Current Issue
Archives Past Issues
Web-Only Articles
About Police Chief
Advertising
Editorial
Subscribe / Renew / Update
Law Enforcement Jobs
Buyers' Guide

Back to Archives | Back to June 2007 Contents

send to a friend
printer-friendly

Civil Rights and Law Enforcement Intelligence

By David L. Carter, Professor of Criminal Justice, Michigan State University, East Lansing, Michigan; and Thomas J. Martinelli, Adjunct Professor, Wayne State University, Detroit, Michigan

Since the terrorist attacks of September 11, 2001, many state, local, and tribal law enforcement agencies have reestablished and reengineered their intelligence capacity largely through guidance provided by the National Criminal Intelligence Sharing Plan, the Law Enforcement Intelligence Unit file guidelines, and various intelligence training programs developed under the sponsorship of the Bureau of Justice Assistance[1] and the Department of Homeland Security Office of Grants and Training.[2] While all of these intelligence programs include instruction on the constitutional guidelines regarding civil rights protections, new challenges are emerging that pose renewed concerns about past abuses.

In particular, there is increasing concern about the Information Sharing Environment,[3] the product of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Based largely on the recommendations of the *9/11 Commission Report*,[4] this legislation is designed to maximize information sharing among all levels of government, including the sharing of terrorism information between the intelligence community and state, local, and tribal law enforcement agencies. The reason, of course, was to ensure that U.S. law enforcement agencies would have the information and the ability to detect an emerging terrorist threat in time to stop it. Although the goal of protecting the United States from terrorism is a noble one, critics of the legislation felt it went too far.

Learning from History

Some previous law enforcement intelligence activities have been criticized for trespassing on citizens' rights. Critics of law enforcement intelligence cite the history of police organizations collecting and retaining information on citizens based on their affiliations, beliefs, pronouncements, and other noncriminal attributes. As evidenced by a myriad of previous lawsuits, these abuses did occur in the past.[5] Unfortunately, today's critics do not recognize the many changes that have occurred in law enforcement practices or the professional nature of law enforcement intelligence. Higher educational standards, better training, adoption of ethical standards, and inculcation of law enforcement as a profession all indicate that the culture of law enforcement has changed, rejecting

past practices that contributed to abuses of intelligence activities.

Information collected and retained in a criminal-intelligence records system must demonstrate a relationship between the person identified in criminal-intelligence records and criminal behavior.

Beyond this history, it should be recognized that the public has a general misconception about the function of law enforcement intelligence; they envision it as involving spying, surreptitious activities, and acquisition of information by stealth. The public, including the media, needs to be reassured that law enforcement intelligence processes will strictly observe individual constitutional protections when collecting and retaining information. Moreover, the public should understand that intelligence analysis is simply the scientific approach to problem solving, similar to the way it has been effectively used in community policing. The difference, however, is that community policing focuses on crime and community disorder, whereas intelligence focuses on methods that may be used to prevent criminal threats from reaching fruition. Generally speaking, critics do not disapprove of using intelligence gathering and analysis to combat terrorism or solve crimes; rather, they demand simply that it be conducted in accordance with the constitutional parameters law enforcement officers are duty-bound to follow.

Commenting on the opening of the Massachusetts intelligence fusion center,[6] the American Civil Liberties Union (ACLU) of Massachusetts issued a press release with concerns that illustrate the need for public education on law enforcement intelligence gathering, expressing concern about the center's role and activities: "We need a lot more information about what precisely the fusion center will do, what information they will be collecting, who will have access to the information, and what safeguards will be put in place to prevent abuse."[7]

The concerns outlined by the Massachusetts ACLU are easily answerable. By simply providing this information to the community, through a public information document or in town hall presentations, a great deal of conflict, criticism, and cynicism can be avoided. Fear of the unknown generates citizen consternation, which translates into mistrust and allegations of abuse of authority. Clear, well-drafted civil rights protection policies pertaining to intelligence operations should be mandatory for agencies of any size that engage in intelligence gathering.

