

---

# Law Enforcement Technology 2015

**Charles “Sid” Heal, Thomas Cowper  
Andreas Olligschlaeger**

## Introduction

On January 28, 2001, the Tampa Police Department used a little-known technology called biometric facial recognition to scan the faces of 71,921 fans attending Super Bowl XXXV for known criminals and terrorists.

On November 14, 2002, the New York Times published an article by William Safire entitled “You Are a Suspect,” accusing the Department of Defense of creating “computer dossiers on 300 million Americans,” an “Orwellian scenario” leading to a police state that would be created by an advanced data mining project called Total Information Awareness.

On Wednesday, October 21, 2004, a young woman in a crowd of some 60,000-80,000 baseball fans celebrating the historic victory of the Red Sox over the Yankees was killed by a pepper-dispensing projectile fired from the less-lethal weapon of a Boston police officer.

On Thursday, February 4, 2005, after spending \$170 million, lawmakers in Congress criticized the FBI for continuing problems associated with its Virtual Case File system to manage criminal and terrorist investigations, and their inability to determine when or if the system would become fully operational.

Technology and law enforcement have always been a complicated and controversial mixture

of crime fighting strategies, labor-management relations, agency budget battles, social policy, Constitutional law and politics. From the adoption of fingerprint identification and the establishment of forensic crime laboratories in the early 20th Century to the use of 2-way radios, radar and laser guns and Plymouth Roadrunners in its latter half, the use of technology by police has been fraught with problems that span the breadth and depth of the law enforcement realm. While there have been many successful implementations throughout the last century, more often than not new technology initiatives, big and small, have fallen far short of expectations, both of the police who use them and the public upon which they are used.

21st Century technology is going to further exacerbate this enduring trend over the next ten years. There are more technology options for law enforcement today than at any time in history and these technologies and their associated systems are more sophisticated, intricate and powerful than ever before. Every new technological breakthrough with application to law enforcement, or of use by criminals and terrorists, brings with it new and unique difficulties and dilemmas for the police and their communities. Every new system or network intended to improve policing can also bring with it unwelcome financial hardship, organizational transformation and public scrutiny to agencies that may not be prepared for them.

Technology is a multi-edged sword that will cut in many directions. Its use for law enforcement and homeland security in the coming years is essential if we are to provide for the safety of our cities and neighborhoods, but used unwisely by government it could have an adverse impact on civil liberties and social stability. Technology will be used by criminals and terrorists, giving them more opportunities for crime, more tools to use against the innocent, and a greater ability to avoid apprehension.

---

And as it permeates more of our world and we become more dependent upon its networks and systems, technology makes us more vulnerable to the severe social and economic disruptions that can be caused by individual criminal and terrorist acts, making the job of stopping those acts an essential component of maintaining both security and liberty.

To accomplish this goal—providing both security and liberty—as we continue the march toward 2015 will not be easy. Dealing with ongoing and longstanding police challenges, adopting new technologies, modifying operational processes to cope with new threats and adapting to a rapidly changing world will severely tax the capabilities of law enforcement agencies and law enforcement officers alike. This article examines a few of the benefits, capabilities, problems and implications of just some of the technologies, systems and networks that will confront and confound the law enforcement profession over the next decade.


## **Coming Out of the Dark Ages**

Like many government agencies, law enforcement has traditionally been slow to adopt new technologies. This is especially the case for information technology. By the early 1990s most law enforcement agencies were still at the level of late 1970s/early 1980s technology. The COPS MORE program in the early to mid 1990s is one example of several programs that provided a much-needed catalyst to law enforcement. It gave those agencies that chose to do so an opportunity to invest in advanced information technology. At the same time the National Institute of Justice was providing grant funding for research into ways in which computer technology could be used to go beyond simple data entry and retrieval. The Drug Market Analysis Program (DMAP), for example, sparked an interest in crime mapping and was one of the main factors

leading to the establishment of the NIJ's Crime Mapping Research Center, recently renamed MAPS, as well as the now almost universal adoption of crime mapping.

