
CHALLENGES AND CHOICES

The job of law enforcement is never an easy one. Operating within a complex society, police organizations must be constantly on the lookout for new threats to public safety and devise ways to counter those threats. Those who endeavor to break the law are constantly adopting new forms of technology. Recent years have shown not just the appearance of crimes that would have been unheard of two decades ago, including identity theft and cybercrime, but also the effects of the most raw and basic technology adoption by criminals. It is difficult to envision a more dramatic demonstration of the technological threat to law enforcement organizations than a shoot-out where police are outgunned by individuals wielding automatic weapons protected by body armor superior to that available to the officers standing against them. The stakes involved in facilitating the adoption of new technologies can, obviously, be very high.

In an age of concern about the responsible use of public funds, however, technology can also play a role in making law enforcement more efficient and effective with the ability to accomplish more with fewer resources. These technologies—via their contributions to management of operations or allocation of officers—can potentially allow society to gain a desired level of public safety at a more reasonable cost. Because of technology’s potential to both increase the effectiveness of police forces in the face of evolving crime and allow more effective police operations, society as a whole has an interest in understanding and, if need be, facilitating technology adoption by state and local law enforcement organizations.

NUMERICAL LESSONS FROM THE SURVEYS

One of the main goals of the RAND Law Enforcement Technology Survey was to identify what technologies were and were not available to law enforcement organizations around the country and to gauge their future technology needs. As a result, the results of the survey could be summarized on a basic level by simply delineating the range of technologies that are generally not available to local police departments. These were technologies that, when asked about their current accessibility and any barriers to their acquisition, respondents indicated were not currently available and were not “unnecessary” (LETS, 22, 25–29). As a result, this represents a list of potentially needed technologies. The listing of the technologies, along with the percentage of local police departments lacking them, is included in Table 30. The table is sorted in order of decreasing non-availability, down to a cutoff of 25 percent. It should be borne in mind that because the surveys did not cover every current or potential law enforcement technology, this represents a limited slice of the technologies which are and are not available to local police departments.

When examining such a summary listing of unavailable technologies, it is important to place the survey responses in an appropriate context. Although the values included above are the percentages of law enforcement that indicated these technologies were both unavailable and not unnecessary, it is highly likely that there is a significant barrier for a survey respondent (especially for a survey of this kind) to designate a technology as unnecessary.¹ For example, it is the case that more than two-thirds of local police departments lack “necessary” radioactive agent detection equipment (Table 30). The degree of necessity of this technology might be appropriately calibrated by considering the net increase in public safety that might accrue from providing each of these departments a Geiger counter compared to providing training equipment to the 28 percent of respondents who lacked it (or upgrading the training equip-

¹There is a legitimate personal and organizational interest not to refuse any resources that might improve law enforcement performance even marginally. As a result, while it is unlikely that a circumspect observer would assert that each of the 57 percent of local departments that lack night vision capability truly “need” it, there is also a clear rationale why many survey respondents would indicate that they did.

Table 30
Technologies Not Available to Local Police

Technology	Not Available	Technology	Not Available
Detection and analysis of cyber-attacks	79%	Computers in patrol cars	58%
Blister/nerve agent protective clothing	79%	Electronic listening	57%
Video conferencing equipment	75%	Night vision devices	57%
Kinetic energy projectiles	75%	Vehicles—special purpose	45%
Chemical agent detection	71%	Crowd or riot control	44%
Long-range video monitoring	69%	Computer-based training	41%
Stun devices/projectiles	68%	Conference call equipment	36%
Radioactive agent detection	66%	Computer assisted dispatching (CAD)	35%
Explosives detection	64%	Integrated data bases	34%
Polygraph equipment	64%	Protective gloves, helmets, and shields	34%
Fleeing vehicle interdiction equipment	63%	Audio-visual equipment to obtain evidence	30%
Concealed weapon detection devices	62%	Training equipment	28%
Bomb containment/disablement equipment	60%		

SOURCE: LETS, 22, 25–29. Numbers are statistically adjusted percent of local departments reporting technology is not available.

ment of the many respondents who indicated that theirs was insufficient). All technology acquisition decisions, whether they are made at a local or national level, are a calculus of trade-offs and it is important to remain cognizant that there are serious consequences of losing sight of that fact.

