This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Moving Toward the Future of Policing

Gregory F. Treverton, Matt Wollman, Elizabeth Wilke, Deborah Lai

NATIONAL SECURITY RESEARCH DIVISION

The research described in this report was conducted within the RAND Center for Global Risk and Security under the auspices of the International Programs of the RAND Corporation.

Library of Congress Control Number: 2011939018.

ISBN: 978-0-8330-5320-6

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Imagine a future investigation of a home invasion robbery. En route to responding to the call, the police officer—she might now be called a customer service representative—searches databases and, while she drives, hears descriptions of any recent relevant incidents in the neighborhood, calls from the house, and previous law enforcement visits. The victims are not hurt, and they provide some description of the perpetrators and their methods. One of the victims also managed to get a slightly dark cell phone picture of one of the thieves in profile. The officer arrives and images the scene for fingerprints. She enters all this information and the cell phone photo in her smartphone, and, by the time she gets back to her car, her report has been filed. Descriptions, methods, prints, and picture are all being matched against information in existing databases. By the time she is moving, a match has been found, the suspect's last address has been identified, and a search has begun based on his cell phone number and location.

Vision of the Future

This vision of the future of policing is not all that futuristic. Most of the technologies are with us today, or soon will be. Some dimensions of this future—for instance, geographical police jurisdictions that less and less precisely match crime's reach across boundaries—have long been with us and will continue to be with us, but they are not immutable. A third dimension that will frame the future is also here: Criminals and criminal organizations are adaptive. They will continue to look

for seams in public safety defenses, and they will become more and more networked, thus able to learn what works more quickly. They will adapt even if we do not. The three dimensions together—jurisdiction, technology, and threat—suggest very different concepts of police operations, some of which also are here, in part, today.

Policing has transformed in the past and so can do it again. Its history can be divided into four overlapping eras. In the political era (most of the nineteenth century), policing was guided by law, but close and mutually beneficial ties between the policing force and politicians resulted in high levels of corruption—hardly surprisingly. As a reaction, in the reform era, which began early in the twentieth century, policing emulated J. Edgar Hoover's restructuring of the Federal Bureau of Investigation (FBI), aiming to become less political, more professional, and narrower in scope; as a result, police became less involved in providing social services to the communities they served. The reform era also saw the beginning of serious efforts to collect and study data on crime.

However, the spike in the nation's crime rate that began in the 1960s undermined confidence in the measures of the reform era. Research suggested that neither preventive patrol nor rapid response was effective. At the same time, issues of racial and gender discrimination boiled up on the political agenda, and these issues further increased the disillusionment with the so-called "objective" policing practices of the reform era, at least for many of America's citizens. For instance, a 1968 *Detroit Free Press* survey revealed that police brutality was the number one problem that blacks felt they faced in the months leading up to the July 1967 riots.

The result was yet another transition in policing, to an era of community-based or problem-solving policing that reemphasized good relations with the local community. Perhaps the most debated approach of this era was order-maintenance policing (OMP). In "Broken Windows" in 1982, George Kelling and James Q. Wilson posited that "fixing broken windows," or preventing public disorder, would not only establish a norm against crime in a neighborhood but also convey to the public that the police was invested in the community. OMP led to a variety of policing initiatives in the 1990s. In 1994,

New York City instituted CompStat, an initiative to hold local commanders accountable for achieving crime reduction goals in their areas, which Police Commissioner William Bratton and others credited for the decrease in crime in the city. The problem-oriented component of this era emphasized analysis as a crucial ingredient in framing effective policing strategies.

The fourth era, intelligence-led policing (ILP), traces its lineage back to Britain in the 1980s but was reinvigorated by the emergence of terrorism as a threat. That threat adds a new mission to policing, but in other respects ILP has much in common with community-based policing: Both require the support of the community; both require better communication and information-sharing within and across public safety institutions; and both seek to improve policing through analysis of empirical evidence, facilitated by better and faster technologies—the movement toward evidence-based policing and the quest for "predictive policing." The terrorist threat is at the margins of this book, but, in driving ILP, it does reinforce the vision of policing set out in this book.