By early 2000, law enforcement was beginning to emerge from the Dark Ages but the events of 9/11 only served to emphasize the fact that law enforcement information technology was still inadequate to the task. For the most part, police agencies across the country were in possession of the bits and pieces of information that in hindsight might have prevented the attacks, but the policies, procedures and technologies were not in place that would have allowed analysts to see the big picture. Today, five years after 9/11, law enforcement is not much further ahead in its ability to “connect the dots” than it was in 2000. Many efforts are underway to standardize law enforcement information (Embley, 2002), provide the infrastructure for widespread sharing of information, enact legislation to permit information sharing, and warehouse data and deploy technologies such as data mining, link analysis and other analytical techniques. Nevertheless, we are realistically still a number of years away from seeing them implemented and coordinated on a national scale.

It is critical that as we proceed into the next decade law enforcement have timely access to modern information technology. Our recent history waging the war on terror has clearly shown that the failure to do so can have serious consequences. Over the next ten years, digital chips and wireless networks will turn more and more previously standalone technologies into information technology nodes, exponentially increasing the amount of information with significance to law enforcement. By 2015 virtually all technology will be information technology. Yet in spite of these emerging changes and our recent efforts to improve, we continue to see well-publicized and well-documented information



technology failures such as Total Information Awareness (TIA), the FBI's Trilogy and Virtual Case File projects, the large-scale abandonment of the MATRIX program and numerous others. The opportunity to avoid similar failures in the future and bring law enforcement out of technology's dark ages is largely dependent upon how we deal with the following issues.

## **The Government Technology Lifecycle**

The first thing police officers and police managers need to understand is that technology in general—and information technology in particular—is evolving at an accelerating rate of change. What this means is that the interval between significant technology innovations is decreasing over time. Private industry, the military and even consumers have been adapting to this accelerated change by replacing or upgrading more often than they did even five years ago. For private industry, this is necessary to avoid falling behind the competition; for the military, it is imperative for victory on the battlefield. Civilian government, on the other hand, has not discovered a mechanism to adequately streamline its processes and overcome the centralized bureaucratic hurdles to timely technology procurements. While private industry has been replacing or upgrading technology every 2-4 years, and the military pursues an ongoing multibillion dollar “transformation” program, the procurement lifecycle in civilian government remains extremely slow. Accelerating change will create an even wider technology gap for civilian law enforcement unless something is done to shorten the government technology lifecycle.

### ***Funding***

While the technology lifecycle for

government remains inadequate for a changing world, many, if not most law enforcement agencies still lack the funding to keep up with technology. Few agencies have enough money in their budget to allow for continuous upgrades and maintenance of computer systems. Typically they are dependent on grant funding to upgrade computer systems. Indeed, in the past it has been federal funding, such as COPS MORE, or state block grants that has been the primary catalyst for technology adoption at the state and local level. When funding becomes available agencies upgrade, but the array of need usually outstrips the available money. Federal funding is often diverted away from information technology projects to procure other (and also much needed) items such as less lethal weapons, bulletproof vests, vehicles and radios. The problem with this is that agencies pit one technology procurement against another, they remain stagnant or fall behind in their ability to process an ever increasing amount of information, and in the long run keeping up with technology becomes more expensive, disjointed and inefficient. For example, if a police department has to wait five years until they can upgrade to a new version of a particular piece of software they will often find that in order to be able to upgrade they will also have to purchase new hardware. In turn this might result in the need for a complete overhaul of a department's computer systems, which is not only an expensive proposition but might make it impossible for the department to upgrade because funding is only available for the software.

### ***Leadership***

Technology today is an integral part of any successful police agency and as such the impact of leadership upon technology procurement, policies and programs is critical. As we approach 2015, the overall law enforcement effort will be hampered by police leaders who do not understand technology and accelerating change, who do not appreciate

---

the advantages that well managed information technology systems can bring their agency, and who continue to focus resources on Industrial Age methodologies based upon traditional cultural attitudes toward information and information-sharing. There are many examples today of large, medium and small police departments that stand out from the norm and do have access to state of the art information systems. In almost all cases the main reason those departments have been successful is strong leadership, either within the department via the Chief of Police or other high ranking official, or externally via a city administrator or IT department head. By contrast, many police chiefs view information technology as less important than other pressing issues. They do not value the contribution information technology can make because they are simply not aware of what modern information systems can do when implemented correctly.