In addition to identifying technologies that are unavailable to state and local police organizations, the RAND surveys also asked for information on the age and quality of currently available technologies. By identifying their current technologies as either obsolete or “old but serviceable,” survey respondents provided a list of technologies

Table 31
Technologies in Need of Replacement by Local Police

Technology	Obsolete	Old but Serviceable	Either Obsolete or Old
Radio equipment	10%	46%	56%
Training equipment	10%	35%	44%
Administrative/accounting systems	18%	26%	44%
Computers in workspaces	7%	34%	41%
Audio-visual equipment to obtain evidence	12%	28%	40%
Crowd or riot control	12%	25%	37%
Protective gloves, helmets, and shields	9%	25%	34%
Ballistic- and stab-resistant armor	8%	25%	33%
Computer-based training	9%	20%	29%
Integrated data bases	8%	22%	29%
Conference call equipment	3%	24%	27%
Vehicles—special purpose	4%	21%	25%
Cellular telephones	2%	24%	25%

SOURCE: LETS, 22, 25–29. Numbers are statistically adjusted percent of local departments reporting as indicated.

that many be candidates for replacement in near to medium term. These responses are included in Table 31 in decreasing order of the fraction of departments characterizing them as “Obsolete” or “Old but Serviceable,” down to a cutoff of 25 percent (LETS, 22, 25–29).

From the perspective of the policymaker, several things stand out from such a numerical summary of the survey results. Most striking is the fact that 18 percent—almost one in five local police departments—indicated that their administrative or accounting systems were obsolete; without such input from departments it would be difficult to see that such an “unglamorous” technology might indeed be a high priority for local police forces. Other entries on this table are less surprising. The appearance of computers and cellular telephones is not unexpected given the short product cycles and rapid obsolescence of those products. The appearance of ballistic-resistant armor (stab-resistant armor is not broadly available) on the list also holds a relevant lesson from the perspective of law

enforcement technology policymaking. While bulletproof vests do “age” and become worn over time, studies have shown that the protective properties of the armor do not break down.² As a result, the notion of an “obsolete” bulletproof vest is a complex one likely based more on the obvious importance of the technology (and its performance) to officers rather than the technology itself.

Just as was the case in examining the summary list of unavailable technologies above, the importance of reasoned trade-offs among technologies must remain firmly in mind. Although a third of departments report that their workspace computers are “old but serviceable” the costs and benefits of upgrading them all to “state of the art” must be weighed against the unavailable technologies above, providing training to better use technologies that are already available, or performing R&D to generate the potential that superior technologies will be available in the future.

CONCEPTUAL LESSONS FROM THE SURVEYS

Just as the aggregate survey results suggest the trade-offs that must be made at the highest levels of technology decisionmaking, they also emphasize the trade-offs and other obstacles that face technology adoption at the micro level. Returning to the general framework presented in the introduction, the results of the surveys indicate that, for law enforcement organizations, each of the four obstacles to technology adoption must be considered. For the broad classes of technologies included in the survey, respondents identified all four:

- Costs
- Technology Risk
- Human Associated Risks
- Unanticipated Potential Costs

Of the reasons cited by respondents, cost routinely stood out as the primary obstacle to the adoption of new technologies. Such a result is not unexpected given that, at some price point, any technology be-

²See “Old Armor Tests As Good As New,” <http://www.nlectc.org/>.

comes attractive for purchase and, until it reaches that level, cost does stand as an obvious initial obstacle to using the technology. If cost is a sufficient obstacle, none of the other barriers to adoption are relevant; if you don't have the opportunity to adopt a technology because the cost is too high, how well you adopt it is not an issue. The fact that many respondents cited cost, however, likely also represents the important and difficult trade-offs that must be made within police departments. Because of the labor intensity of their activities, technology acquisition must always compete with "placing more police on the street" or paying overtime to extend an investigator's work on a pending case. In addition, because of the variety of ways police departments could allocate their funds, trade-offs among technologies are also likely very important. It is not just the cost of the technology that dictates its desirability but the perceived benefits that are associated with purchase. In this light it is not surprising that fewer large urban departments cited cost for some technologies that are particularly suited to solving the problems of an urban police force.