More-dramatic parts of that vision are also already with us, at least in part. ILP suggests a form of deterrence based less on the presence of police on the beat than on an increased risk for criminals of being caught. It also indicates a changed balance between policing's front office—the customer service representative described earlier—and its back office, especially analysts and those who manage databases. Outsourcing of some police functions is on the rise, and it suggests a changed balance between sworn officers and civilians. It also hints at new possibilities for partnership.

Companies are now developing niche capacities for policing: Palantir, for instance, is a company built by creators of PayPal that specializes in "smart searches" of large amounts of data while meeting the privacy and civil liberties standards of federal law; another company, 3VR, aims to become the "Google of surveillance video" by creating "pictures" that are a fully searchable virtual template of facial features. But imagine if Google or another technology giant wanted to become policing's valued partner across a wide range of functions and departments. The economies of scale would dwarf those now present when departments share outsourcing for a single function, such as finance.

Privacy concerns would also loom large. Could they be managed, along with lines of accountability?

Drivers of the Vision: Jurisdiction, Technology, and Threat

Policing is mismatched to crime, for it is still primarily organized by geography, while crime is not. At one extreme, the bank robbed in a cyber crime may be in New York, but the criminals may be in Estonia, operating through a half dozen computers that they have commandeered in six different parts of the globe. At the other, Santa Monica is surrounded by Los Angeles but has its own police force. Most sharing of information is driven by particular crimes; routine sharing is rare. As late as 2009, Santa Monica also had different communications networks than Culver City, five miles away, and so found communication difficult. If working across borders in a single metropolitan region is hard, imagine working across international borders. The U.S.-Mexico border is a stark example, for it becomes as much a seam in police defenses and a sanctuary for criminals as it is a protection.

Two features of technology and policing are striking. The first is that, until recently, the innovations that changed policing the most—from automobiles to telephones to computers—were not invented for police or to improve policing. Rather, they were invented to make everyday life easier or richer. The second is that whatever technologies the police employ, the criminals can too. The key to the future of policing, then, is not technology but the ways in which police forces adapt it to their purposes. At its core, technology has the potential to change (1) data and intelligence gathering, (2) problem-solving processes, (3) partnership structures, and (4) departmental organization.

The globalization of commerce and technology has helped to fundamentally alter the nature of the threat to society from crime. The threat will continue to morph. Criminals are now able to commit crimes, such as identity theft, from home that previously required teams of people and intense coordination. Individuals and small groups can commit major crimes and thus are changing what "organized crime" means. Technology-enabled crime has arrived and will continue to

develop. And the next step, "virtual" crimes, is not far off; already there are harbingers of that new arena of crime. At the same time, "old" crimes are evolving as to be almost completely distinct from the real-world crimes from which they emerged. For example, what amounts to bank robbery can be done virtually, with no need for guns, money bags, and escape cars. In addition, the environment in which criminals operate will morph as technology, law, and law enforcement change. None of these dimensions operates independently of the others; they are all interconnected in complex ways.

Moving Toward the Vision

The following are concrete steps that police departments and other public safety agencies can take to move toward the vision, along with examples, both suggestive and cautionary:

Educate personnel and leaders. Building internal support for change is critical. For instance, police organizations thought preventive patrol was effective until analysis of data revealed very little difference among patrol patterns. Just as officers are taught how to spot an intoxicated driver, they should learn how to use technology: In some cities all patrol cars are equipped with fingerprint kits, and police are taught how to use the Automated Finger Print Identification System, a computerized system for matching fingerprint specimens. Education will be especially important as human resource needs change. Departments will need more data scientists to deal with large amounts of personal data and more security clearances to deal with sensitive information.

The use and exchange of possible sensitive personal data on suspects, criminals, and civilians will entail a strong commitment to data safety. The increasing interconnectedness of departments brings many benefits but also creates more vulnerabilities by which data can become insecure. It also obscures lines of responsibility for data and information. Data management plans will need to be constructed and implemented to ensure that the information that is being transferred across partnership networks is not compromised.

Police leaders will have to change culturally to accept integration as well. Police personnel will have to learn alternative ways of interacting with the public effectively—for instance, the Boston Police Department and its Twitter feed. With increased community involvement will come increased volume of communication and interaction between police personnel and citizens. This means that the majority of police personnel—not just officers working the street beats—will need training in customer service and client interaction in order to effectively engage the community.