## **Marketing New Technology**

It is fair to say that most governments have never been very adept at marketing new ideas. This is especially true for law enforcement. A good example of this was the Total Information Awareness (TIA) project, an information technology research and development program designed to improve law enforcement's capacity to handle the rapidly increasing amount of information in our world and make rational decisions based upon it. The goal of TIA was to develop information technology that is desperately needed by law enforcement in order to prevent future terrorist attacks. Yet there was little public dialogue about what the project was hoping to achieve, nor were there sufficient guarantees that the project would not unduly violate the public's right to privacy. In the end the project died from lack of a true understanding of the technology, its capabilities and

its purposes, as well as the public's concern about Big Brother.

The same fate awaits the next generation of information technology for law enforcement unless police leaders can effectively educate policy makers, the media and the public as to why IT is critically important to preserving, and not infringing upon, civil liberties.

## ***Disconnect between IT and Law Enforcement Practitioners***

One issue that has historically hampered the development of law enforcement information technology is the fact that information technology and law enforcement practitioners tend to have difficulties communicating ideas to each other. Because neither side understands the other's work, many efforts to implement information systems have failed. For example, law enforcement administrators often severely restrict the functionality of information systems by needlessly limiting access to information. Conversely IT practitioners have been known to limit system functionality by needlessly locking down certain functions for ease of maintenance.

## ***Mega Projects vs. Living Systems***

While private industry certainly has had its share of failures, government agencies seem to have more problems succeeding with the implementation of large technology projects. Due to the details and complexities associated with large technology projects it is easy for law enforcement agencies to lose focus and become overwhelmed, primarily because they lack in-house expertise to guide the project. More often than not, the result has been millions of wasted taxpayer dollars and little or no advancement in the police use of information technology. The problem is that ideally, a law enforcement information system should never be

---

“finished.” Rather, it should be an ongoing project, a “living system” that evolves over time. Creating a new mega project from scratch every 5-10 years is not only counterproductive, but also inefficient in terms of cost and increased agency turmoil. In the long run it is much cheaper and operationally more effective to create a living system that continuously scales and expands through the upgrade of components and software as new technology becomes available.

### **New Technologies: On the drawing board today, on the street tomorrow**

Law enforcement will continue to face many technology related challenges over the next ten years, not only with respect to obtaining and maintaining new technologies, but also in terms of implementing policies and procedures that will allow the free exchange and processing of information without unduly violating the public’s constitutional rights and privacy. While there is no guarantee that information technology will, for example, prevent another terrorist attack, the failure to implement it will almost certainly result in another missed opportunity to prevent attacks on U.S. soil, should such an attempt be made. It is therefore inevitable that we will see an increasing use of other advanced technologies, by state and local law enforcement many of which are currently only available or affordable to federal agencies, the military and large corporations.

**UAVs.** Unmanned aerial vehicles (UAVs) will undoubtedly begin to augment conventional police helicopters as law enforcement eyes in the sky, especially at crime scenes. UAVs being tested for police use today are light weight and can be set up, deployed and controlled by one or two officers in a relatively short time. By 2015 ultra-light UAVs of many different types and will be able to deploy

directly from patrol cars and function autonomously, providing digital information for surveillance, pursuits, traffic enforcement, tactical operations and any other law enforcement mission that benefits from aerial observation.

Running on a combination of battery and solar power, these UAVs will be equipped with small electric motors, wireless cameras, sensors, devices, and GPS locators. They will be capable of loitering in one location at a preset altitude for hours or following a programmed route while sending real-time data to both officers on the ground and incident commanders. And unlike helicopters, these UAVs will be nearly invisible while in the air, have almost no noticeable noise signature from the ground and will be very inexpensive to purchase and operate, making them widely available for law enforcement operations.

**Robotics.** Robots will also begin to proliferate over the next ten years. Dozens of different models of robots are available today suitable for a variety of purposes and in the near future the numbers and types of robots available for law enforcement will multiply. Market estimates predict that within a few years millions of robots will be operating in our world. Under development today are small snake-like robots for operation in pipes and confined spaces and robots that climb walls using technology that mimics the biological capability of the gecko lizard. Police robots have been confined to the larger wheeled and tracked types that are equipped with cameras, robotic arms and shotguns but in the future these platforms will be used for many different missions such as area and perimeter security, surveillance, search and rescue and hauling equipment.

