Commentaries on:

Development of Policy Governing the Use of Technology in the Criminal Justice System

Alfred Blumstein

Peter Young

Jennifer Granholm

Commentary by Alfred Blumstein,* Professor H. John Heinz III School of Public Policy and Management Carnegie Mellon University Pittsburgh, Pennsylvania

Science and technology have come a long way in their use by the criminal justice system since I was first given the task of identifying their roles for the President's Commission on Law Enforcement and Administration of Justice in 1965.[1] At the time, computers were relatively new, but they were already being used in remote inquiry systems (for example, the Federal Bureau of Investigation's (FBI's) National Crime Information Center (NCIC)[2]). The one area where there was a major technological barrier was fingerprint identification, but the Automated Fingerprint Identification System (AFIS)[3] has largely solved that problem. In all other areas of technology examined by the Commission, the issue was much more one of deciding how to exploit available technology, with appropriate attention to cost, unintended consequences in disruption of operations, and invasion of privacy, broadly defined.

At the meetings of the Science and Technology Task Force and those of its outside advisory committee, more time was spent on the privacy issues involved in creating, maintaining, and accessing criminal history records than on any other issue, and on almost all other issues combined. There was a major concern about the centralization of criminal history records (J. Edgar Hoover was FBI director), and that led to the design of a system that featured a centralized index, with individual criminal records maintained by the States. It is very close to the Interstate Identification Index (III), a criminal history records system implemented through SEARCH (the National Consortium for Justice Information and Statistics).

Three Major Technologies

Three technologies in my view have the potential to make major contributions to criminal justice operations:

- Networking of criminal justice data, including personal criminal history information, throughout the system and among its various agencies.
- Use of global positioning systems (GPSs) and individual transmitters to track and monitor certain categories of people who are under the control of the criminal justice system.
- Use of unique personal identifiers (for example, fingerprints and DNA) to identify perpetrators or to establish a suspect's innocence.

* Dr. Blumstein chaired the Science and Technology Task Force of the 1965–1967 President's Commission on Law Enforcement and Administration of Justice.

Each represents an important opportunity for policymakers and poses the kinds of problems the paper addresses. I will discuss why each can make an important contribution to criminal justice operations, present some of the hazards it may involve, and suggest ways to limit the risks.

Networking of Criminal Justice Data

To a significant degree, the primary function of the criminal justice system is to process information—to record and analyze data on crime incidents and individuals. The system performs this function very inefficiently, however, because each agency has only its own store of information, and the same information is entered many times at each site. If there were better ways to enter information, the result would be better and more informed decisions, with consequent greater equity of decisionmaking and less risk of a wrong or embarrassing decision. Broader information sharing within and, eventually, among jurisdictions would seem desirable.

Information sharing has been widespread for some time in industry and in many areas of government other than the criminal justice system. Why has it not happened in the criminal justice system? The first explanation is that the system has no single supervisor. It is intentionally (and appropriately) fragmented on decisions relating to individual liberty to maintain the checks and balances essential to a democracy. No single individual is in a position to arbitrarily issue orders to everyone else. The second explanation is that each agency has a degree of institutional paranoia. None wants its sister agencies to know what it knows or does not know, as that might put one agency in the position of being able to challenge the decisions of another.

A third explanation is that all agencies maintain their information in different and incompatible databases. That precludes sharing. In an era when everyone can access the *New York Times*, the *Washington Post*, or almost any other newspaper on the World Wide Web, it is the weakest explanation. All agencies maintain various kinds of controls over access to various parts of their Web pages. The fourth and perhaps most appropriate explanation for the failure to share information more broadly is the need to protect the privacy of incriminating information about the many clients of the criminal justice system, especially those who are young and not yet criminally responsible.

All these concerns are legitimate and can be addressed with a combination of rules of access and the technology to enforce those rules. Various kinds of information can be protected by different levels of security, depending on the category of user. Logs of use can be maintained and audited so that improper use can be detected. An information system development team, composed of representatives of all relevant agencies, could be established. It would include the courts, which must of course maintain independence in their decisions but should not be unwilling to be involved, as they also need information controlled by others.

When computers were first used to handle criminal history information, one concern was that they did not understand “the Judeo-Christian concept of redemption.” In fact, it is much more difficult for paper records than for computers to carry out that concept. Records in which no new entries have been made for X years (with the number represented by X to be negotiated and supported by analysis of reasonable risk of committing new crimes and estimates of how

frequently a new case occurs after X years of quiescence) could be either erased completely or placed in a secure status where they could be accessed only for a grave reason, such as a serious new felony.

