

Criminal Activity Patterns

Intelligence

Author:

Stephen G Serrao

Date

December 2009

Changing the Game: The DNA for Detecting Criminal Activity Patterns

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

Over the last two decades, one of the most significant developments in solving specific violent and sexual crimes has been the wide-ranging collection and testing of DNA evidence. Where once investigators were hamstrung by more primitive forms of physical evidence and less-than-reliable eyewitness accounts, today DNA evidence provides a more scientific and verifiable means of linking specific perpetrators to the victims they have committed their crimes against.

Of course, there have always been concerns about whether the use of DNA evidence by law enforcement violates suspects' rights. But in practice, it has actually proven invaluable in confirming the innocence of the wrongly accused. The newspapers regularly run accounts of inmates being released from prison years after their convictions, which may have been based on faulty eyewitness accounts, the inability to establish a credible alibi and even the subjective points of view of law enforcement officials. In short, DNA testing is a benefit to protecting the liberty of the innocent while sealing the fate of the guilty.

Today, a different, new technology is providing similar benefits to law enforcement – and meeting with similar resistance. Only this time, instead of involving hair and bodily fluid samples gathered from the scene of the crime, this new technology is centered around data-, information- and intelligence-sharing between agencies and jurisdictions.

The computerization of longstanding paper-based record systems has been a game-changer for law enforcement entities at all levels. Where once the information police had access to about a specific person was limited to what was contained in their filing cabinets – and what they could find within them – investigators now have the ability to draw upon the combined records of every department and agency that is willing to share what they know.

One benefit has been learning more about a suspect or person of interest before he/she is taken into custody. For example, by checking the combined agency CAD (Computer-Aided Dispatch) and RMS (Records Management System) records, an officer may discover that a man suspected of DUI in Arizona may also be a suspect in a hit-and-run in South Dakota. The real value of access to large volumes of data, however, is in the ability to conduct analysis and detect patterns of criminal activity.

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 multiple jurisdictions. These are all positives that result from sharing and accessing information across jurisdictional boundaries.

The FBI's new National Data Exchange (N-DEX) criminal justice information-sharing program is facilitating this detection by enabling police jurisdictions across the country to share incident-based data with each other – information to which they would normally not have automated access.

Data and information-sharing have not been met with universal acclaim, however. Privacy and civil rights groups want to place limits on how much of this data police are saving, storing and searching. They worry that access to the data will be abused, with the result that “suspects” are made of innocent people.

There is certainly validity and precedent to those concerns. Yet the fact is privacy rights and the civil liberties of individuals are much less likely to be violated when information is automated as it is in these new information-sharing systems.

One of the key reasons why automated systems can protect civil liberties is that they can be set up to search in a way that mitigates the personal bias of the person performing the search. Rather than relying on a personal relationship with a counterpart in another jurisdiction as to who or what to look at, an officer using an automated search is looking for objective data and facts. When those are coupled with a valid, logical and competent police investigation, the human element is removed, and the result is the best practice for solving crimes.

It's no different, really, than replacing eyewitness accounts (or an informant's tip) with DNA evidence. Speculation and opinion are replaced with hard, verifiable facts – a methodology that is far more likely to return more accurate results.

Another thing to keep in mind, especially when working within the homeland security environment, is that it can take years for embedded operatives to be activated and for patterns of suspicious activity to appear. That is the whole purpose terrorist groups use so-called sleeper cells – to hide in plain sight among us until the time is right to commit the act of terror. This means careful consideration should be given to placing limits on how long data can be retained. Critical information that could help prevent catastrophic loss of life and/or destruction of property may not be available when it's needed most if data is purged from automated systems too frequently.

There will always be those among us who believe that anything that intrudes upon an individual's right to privacy is unacceptable. Yet that view must be tempered by the realities of the goals for a “free” society.

Improved data and information-sharing help safeguard society as a whole from threats by allowing law enforcement to rely on empirical facts rather than opinion or relationships, and by providing a bigger picture view than any individual department or government agency can attain by itself. With proper controls in place to make sure information sharing doesn't become “tainted,” it is poised to do for informational evidence what DNA testing has done for physical evidence.

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>