability for users to access the shared data anywhere they need it. A true data-sharing system must include a place where first preventers – from desktop workstations or, perhaps more importantly, in the field over laptops, MDCs, or handhelds – can query suspects' names, license plates, businesses, and vehicles, as well as any other items they can glean information from in real time. This portal should be web based, requiring zero deployment – accessible from anywhere in the field without the need to bring devices (laptops, pda, etc.) into the location to deploy or load the software. The key to this phase is that data is available at a tactical field level in real time, as it happens, in addition to a desktop location. Most first preventers operate in the field, so this is where the information needs to be.

To reinforce and bring this article back to the benefit, implementing and using a data sharing system that includes the above elements will mean that seconds after a user at Agency 1 (using RMS Vendor 1) saves data into its local database, a user in a mobile unit 100 miles away at Agency 2 (not using RMS Vendor 1) can query that data and get results back instantly thus allowing the field agent, investigator or other first preventer the ability to take the criminal, sexual predator, or would-be terrorist off the street before he can commit his planned for act. The adage goes, "an ounce of prevention is worth a pound of cure," and it certainly applies fully to the promise of public safety data sharing. ■ 9-11

Fred Johnston is the director of business development for CODY Systems and a former law-enforcement agent with over 10 years experience as a lieutenant in patrol/investigation/LA and jail management in Colorado. see: www.codysystems.com

DATA SHARING

Continued from page 18

transmitted.

STORAGE

The centralized server works with the universal data source translator enabling all disparate databases to be virtually integrated. With this centralized server, each agency has its own insulated data silo to ensure that no agency's data is ever comingled with any others'. All agencies' data silos and business rules for sharing are stored in the centralized environment (server, data center, blade cluster, etc.).

NOTE: Maintaining absolute segregation of one agency's synched data from all others in the central environment is the lynchpin