Focal Points of Concern

In addressing these civil-rights issues, three primary areas of concern emerge:

- The information in a criminal-intelligence records system must be collected and retained in a proper manner, both legally and ethically.
- Individual privacy rights must be protected for all information that has been collected and retained.
- The integrity of data quality and data security must be

ensured.

Although there are additional intelligence issues that have civil-rights implications, these three are among the most fundamental and challenging.[8]

Proper collection and retention of information in a criminal-intelligence records system: The authority of state, local, and tribal law enforcement agencies to participate in any type of intelligence operations lies in their statutory authority to enforce criminal law. As such, any information collected and retained in a criminal-intelligence records system must be based on a criminal predicate. That is, a relationship must be demonstrated between individuals identified in criminalintelligence records and criminal behavior. The level of that relationship is more than mere suspicion; reasonable grounds must be articulated to link suspected individuals to specific criminal behavior.

Protection of privacy for all collected and retained information: Ensuring that information about individuals is collected and retained with a proper legal basis constitutes one form of civil-rights protection. Formulating an explicit privacy policy helps to achieve this goal. A privacy policy is a published statement that articulates the policy position of an organization on how it handles the identifying personal information it gathers and uses in the normal course of business.[9] Law enforcement agencies must have mechanisms in place—including proper training, policies, procedures, supervision, and discipline—to make certain that identifying information is not disseminated to anyone who does not have the right or the need to access it. A privacy policy ensures the implementation of proper safeguards as long as the policy incorporates a clearly defined process of discipline, demonstrating strict, swift, and certain sanctions for any sworn department members who fail to strictly comply with the policy's provisions.

Ensuring the integrity of data quality and data security: Preserving the quality of data involves procedural mechanisms to ensure that raw information is collected and recorded in a valid, reliable, and objective manner. Ensuring data quality means maximizing the accuracy of raw information used in the intelligence records system. Preserving the security of data requires processes and mechanisms to ensure that individuals cannot access a given piece of information who do not have the lawful right and need to do so. Security measures reinforce the procedural processes of individual privacy protections without divulging the substance of the intelligence gathered. Giving procedure priority over substance is a broad policy philosophy that can be shared with the community to quell mistrust, without jeopardizing an agency's efforts to protect the quality of data retrieved.

Steps to Ensure the Protection of Citizens' Civil Rights

Several mechanisms may be implemented to address the concerns of intelligence critics and ensure that civil-rights protections remain intact. By taking the following steps, an agency assures the public that it has made a reasonable effort to comply with the latest Supreme Court rulings pertaining to best police practices in accordance with the increased need for police vigilance in the post–September 11 era.

Step One—Policy: Every law enforcement agency should implement a privacy policy, a security policy, and an accepted-records management policy, such as those found in the Law Enforcement Intelligence Unit file guidelines.[10] Relying on policy

models and policy development processes recommended by the Global Intelligence Working Group has a twofold advantage. First, it demonstrates to the community that the law enforcement agency has an intelligence policy foundation consistent with nationally recognized standards. Second, in the case of a lawsuit, following such recommendations can be used as an affirmative defense that the agency's policies are consistent with professionally recognized good practices.

Step Two—Training: Training has three fundamental levels. First, every agency should follow the recommendations of the National Criminal Intelligence Sharing Plan, which include an intelligence awareness training program for all officers.[11] Second, beyond these training standards, appropriate personnel within an agency should receive training on agency policy and fusion center policy related to all aspects of the intelligence function. Special attention should be devoted to collection, retention, and dissemination of intelligence as well as special issues such as suspicious-activity reports, intelligence related to juveniles, and other unique forms of information. Finally, sworn personnel must appreciate the gravity of constitutional-rights violations resulting from improper intelligence gathering. Not unlike other critical issues in policing, a "zero-tolerance policy" toward such infractions is mandatory. Such a policy demonstrates to law enforcement personnel as well as the community that an agency takes civil-rights violations very seriously and will take immediate disciplinary action against violators.

