

Detection and Protecting Civil Liberties

Intelligence

Author: Stephen G Serrao
Date December 2009

Detection and Protecting Civil Liberties

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

For decades, police and other government agencies have documented their interactions with citizens – whether they take the form of helping a stranded motorist, offering first aid or responding to a crime – as a matter of procedure. Historically, this documentation was performed on paper. The main purpose of this record-keeping was just that, record-keeping. A secondary and often overlooked use for all of this information has been to detect and identify aberrant behavior or anomalies that may support planned or ongoing criminal activity.

Traditionally, police have been lawfully permitted 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 (Computer Aided Dispatch) systems and RMS (Record Management Systems) 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, information sharing 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.

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 access.

In other words, the proactive detection of criminal activity is achievable by using sophisticated software searching for the proverbial needle in the information haystack. Law enforcement now has a "big magnet" which can literally pull that needle right out of the haystack.

Privacy and civil rights groups, for their part, want to restrict and control how much of that data police are saving, storing and searching because they fear overzealous officers, investigators and the FBI will abuse this access and make suspects of innocent people.

But the privacy rights and civil liberties of individuals are much less likely to be violated with the automation of information. Here's why.

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.

There are systems in place all over private industry that make evaluations and judgments based on objective examination of personal data (e.g. credit reporting bureaus), and that should be the standard police practice, too. The data speaks for itself. With automation, proper training and other safeguards in place, fewer abuses will occur.

In all of this, law enforcement officials have never suggested that information should be shared outside of the law enforcement community with private entities, or in violation of any existing privacy statutes.

That's where abuses can be introduced because of the profit motive. The only exception would be the limited sharing of critical information with private organizations responsible for safeguarding infrastructure, such as tunnels or buildings – and only when the standard of reasonable suspicion of criminal activity has been met.

The detection of crime and the protection of civil liberties need not be in conflict. The automation of law enforcement record-keeping and use of sophisticated technology will help police organizations prevent crimes while respecting individual rights.

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>