But perhaps the biggest innovation to hit the UAV and robot market will be their increasing autonomy and ability to coordinate with each other to perform tasks as a group or “swarm”. A



---

major technology initiative of the U.S. military, the autonomous operation of UAVs and robots will be commonplace by 2015 adding to their usefulness and freeing up police officers otherwise tasked with their operation or close supervision. For example, a police officer on patrol might have an assigned UAV and robot equipped with video cameras, microphones and sensors that could perform many different tasks to enhance that officer's performance. They might be affixed to the patrol car when not needed or continuously roam the area around the officer providing important information that would increase the officer's situational awareness. In a pursuit situation the UAV might launch and track the fleeing vehicle or person allowing the officer to follow from a distance at a safer speed. The robot might simultaneously perform other tasks to aid the pursuit such as helping to alert traffic at approaching intersections or following the suspect into areas where the UAV cannot follow, such as tunnels or buildings. The officer, robot and UAV would form a coordinated team working together to accomplish their assigned mission, adjusting and adapting as the situation demands.

**Biometrics.** One of the biggest problems confronting law enforcement today is the ability to positively determine a person's identity, especially in relation to the on-going wars on crime and terrorism. In 2015, biometrics will have advanced to the point that personal identification will be highly accurate and near instantaneous. Biometric identification systems use a person's unique physiological or behavioral characteristics to determine their identity, matching for instance, a real-time scan of a person's features with a digital record of those features previously scanned and stored in a database. Commonly scanned characteristics are fingerprints, retinas, facial features, speech patterns and hand geometry but there are numerous other unique identifiers that may be used.

Being adopted today in many commercial settings some retailers in high-security environments, including the banking industry, and biometrics systems of 2015 will be multimodal, using several different biometrics at the same time to increase accuracy. The days of signing checks and credit card receipts or remembering Personal Identification Numbers (PIN) will have long passed and it is likely that within ten years the courts and other government agencies could begin requiring biometric identification in place of signatures on driver's licenses, bail bonds, passports and the like. While the courts will certainly limit the extent to which they can be used, by 2015 the technologies may be ubiquitous in the private sector, thus mitigating the privacy controversies we experience today. Indeed, the growing problems of identity theft and fraud coupled with their ease of use and the protections afforded by biometric identification could mandate its widespread use.

**Electronic Monitoring.** Perhaps equally important to the identification of individuals is the ability to monitor and track their movement when necessary. By 2015 this will be easily accomplished using various attachable and implantable devices placed on suspects, convicted criminals and other objects of interest such as personal property and evidence. Many of these technologies are already on the market such as "EZ-Pass" transponders for toll-road access, cell phones for E-911 location and On-Star devices in new cars. Others are under development. The Radio Frequency Identification (RFID) chips and GPS receivers that make this location and tracking possible will proliferate in the coming years as they become smaller and cheaper to manufacture. There are currently implantable RFID chips for humans, and several companies are working on implantable GPS receivers that will eliminate the need for an externally worn device. By 2015 these technologies will be commonplace within

---

our environment and will work together to enable tracking of anyone and anything.

For example, this technology will allow for secure “home detention” of suspects or non-violent convicted criminals. A suspect may be permanently assigned to a home, restricted to certain neighborhoods or communities, or allowed to travel to and from work along specific routes and at specific times of day. If a suspect diverts beyond the prescribed parameters the system could automatically alert local police and transmit his present location. Further, parameter alarms will prohibit suspects on probation or parole from violating terms of their release, such as being within a given distance from a spouse, school or another parolee. This system should prove to be far more cost effective than total incarceration and could be used for a wide variety of “low risk” crimes such as drunk driving, shoplifting, and so forth. It could also be used for some types of crimes, such as spousal abuse, minor assaults, and similar offenses but with more restrictive circumscriptions. Depending on the court sentence and circumscriptions, such a system allows a suspect to continue earning a living and greatly reduces the burden on the community for the necessary supervision.