But just as cost is clearly a barrier, other barriers to adoption are important as well. Departments are concerned about the technical risks associated with some technologies as expressed by their indicating that the "reliability/effectiveness" of the technology could be a barrier to acquisition. Smart guns stand out as such a technology where, if police departments are to adopt the technology, steps must be taken to develop it to the point that these concerns are satisfied. The human factors associated with technology adoption, as emphasized in concerns about training, training technology, and other sources of information are also clearly important for both law enforcement agencies and forensic science laboratories. The barrier that finding sufficient trained personnel poses to the effectiveness of forensic science laboratories stands as a troubling but important finding of this study. Currently, most law enforcement organizations' technology adoption efforts are less affected by concerns with unanticipated effects like public opinion. Important exceptions exist to this trend, however, including stand off and direct electrical devices, once again emphasizing the differences that exist among technologies with respect to adoption barriers.

LOWERING THE BARRIERS TO TECHNOLOGY ADOPTION

Because of society's interest in law enforcement adopting technologies which make its activities more effective, promote public safety, and advance the cause of justice, how policies can be crafted and targeted to reduce barriers to adoption is of clear interest. As discussed in Chapters 7–10, it is clear that federal programs designed to lower these barriers, whether through R&D, provision of technical information, support of training, and other activities are making progress in making the acquisition process easier for law enforcement organizations. The relatively modest percentages of particularly local law enforcement departments that are currently being reached by these programs suggests that they have the potential to more broadly serve the needs of the nation's police, provided sufficient organizational and financial resources are available. It would be counterproductive to encourage more police forces in the country to take advantage of these resources if the increase in demand would overwhelm the system and make it less effective for everyone. On the other hand, while the generally positive views of federal support programs on the part of those departments that have benefited from them are encouraging, the low intensity of these views suggests that there is more that can be done to increase the relevance of the aid and advice and craft it to better serve the needs of local police. The generally much more positive views of federal programs by the crime laboratory respondents to the survey is noteworthy suggesting that these programs are more effectively reaching their intended audience.

Policy Considerations

When considering federal responses to these issues, it is important to consider policies not just in terms of short-run effects but also how their long-term effects can be crafted for the social good. The programs that were viewed most positively by respondents to these surveys—direct provision of technology and transfer of federal monies to the local level for technology purchases—are uniquely short-run strategies. Although it is understandable why law enforcement practitioners, who are primarily asked to solve problems in the short term, would find the quick effects of these types of programs appealing, they may not be the best way of

investing limited federal resources. Provision of money that is designated for technology support also eliminates the trade-offs that must be made at the local level among competing potential uses for the resources; when a particular technology is mandated as a condition of support, even trade-offs among technologies may be eliminated.³ While providing a technology to a police force today will generate immediate benefit (assuming that the other barriers to adoption of the technology are surpassed), its return will gradually decrease over time as the system is worn out or becomes obsolete. It is possible that other programs, whose returns increase with time rather than decrease, might be better policy targets.

One example of such an increasing returns target is the provision of technical training to help overcome human barriers to technology adoption. Training of individuals has the possibility to not just improve how individuals use today's technology but improve their use of technologies in the future; the potential for trained individuals to spread their knowledge within their organizations provides the chance for increased returns on the investment even in the short term. The RAND survey results and findings from interviews strongly suggest the need for increased training, including training to use technology already available or being procured. This particular topic was brought up with respect to small rural departments all the way up to a large urban department with a billion dollar budget. Respondents spoke of considerable, wasteful redundancy in training curricula. Training technology is developing rapidly on many fronts, including law enforcement. Distance learning and interactive computerized training offer promise for overcoming at least some of the obstacles (e.g., lack of time and money) agencies face in training their personnel.

Like training, R&D can also address the technology adoption barriers of organizations, but it is a much more long-term strategy. It is only through research that new technological possibilities are discovered and current technologies are adapted and applied to the needs of law enforcement. Because of the unique characteristics of the law en-

³It should be noted that these effects have the potential to generate significant distortion in the way that funds are used at the local level since it is the competition among different potential uses and the trade-offs among alternatives that could lead to more efficient allocation.

forcement technology market, private firms may ignore roles in this area not taken by the public sector. The importance of research as an enabling approach to these problems—exemplified by the important advances in body armor and other technologies which outfit today's officers—point out that, even though local forces may not see immediate benefits and, as a result, may not be as supportive of these programs, they are important nonetheless. Research and development can also take as a goal not only developing new technologies but improving those which are already available; selecting a target of providing rapid, cost-effective DNA analysis capabilities could go a long way toward removing the backlogs and staff shortages that currently prevent forensic laboratories from making their full potential contribution to law enforcement. Research and development therefore likely represents a unique role for government to support work that not only lowers adoption barriers for current technologies but attempts to apply novel technologies to other needs of law enforcement as well.