Step Three—Supervision: Good policy and training are only part of the equation—an agency must also ensure compliance with policies and procedures as intended. When systemic accountability and uniformity in meting out appropriate discipline are lacking, officers can misinterpret or otherwise fail to follow policy. Street-level supervisors must be vigilant in supporting their agency's commitment to constitutional policing and must hold their subordinates to the highest standards of the profession, especially when dealing with intelligence gathering. When investigators uncover patterns and practices of civil-rights violations over a period of time, plaintiffs' attorneys simply have to demonstrate to juries that street-level supervisors, as well as their supervisors, knew or should have known of these violations and deliberately chose not to take disciplinary action. Deliberate indifference has proven to be very costly for law enforcement agencies that have opted to look the other way when citizens, or officers, have reported possible civil-rights violations.[12]

Step Four—Public Education: A critical element of successful law enforcement intelligence is informing the public of law enforcement intelligence initiatives. There are two critical reasons for doing so. The first, as noted earlier regarding the ACLU's concerns, is simply to educate the public about the intelligence process. This helps to eliminate false assumptions and second-guessing. Much of the lay public assumes that law enforcement agencies perform some type of widespread clandestine information collection and operate in a manner similar to the national intelligence community. Correcting this misperception can go a long way toward developing positive support for the law enforcement intelligence process.

The second benefit to public education is to inform citizens of the signs and symbols of terrorism so that they can assist in the information collection process. For example, the Regional Community Policing Institute at Wichita State University, Wichita, Kansas, conducted a trial program in association with various Kansas police departments, providing community training on what to look for and how to report information regarding possible terrorist threats. Those attending the training were provided with a document

called “Observe—Document—Report,” describing how to recognize suspicious behavior, what to document, and how to report observations to law enforcement. This model also helps citizens feel that they can contribute to the security of their own community and helps minimize the level of distrust toward agencies’ efforts to combat crime and terrorism.

Step Five—Transparent Processes: The processes of the intelligence function, like all other aspects of a U.S. law enforcement agency, should be clearly understood and transparent. Whereas certain information used for intelligence purposes must be secured, the process by which that information is used must be open. Critics of law enforcement intelligence argue that the intelligence process is too secretive and that agencies have committed widespread spying on citizens.[13] Agencies can counter this argument successfully by being open and transparent about the inner workings of their intelligence processes, including their relationships with other organizations, such as fusion centers. Without divulging the substance of intelligence records, such efforts can help citizens to appreciate and support intelligence gathering.

Step Six—Accountability Audits: Periodic internal audits of intelligence processes should be mandatory within any agency. It is helpful to follow a two-step process. First, a supervisor or manager reviews and documents intelligence processes following a recognized checklist of variables and writes an inspection report.[14] After the completion of this report, an external auditor—a balanced, independent party such as a retired judge or other respected individual—reviews the report and asks challenging questions of both the author of the report and the agency’s chief executive. It is important that the agency view the audit as a positive process designed to identify rectifiable weaknesses. An audit can proactively ensure that all aspects of the process are operating as constitutionally mandated. It can identify unforeseen problems and serve as affirmative evidence that the agency is operating in good faith and without malice.

Step Seven—Assistance of Legal Counsel: Case law, as it pertains to police misconduct, relies on police best-practice concepts such as good faith, reasonableness, and discretion without malice when judging an officer’s conduct in hindsight. Juries typically prefer not to find officers guilty for their alleged misdeeds or policy violations and, more times than not, will give the officers the benefit of the doubt. But without clearly drafted policies, in-depth training scenarios, and evidence of an organization’s strict compliance with constitutional law issues, an agency’s legal counsel may find it difficult to defend against allegations of civil-rights violations in a court of law.

Competent legal counsel may be the best preventive measure agencies can take to avoid litigation involving allegations of civil-rights violations. Whether a sole practitioner or the department insurance carrier’s legal counsel, an attorney well versed in municipal law, Section 1983 actions,[15] and police misconduct cases can assist with the drafting of the agency’s privacy and security policies as well as the formulation of the processes for intelligence gathering and analysis.