**Data Mining.** All of these digitally based technologies and many others that will emerge generate a tremendous amount of data that will need to be managed, a process that will continue to be one of law enforcement’s biggest challenges in the Information Age. Consider the massive amounts of data that are expected to be collected as a result of information sharing. Because the data are compiled from various sources it will be difficult to match similar records. Last names can be spelled differently, pieces of information might be missing, and there are rarely unique identifiers such as social security numbers that will guarantee an exact match. Such issues are important not only because we want

to avoid missing potential matches, but also because we wish to avoid taking erroneous actions based on false positives.

To accomplish this within today’s homeland security environment, made up of extremely large data sets, it is inevitable that law enforcement will eventually use today’s most controversial information technology—data mining. Manually sifting through large amounts of information for a few small bits of information critically important to solving a problem is humanly impossible unless an analyst knows exactly what he or she is looking for and where to find it. This is why practically every area of human endeavor, from global banking to disease control, is developing and using data mining technology. In this respect, data mining can be of tremendous help to law enforcement in stopping crimes and attacks before they occur or assisting criminal investigators in their aftermath.

There are essentially two types of data mining: looking for known patterns or detecting previously unknown patterns. The former is the most commonly implemented type of data mining and is well researched, with an extensive available literature (here omitted). Detecting previously unknown patterns however is far more complex and requires more sophisticated algorithms: this latter area is the realm of DARPA’s ill-fated Total Information Awareness project. Data mining research efforts will continue to be concentrated in this area because it potentially produces the most promising results. Like health officials striving to identify the outbreak of serious diseases before they become epidemics, or bankers trying to stop identity thieves after just a few people are defrauded instead of thousands, data mining will play a critical role in identifying serious crime trends in their earliest phases and in preventing terrorist attacks before they occur. Of equal importance however, is to accomplish these things while protecting the privacy

---

of the innocent, a function that is possible to design into the technology.

Another important area of information technology research is combining and utilizing data from different media formats. For example, law enforcement data can be in the form of audiotapes or files, surveillance footage and/or, phone records. Technology exists today that can transform those media into formats that can be processed and queried. In addition, much potentially valuable information in the form of free form text is never processed. At most, systems in the past have been able to search those items using keywords. Smart techniques such as entity extraction and natural language processing could be employed to process free form text a priori, extracting meaning and linkages and integrating it with other information. This in turn will require preprocessing techniques, not often used in current law enforcement information systems.

## **The Power of Networks**


The power of technology in the Information Age lies not only in the tools that will identify, track and monitor people and things in our world, nor in the individual tools for gathering, processing, storing and analyzing the data that are generated. Power in the Information Age rests upon the ability of law enforcement officers to act collectively in a synchronized and complementary way, quickly and effectively using information to solve problems before they occur or as they are emerging. Individual officers will need to use the new and powerful tools being developed today and law enforcement agencies will need to process and analyze vast amounts of information and turn it into useful intelligence, but it will be the linking of law enforcement officers with all the information necessary to succeed that will have the greatest impact on the profession by 2015.

The Industrial Age manner of ensuring that members of a group are synchronized and working collectively toward a common goal is to create hierarchies and bureaucracies. Bringing many disparate departments under one organizational umbrella with centralized decision making and a single command and control process is one way to achieve information sharing and synchronization of individual actions and is the traditional law enforcement method of organization. We are continuing in this tradition even as we strive to improve police operations in the 21st Century. There are efforts in some localities to regionalize smaller agencies into larger ones, and at the federal level we have seen the creation of large bureaucracies governing previously independent agencies or the creation of “czars” controlling many disparate agencies in order to mandate their cooperation.

But technology today is creating a new operational paradigm—networks. Pervasive digital technologies are allowing people and information to connect in ways that have never before been possible. Bypassing hierarchical hurdles and tapping immediately into sources of information without the need for bureaucratic process and permission is inherently more efficient than traditional highly structured organizational models (Barabasi, 2003). In fact, in this new Information Age context increased bureaucracy may be antithetical to operating effectively in a dynamic and rapidly changing world.