OVERARCHING TECHNOLOGY CHALLENGES

Another place where federal involvement can play a very important role in the technology challenges of law enforcement is by facilitating or spearheading the type of “large scale” technical changes that can only come from the upper levels of a social system. One example of such a role is systems integration among the many different government activities that have an effect on law enforcement agencies. Although taking an integrated view toward crime control as involving more than law enforcement seems sensible to many people, it requires at least two technical changes:

First, as we find the need to integrate criminal justice and social services databases, we will need to work through confidentiality requirements. Second, optimal analysis would allow us to commingle an individual's data from various disciplines. This will be problematic because all data systems have difficulty in positively identifying and tracking individuals. The problems of individual identification will increase significantly as we try to join databases (O'Connell, 1998, p. 95).

That is the big challenge before us at the dawn of the twenty-first century: to embark on the unification of our technology with our humanity (Dertouzos, p. 314).

One person we spoke with described broad integration concerns and challenges as follows:

As we're looking at integration issues throughout the country, the general focus that we're driving towards is not only criminal justice but *justice*. We're looking into expanding the civil aspects as well as the criminal and [asking] what are the juvenile, family court, and domestic relations issues. [You can draw the boundary around law enforcement] but that's not where most of the thinking has gone these days when we're talking about integration and flow of information.

What we're seeing more and more often is that the CIOs [Chief Information Officers], if they're powerful people and if they're very directly connected to the governors, are playing this role of defining the infrastructure, the standards, and the architectures that should be used for the sharing of information. They are right at the center-piece of the design of the integrated criminal justice information systems. That's as it should be, because there is a growing recognition among probably more of the urban or more sophisticated sheriffs and police chiefs that there is a need to flow information in and out of the criminal justice system with transportation, education, social services, and the other non-criminal justice entities that plug into [a Unified Criminal Justice Information System] from both the front end and the back end.

The Office of Justice Programs and its Bureau of Justice Assistance of the Department of Justice have been working in partnership with SEARCH, the National Consortium for Justice Information and Statistics, to better define both "the system" and "integration."⁴ The Justice Department's Office of Justice Programs has also funded the National Association of State Information Resource Executives

⁴See SEARCH Special Report, "Integration in the Context of Justice Information Systems: A Common Understanding," Revised April 2000, at <http://www.nasire.org/hotIssues/justice/SEARCHintegdef.pdf>.

(NASIRE) to develop architectures and standards for sharing information.⁵

CONCLUDING THOUGHTS

Although recent crime rates have been at low levels, preliminary figures show some increases in 2000. As one response to this change, federal officials may choose to increase technology-related support to state and local law enforcement agencies. Although the primary motivation for this may be desire to increase public safety (through reducing crime), the goals of improving law enforcement efficiency (reducing costs over the long run) and promoting justice (while reducing incidence of injustice) can and should also be taken into account.

Historically, “cops on the street” and hardware have had much more political appeal than “softer” technologies. Respondents to the RAND surveys are crying out for training and software support, for increased ability to access and share data, and for forensic capacity to prevent and to solve more crimes. Police leadership—especially in the larger jurisdictions—sees the need for technology to support accountability.

Progress in some of these areas is just a matter of funding—and distributing funds where they are most needed. In other areas, such as data sharing, there are both technical and legal obstacles to realizing full potential. For example, agencies have legitimate concerns about ensuring security and integrity of data they share; recipients of data need assurance that it is accurate and current. Laws may need to be revised, to allow data sharing, where appropriate, while safeguarding legitimate privacy concerns.

In some areas, progress can be made simply by “doing business” differently. For example, if agencies within or among jurisdictions were able to form buying consortia to purchase technology, substantial unit cost reductions could be achieved. To do this, however, consortia members have to consider individual agency purchasing systems

⁵See NASIRE Report, “National Information Architecture: Toward National Sharing of Governmental Information,” at <http://www.nasire.org/hotIssues/justice/Fullrept.pdf>.

and provide ways to access the pool without violating purchasing agreements. This is, of course, much easier said than done, given the desire of local government to maintain local control.