Tracking Individual Offenders

Now that the country's prison and jail population has passed the 2 million mark, even more people are starting to challenge the desirability of all that use of imprisonment at a cost of more than $20,000 per year per prisoner. This "cause" is uniting fiscal conservatives and social liberals as well as leaders of public higher education whose budgets are the principal source of the increments made annually in the $40 billion spent on corrections. The solutions being considered limit the kinds of offenses warranting incarceration and specifically focus on violent offenders, with various proposals for community or intermediate punishment for many others, especially drug offenders, who constitute more than 20 percent of all prisoners. One technique, used thus far to only a limited degree, is house arrest. The offender under house arrest stays at home with a transponder bracelet attached to his leg that responds to telephone calls made randomly to him by the corrections agency. Failure to respond to calls triggers an alarm and can result in an arrest warrant.

This method of monitoring could be much more widespread and efficient. The link to the telephone could be replaced by a small, low-cost global positioning system (GPS) that would enable a central computer to track him wherever he is. The technology is already available (to track the whereabouts of private passenger cars, for example). The offender would be subject to the same restrictions (for example, he would be obliged to remain at home except to go to work or attend school; he would be required to stay away from bars or other prohibited areas), but the added benefit would be that any movement outside the home—especially in the vicinity of a crime scene that might fit his modus operandi (MO)—would be detected. The data on his movements would be entered into a computer through a cell phone linked to the GPS.

This approach is preferable to incarceration, both from the perspective of both the individual and the justice system. For the individual offender, it means he or she does not spend his days in prison. For the system, it means lower costs. Another advantage for the system is the greater control it affords compared with other forms of community supervision, such as probation or parole. The problem with this approach, as with all community-based control systems, is that it is likely to "widen the net." For example, it would subject to tight control individuals who might otherwise be appropriately placed in the less restrictive status of probation. This is always a risk. It can be addressed by integrating these approaches into sentencing guidelines, where they exist, or it could be used for high-risk parolees or only if authorized by the courts.

Unique Personal Identifiers

The method of establishing a crime suspect's identity has morphed from the era of paper fingerprint records through the AFIS era and into the era of DNA, and it could move into an era of brain-scan magnetic resonance imaging (MRI) or other, similar methods of identification. The advantage of using a file of coded DNA from a set of high-risk offenders maintained in a "latent

DNA" file is that crime investigators are not dependent on latent fingerprints alone (criminals circumvent fingerprint analysis simply by wearing a glove). They can use any other body material, such as hair, skin, or semen, to identify crime scene suspects. DNA has also proven particularly valuable for identifying individuals who were *not* at the crime scene, thereby establishing the innocence of people who might otherwise have been suspects and, most significantly, exonerating a number of individuals on death row.

The problem with the more recent identifiers like DNA is the volume of personal biological information they contain, none of which is contained in a fingerprint. As long as the information is used only to identify individuals and not to probe for other biological characteristics, there is no problem in using it. But because the temptation to probe further may be irresistible, there must be regulations that prohibit such probing, with penalties imposed for use of biological information for other than individual identification. Technology can also help if DNA were coded to ensure identification is unique, but all biological characteristics suppressed, with only the coded identifier maintained.

Role of the Federal Government

The Federal Government has a most important role in developing and testing new technologies and facilitating their deployment by the criminal justice system. It also has an important leadership role in identifying the problems—and particularly the privacy problems—posed by these technologies and in helping to develop rules and procedures to ensure that the inherent tension between privacy and access, between liberty and control, and between efficiency and invasiveness is resolved in a way that reflects appropriate tradeoffs. Intrusiveness and control are more acceptable with respect to people who should be in prison than with respect to people convicted of a driving violation.

The National Institute of Justice (NIJ) is the Federal agency designated to sponsor research in and development of technologies for use by State and local criminal justice systems. For some technologies, like soft body armor, NIJ has performed this function well. For body armor, as for many other technologies, NIJ has also sponsored the development of standards for the product, so that consumers who are technically naive (a reasonable assumption for most agencies in the criminal justice system) can confidently make purchasing and deployment decisions. NIJ's research and development are guided by a users' advisory committee that helps ensure user concerns and needs are taken into consideration. To meet diverse needs, the Institute offers a range of each type of product assessed and intended for public use. That way, individual agencies need not customize a given technology for their own use and are less vulnerable to the seductions of more aggressive suppliers. NIJ convenes stakeholder groups that agree on rules and procedures to minimize the risk of a technology being used inappropriately.

These roles are entirely appropriate because, by taking advantage of the economies of scale made possible by the Federal Government, they allow the States to avoid having to take on these roles individually. They facilitate the purchase of "public goods" in a way that would not be done at the level of the individual agency or even at the State level. All this suggests there is a continuing

role for NIJ in facilitating the development, implementation, and control of these important technologies.