Our criminal and terrorist adversaries are already beginning to understand the advantages of the network-centric model over traditional hierarchical organizations. Networks foster information flow to and from the individuals those members at the edge of the organization, doing the work that accomplishes a collective mission, and allows them to coordinate their actions without the centralized direction and control that slows





operations and decision making in traditional organizations (Alberts, Garstka 1999). The US military has been developing a network centric warfare model of operation for many years, and we are now beginning to understand its potential benefits within the law enforcement community in the wake of the 9/11 terrorist attacks. The notion of “connecting the dots” and the mantra of “sharing information” are an early manifestation of this network-centric movement in law enforcement, a realization that in order for information to serve a useful purpose it has to be readily available to the right people at the right time no matter where they might be working, regardless of agency or level of government.

Over the next decade a shift toward network centric operations will become a law enforcement imperative as digital devices such as Radio Frequency Identification (RFID), Global Positioning System (GPS), and micro-sensor devices are incorporated into everything and everyone in our communities. As more and more people become “wired” and the individual components of our world are weaved together into “intelligent environments,” traditional business processes will be eclipsed by those that take advantage of networks and their inherent ability to connect people with information seamlessly and immediately. Net-centric policing will be further improved as shared interagency networks, both wired and wireless, are constructed to accommodate multiple agencies from multiple jurisdictions, breaking the arbitrary agency boundaries that have historically constrained the flow of information.


## **Conclusion**

In today’s 21st Century Information Age world the number and types of technologies capable of being applied to one or more aspects of law enforcement is mind boggling. Coupled with

a rapidly expanding definition of what actually constitutes policing in the age of homeland security and the war on terror, the perpetual shrinkage of available resources, and the rate of change technology is bringing to the rest of society, it is easy to imagine civilian police agencies being overwhelmed by events and becoming less effective in the coming years. Developing and implementing the technologies and constructing the networks that will improve law enforcement operations by 2015 will take a concerted and Herculean effort. For a profession that continues to grapple with basic concepts such as combat vs. community policing and the appropriate role of sworn vs. un-sworn crime fighters in our organizations, the issues of Information Age technology seem daunting.

When it comes to improving law enforcement through technology, however, our most important consideration should be the effect that improvement will have on constitutional liberty. While it might be true that another or a series of 9/11-type terror attacks may do as much to damage civil liberties as overly aggressive law enforcement, that should not be a reason for police to willingly disregard the Constitution and use technology in ways that overstep our traditional democratic values. Law enforcement in a free society is only improved when it serves those values while fulfilling its mission to protect the innocent.

At the same time it is also important to remember that the technologies useful for law enforcement in the Information Age are already under development, most of them for military and commercial application. In the face of a growing terrorist and criminal threat to an increasingly vulnerable society these technologies will inevitably be used to stop or eliminate the threat, if not by civilian law enforcement agencies then by someone else. The military and private security firms are gearing up to take on those challenges today and



have the means and willingness to step up to the plate whenever necessary. As technology continues to advance even the general public will have the means to use technology for their own protection.

There is nothing inherently wrong with the military, corporations or the public assisting the civilian police in our collective law enforcement effort. They have been doing so for many years with great success. The danger we face in the Information Age comes from the very significant impact technology plays in our efforts to fight crime and stop terrorism and the threat those same technologies pose toward civil liberties if used inappropriately. Civilian law enforcement is the only organized component in society with a mandate to both protect civil liberties and enforce the law equitably for all people while being trained to do so. To accomplish these equally important objectives it is imperative that civilian police lead all efforts to fight crime and terrorism domestically, coordinating all other agencies and groups, public and private that are contributing to the effort, ensuring that the protection of civil liberties is at the forefront of every action and operation within our communities. If we fall too far behind the military and the private sector in our ability to understand, acquire and use advanced technology, the dominant law enforcement leadership role will shift to those who have the technological capabilities we lack.

## References

- Alberts, D., Garstka, J., Stein, F. "Network Centric Warfare: Developing and Leveraging Information Superiority," Department of Defense, Washington, DC. 1999.
- Barabasi, A., "Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life," *Plume*, New York, New York. 2003.
- Embley, Paul S: "XML in Justice Information Sharing: An Executive Summary," *Police Chief*, December. 2002
- MacDonald, Heather: "What We Don't Know Can Hurt Us," *City Journal*, Spring.