The Future

In the evolving world of law enforcement intelligence, driven increasingly by fusion centers and the information sharing environment, law enforcement executives face new challenges in managing sensitive information and intelligence. As intelligence

gathering becomes standard practice for agencies at all levels, the practice will draw greater scrutiny from civil-rights activists to ensure that information is collected, retained, and disseminated by law enforcement agencies in a lawful and ethical manner. Professional law enforcement has both the knowledge and the tools to accept the responsibility of preserving citizens' civil rights while protecting the community. Ensuring that law enforcement intelligence processes and tools are transparent and accounted for places them in the proper perspective for the future protection of civil rights.■

David L. Carter, Ph.D., is a professor of criminal justice at Michigan State University (MSU) and the director of the MSU Intelligence Program. Dr. Carter manages several intelligence training grants from the Department of Homeland Security, is a member of the Department of Justice Intelligence Training Coordination Working Group, and is the author of the Community Oriented Policing Services (COPS)–funded book Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*.*

Thomas J. Martinelli, J.D., M.S., is an adjunct professor at Wayne State University and an attorney who researches and writes about police misconduct issues. Mr. Martinelli trains police agencies in ethics and liability issues and is a member of the IACP's Police Image and Ethics Committee.

Notes:

[1]Programs include the Criminal Intelligence for the Chief Executive (CICE) course, the State and Local Anti-Terrorism Training (SLATT) program, and the Criminal Intelligence Commanders course that is in preparation as of this writing. See the SLATT program Web site (slatt.org) for details.

[2]Most notable among these programs is the Intelligence Toolbox Training Program. See the program's Web site (intellprogram.msu.edu) for details.

[3]See "Program Manager, Information Sharing Environment," http://www.ise.gov .

[4]National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004).

[5]See Frank J. Donner, *Protectors of Privilege: Red Squads and Police Repression in Urban America* (Berkeley and Los Angeles: University of California Press, 1990).

[6]For more information on fusion centers, see Peter A. Modafferi and Kenneth A. Bouche, eds., "Efforts to Develop Fusion Center Intelligence Standards," *The Police Chief* 72 (February 2005): 47–53.

[7]American Civil Liberties Union, "ACLU of Massachusetts Questions Scope of Fusion Center Activities," press release, Boston, Massachusetts, May 11, 2005, http://www.aclum.org/news/05.11.05.Fusion.pdf, April 26, 2007.

[8]It should be noted that these issues concern only information and records that identify individuals. Aggregate information that describes trends, collective behaviors, philosophies, methodologies, or other information that is useful for the intelligence process but does not identify individuals is not afforded the same privacy protections. The Bill of Rights was added to the U.S. Constitution to protect individual citizens' rights, not intangible group rights such as methodologies or trends.

[9]Global Justice Information Sharing Initiative, *Privacy Policy Development Guide and Information Templates* (Washington, D.C.: Office of Justice Programs, U.S. Department of Justice, n.d.), 4-1.

[10]Law Enforcement Intelligence Unit, *Criminal Intelligence File Guidelines* (n.p., March 2002), http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf, April 23, 2007.

[11]Intelligence training resources can be found at the following Web sites: http://slatt.org, http://www.counterterrorismtraining.gov, and http://intellprogram.msu.edu.

[12]Thomas J. Martinelli and Joycelyn M. Pollock, "Law Enforcement Ethics, Lawsuits, and Liability: Defusing Deliberate Indifference," *The Police Chief* 67 (October 2000): 52–57.

[13]As an illustration, the reader is encouraged to conduct an Internet search of the phrase *spy files*; the results will provide insight on the breadth of concern about the intelligence process as well as the issues of concern for many citizens.

[14]Two examples of intelligence audit checklists can be found in the appendices of David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (n.p.: U.S. Department of Justice, Office of Community Oriented Policing Services, November 2004), intellprogram.msu.edu/Carter_Intelligence_Guide.pdf, April 23, 2007, and Law Enforcement Intelligence Unit, *Audit Checklist for the Criminal Intelligence Function* (n.p., September 2004), http://it.ojp.gov/documents/LEIU_audit_checklist.pdf, April 23, 2007.

[15]*Civil Rights Act of 1871*, 42 *U.S.C.* 1983 (1996).

Top