Notes

1. See *The Challenge of Crime in a Free Society*, by the President's Commission on Law Enforcement and Administration of Justice, Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration, 1967; and *Task Force Report: Science and Technology, A Report to the President's Commission on Law Enforcement and Administration of Justice*, by the Institute for Defense Analyses, Washington, DC: U.S. Department of Justice, National Institute of Justice, 1967.

2. NCIC (the National Crime Information Center), established in 1967 by the Federal Bureau of Investigation, is a set of computerized databases containing information about stolen property, people wanted by the police, missing persons, and other data. All records are entered locally, but authorized users nationwide can access the system to investigate crime. All 50 States and the District of Columbia are linked to NCIC.

3. AFIS (the Automated Fingerprint Identification System) is a system of identifying suspect fingerprints by matching them against a huge database containing digitized and stored prints.

Commentary by Peter Young, Deputy Director
Police Scientific Development Branch
Police Policy Directorate, Home Office
St. Albans, United Kingdom

Some of the initiatives now under way in the United Kingdom to advance the use of technology in criminal justice operations are presented in this paper. Their policy implications are also presented. That discussion is first placed in the context of issues that are central to the development of technology policy in the UK.

Policy Development Issues in the United Kingdom

Stakeholders need clear policy aims

The mission of the Home Office is to build a safe, just, and tolerant society in which the rights and responsibilities of individuals, families, and communities are properly balanced and the protection and security of the public maintained. Within that overall mission are several aims, as follows:

- Reducing crime, particularly youth crime, reducing fear of crime, and maintaining public safety and order.

- Delivering justice through effective investigation, prosecution, trial, and sentencing and supporting victims of crime.

- Preventing terrorism, reducing other organized and international crime, and protecting against threats to national security.

- Effectively executing sentences imposed by the courts as a means to reduce reoffending and protect public safety.

- Helping to build, under a modernized constitution, a fair and prosperous society in which everyone has a stake, and in which the rights and responsibilities of individuals, families, and communities are properly balanced.

- Regulating entry into and settlement in the UK in the interests of social stability, economic growth, and facilitation of travel by UK citizens.

- Reducing the incidence of fire and related death, injury, and damage and ensuring the safety of the public through civil protection.

The first aim—crime reduction—is the overriding one. It encompasses reducing both crime and the fear of crime. The focus of crime prevention is on reducing the amount of crime; that is, driving down overall crime rates. The types of crimes most frequently committed in the UK are—

- Burglarizing homes.
- Burglarizing commercial premises.
- Theft of or from vehicles.
- Theft from shops.
- Trafficking stolen goods.
- Criminally damaging or destroying property (including endangering life).

Policy support from top leadership is needed

The government of the UK has made crime reduction a key priority. This priority is reflected both in the aims of the Home Office and in the provisions of the Crime and Disorder Bill. Reducing crime is an imperative both for international and national security and for citizens' safety. In an effective crime prevention strategy, technology is an increasingly important consideration.

Because law enforcement is fundamentally a human activity, the interface between humans and technology is vital. Technology should be used to augment and support human effort in law enforcement.

Crime committed by people under the influence of drugs—from traffic violations to murder—and crime committed by drug users seeking to fund their addiction account for many of the most frequently committed crimes. They affect the lives of so many people, reduce the quality of life, leave citizens in fear, and absorb an enormous amount of resources from the police, the courts, and health and social services. Drug marketing is transcontinental as well as transnational, and developing effective, reliable, and affordable technologies to detect illegal drugs is a high priority.

Technologies must be user friendly and acceptable to the public, be efficient and effective, and support criminal justice requirements and priorities. A good example of an acceptable technology is town-center closed-circuit television (CCTV) systems that help detect and prevent crime. Politicians, public officials, police, and technicians have all worked hard to ensure that this technology is not only effective in preventing and detecting crime, but is also acceptable—indeed, welcomed—by the public. This integrated approach and close cooperation at every level has been a real success story. Solutions also need to be cost-effective. Every national government in the free world is experiencing pressure from priorities that compete for resources.

In the past, not enough care was taken in every instance to ensure that the user requirements, and thus the operational requirements based on them, are fully defined, quality assured, and up to date. This is a two-way process, for often we the customers—the users—need help from scientists and technicians to ensure we really understand our requirements, and that our policy and operational needs are faithfully translated into reality. We also need to work together across

sectors. By working with the commercial sector to ensure that manufacturers and vendors of hardware and software fully understand law enforcement's needs and priorities, enormous gains can be made in efficiency and effectiveness. The temptation is for everyone to perceive one's own technology requirements as unique, with the result that systems can easily become overspecified and overcomplex, and therefore call for specially designed and high-risk software. If someone else has a proven system that meets 90 percent of our requirements, adopting it may enable us to move forward faster, less expensively, and with fewer technical and business risks.