Transition to common technical platforms. This should be low-hanging fruit but does not always seem to be. According to one assessment, the gaps across jurisdictions, like those detailed in Los Angeles, can now be overcome, and connecting the department with every other law enforcement agency operating in or around the jurisdiction should be the goal. While ILP, in general, requires integration of information from many intelligence-gathering entities, integration does not necessarily require a common technical platform. It does require at least a common platform for sharing information. Interpol and other cooperative initiatives can facilitate this process, and bilateral working arrangements are on the rise—for instance, allowing officers from other jurisdictions to pursue investigations across those jurisdictions even when the jurisdiction lines are national borders.

In Los Angeles, the LA-SafetyNet initiative aimed to connect 34,000 first responders across the county's different police, fire, and public health jurisdictions. Yet these initial efforts are being constructed before there is any broad agreement on standards for equipment and networks. As a result, there is no guarantee that other jurisdictions that seek to join the networks in the future will be operating, literally, on the same wavelength. Los Angeles County pioneered these efforts with the Terrorism Early Warning group, which began in the mid-1990s. It was explicitly designed to anticipate emerging threats, especially terrorism, and to try to deny networked adversaries the advantage of working in the seams of existing policing organizations. It sought to blend networking with traditional organization by including law enforcement, fire service, and health authorities at all levels of government.

Biometrics, like blood samples, iris scans, and DNA typing, may come to replace fingerprinting as cheaper, more-precise ways of identifying criminals. They may also be able to serve as unique identifiers across databases, yielding more-accurate cross-database search results. The advent and rapid improvement of database management and biometric technology facilitates information exchange. The FBI is in the process of developing a database of biometrics called Next Generation Identification that will share standards held by Britain, Canada, Australia, and New Zealand and will interface with the National Crime Information Center database to further the goal of instant and seamless cross-border information-sharing.

Leverage winning technologies. Over time, these winning technologies are those used for collecting, sorting, storing, and recalling information. Computer terminals in their cars, followed by handheld devices, have given officers on patrol access to information systems, enabling them to check quickly for stolen vehicles or outstanding warrants. Smartphones and mobile computing systems are likely to have a major impact, as are improvements in camera technology and programs designed to interface with them. Supercomputing—the ability to store, categorize, and retrieve massive amounts of data in a few seconds—will be the next step in transforming police investigations. The searchable data stored by programs like 3VR's could save hundreds of man-hours and free up human resources for tasks that computers cannot do. Not only can cameras hooked up to powerful software detect facial and other identifying features, but they can also be programmed to "learn" normal human behavior in order to detect unusual or suspicious behavior.

Leverage changing interactions and relations between police, the public, and the private sector. For example, to address its shortcomings in video surveillance, the Dallas Police Department Narcotics Unit turned to the private sector; a detective from the Technical Operations Unit worked with a local company to devise a new and improved video system. AT&T partnered with the FBI to allow it access to AT&T's call records after 9/11. When Mississippi Senator John Burton's Chevy Impala was stolen, he called OnStar. OnStar then called the police. When officers had the vehicle in sight, they requested

that Stolen Vehicle Slowdown be initiated, and the vehicle was safely slowed to a stop. Several technology firms and financial companies have regular meetings with police officials in the areas in which they operate in order to keep police abreast of new and emerging trends—for example, in identity fraud. The Boston Police Department has a weblog and a Twitter feed to alert Bostonians to activities of interest and keep them informed of goings-on in the city.

Draw maximum benefit from federal leadership and funding. Here, the spillover from the fight against terror is positive, providing both funding and some leadership. To be sure, terrorism gets a much larger share of resources than its societal damage would warrant, but departments have turned that aid into all-hazards assistance. Terrorism also spurs the trend toward intelligence-based policing. It also provides incentive for integrated efforts. The story of the public safety wireless network is still unfinished, but the transition from analog to digital television at least freed up space on the spectrum for an integrated public safety network. For all their shortcomings, the fusion centers are another example. They are intended to complement the joint terrorism task forces (JTTFs). JTTFs work on cases once they are identified, and the fusion centers are meant to assemble strategic intelligence at the regional level and pass the appropriate information on to the investigators in the task forces.