It is becoming increasingly evident that a systems approach to public safety, cost reduction, and justice is the most appropriate way to pursue each of these goals. Concentrating solely on one aspect, such as public safety/crime reduction, leads almost invariably to imbalances and undesirable side effects. For example, concentrating only on apprehending, convicting, and incarcerating criminals leads to prison costs that are not sustainable in the long run and the perception of injustice among groups disproportionately incarcerated.

Inherent in a systems approach is the need to look beyond narrowly defined law enforcement. We have done that in this study by including forensic science and touching on courts, corrections, and schools—as well as by considering training in conjunction with technology and by relating technology and accountability. But there are many aspects of the systems approach that can be dealt with adequately only in the context of specific locales and situations—and that is beyond the purview of this study.

Strategies for promoting the diffusion of worthwhile technology deserve careful consideration. Differences among technologies, as suggested by the survey results, are very important. Diffusion of simple technology, such as collapsible batons replacing older types, probably don't require more than vendors' marketing strategies and natural word-of-mouth communication among police. Other technologies, such as AFIS, NCIC, or the futuristic lab-on-a-chip or lab-in-a-box, will most likely require more holistic diffusion strategies, including training and interagency protocol development, to overcome the considerable barriers that exist to the adoption and effective deployment of any new and powerful technology.

Recommendations

In light of the information contained in the RAND surveys and the discussions surrounding it, it is relevant to ask how the discussion contained here can contribute to the construction of a reasonable, forward-looking federal technology strategy to support state and local law enforcement. To that end, we suggest the following points:

- To avoid wasteful spending and to ensure technology is used to good effect, we recommend that federal initiatives providing technology hardware or software include provisions for training. It appears that all too often procurements are made under the false assumption that “somebody else” will take care of training.
- To help law enforcement agencies make more effective and less disappointing technology acquisition decisions, we recommend continuing and publicizing federal testing, evaluation, and standards setting for technologies needed by state and local agencies.
- To enhance public safety, we recommend providing data network access to all police and sheriffs’ departments that have unmet needs for it. No American community—large or small—wants its officers to lack information that could have been available to recognize and apprehend dangerous criminals wanted in other jurisdictions.
- To meet the demands of investigation as well as prosecution, we recommend building forensic capability well beyond current levels. This could include providing screening-test technology to first responders, as well as increasing training, recruiting, and retaining forensic scientists. We recommend it include increased federal support of R&D of forensic science techniques and technologies. One possible focus of this R&D might be on lowering the acquisition cost for a standard, known throughput capability suite of forensic laboratory equipment.
- To correct evident competitive disadvantages of smaller law enforcement agencies, we recommend that federal agencies make a serious effort to make it easier for rural and small urban police and sheriffs’ departments with real, unmet needs, to obtain funding and other technology-related support. Although some rural and small departments may have crime rates too low to warrant more substantial investment in modern technology, other rural or small departments suffer unmet needs because they lack political clout or skilled personnel available to write grand proposals.
- As a cost-effective investment, we recommend increased federal funding of R&D of technologies that automate or otherwise increase productivity of what are presently labor-intensive or

training-intensive processes. Such technology can help make high quality law enforcement more affordable.

- To promote police accountability and to provide more objective evidence of lawbreaking, we recommend that all or most patrol cars be equipped with video cameras and wireless networked computers. Videotaping provides objective evidence useful for suspect identification and prosecution, as well as for resolving complaints of police misconduct. Rapid access to current data on stolen vehicles, outstanding warrants, etc., can reduce officer uncertainty in confrontational situations. The most practical federal role in this may be in defining or developing equipment suites or standards, rather than in directly funding their acquisition.
- To reduce confrontational uncertainty, risk of injury to officers and the public, as well as risk of confrontations escalating into civil disturbances or abuse of police power, we recommend continued federal support for the development, testing, and deployment of technology that can be carried in patrol cars or on officers to detect concealed weapons at a safe distance. We note that military and other security forces have similar needs.⁶

These technology-specific goals, if coupled with attention to the technology adoption considerations discussed here, could lead to more effective use of technology by law enforcement organizations nationwide which, we believe, has the potential to contribute significantly to public safety, long-run cost reduction, and justice.

⁶It is also important to note that there are significant applications for any non-portable versions of this technology that might be produced during development of patrol car or police officer models. For example, stationary devices that could detect the presence of concealed weapons could be placed in schools and airports detecting the "arrival" of any weapons into a monitored area. Such technology, if it was made reliable and cost effective enough, could allow educational institutions in particular to devote less of their resources to security and more to the primary goal of student instruction.