We need to work across national boundaries. International cooperation is vital in the war against crime, so we need to be especially creative in finding either novel solutions or novel applications of existing technology. We need to work together to share technology, ideas, and both the technical and financial risks of developing technology.

Major criminals use sophisticated data encryption systems in an attempt to prevent law enforcement from accessing their communications or the records of their criminal activities. I believe this is going to be an increasing problem for surveillance and evidence gathering, particularly for financial transactions. Unless it is addressed soon, we could reach the point at which no usable evidence could be presented in court because it is indecipherable.

It raises the difficult issue of protecting sensitive technology and sources and methods both in operations and when prosecuting defendants. We must ensure that we have resilient and effective protection and preservation measures. Policymakers have a central role not only in facilitating sharing, but also in promoting adequate protection.

Collaboration in policy development

The UK government places great emphasis on collaboration by public agencies—working together to produce coherent, crosscutting policies (referred to in the UK as "joined up" policies). The overall aim is make policy more effective and produce greater return on the investment of resources. A good example is the unification of crime policy by three UK government departments—the Home Office, the Lord Chancellor's Department[1], and the Attorney General's Offices—into a single, strategic plan and a business plan. The strategic plan sets out seven key crime policy objectives, while the business plan determines how the objectives will be achieved. The "whole system" approach is aimed at—

- Increasing efficiency.
- Improving the confidence of the community as a whole, but especially ethnic minority communities, in the criminal justice system.
- Creating better employment/promotion opportunities for ethnic minority staff with the police and other criminal justice agencies.
- Appropriately integrating policy change into operational and financial planning.

- Making the best use of resources based on “what works” in achieving aims and objectives.

- Increasing the proportion of offenders who are apprehended and either cautioned or convicted.

- Tackling the causes of crime, such as substance abuse.

Managing technology development

In managing technology development, policymakers must first ask whether new technology can be introduced with existing legislation or whether new legislation is needed. In the latter case, the earlier this step is initiated the better.

The key to successful technology projects is to identify the stakeholder and user communities and then persuade them to develop and agree on their operational requirements. Unless this is done, there will be no customer “ownership” and acceptance is likely to be minimal.

The project needs to be controlled and directed by a steering committee consisting of the stakeholders and representative of the user community. Of course, a project planning methodology is needed if there is to be reasonable confidence that all interested parties will produce what is wanted (with attention to such issues as reliability and affordability), when it is wanted.

Selected Technology Policy Goals

The Home Office is focusing on policy initiatives related to the use of several new and newly emerging technologies.

Full interoperability in voice communications

With respect to communications technology policy, the goal of the Home Office is to move from the current system, in which police, fire, and ambulance services all have separate analogue radio systems, to an integrated digital communications network connecting them all, with all operating shared emergency call centers. The benefits of the Public Service Radio Communication Project (PSRCP) are projected as follows:

- Officers will be able to communicate with base wherever they are in the field.

- Officer safety will increase because all communications will be encrypted.

- The time patrol officers spend in the station on paperwork will be reduced by 37 percent.

- New features will include telephones, mobile access to national police databases, and image transfer capability.

- Transmission interference and dead spots will decrease; more capacity will be accessible to cope with peak demands.

To implement the policy, the Home Office first obtained input from the Association of Chief Police Officers, which reviewed its future needs for communications and then defined its user requirements. Implementation of the PSRCP is based on the TransEuropean Trunked Radio (TETRA) Standard, operating in the 380–400 MHz band. Project definition was completed in 1998, pilot trials were completed in 1999, the main contract was signed in 2000 for UK-wide implementation, and rollout across the country is expected to be completed by 2003.

Integrity of digital images

New technologies for digital imaging, including video imaging, are now being used by the police, and digital images are being presented as evidence in court. Some concerns have been raised, however, about the integrity of this evidence. How do we know, for example, that the image is the original, not one altered to make changes impossible to detect?

A committee of the House of Lords recently examined the issue and made recommendations intended to reduce uncertainties about the validity of digital images. Some of the key points of these recommendations, which have largely been accepted by the government, are as follows:

- Digital CCTV systems are covered by the Data Protection Act (2000).

- Data matching systems (for example, those that identify and track individual offenders) are adequately covered by the Act.

- The Act also strengthens the available judicial remedies if a data controller does not comply with its provisions.

- The use of authentication techniques is encouraged. Work is under way to develop standards, guidelines, and procedures for digital imaging that will ensure the acceptability of this type of evidence in court.

- Consideration is being given to legislation requiring "type approval"[2] of digital imaging equipment used to record evidence for enforcing traffic laws and taking fingerprints.

- Evaluating the performance of digital cameras, scanners, printers, and image formats and assessing verification and handling protocols will yield a better return on investment in these technologies.

- Improved digital enhancement techniques are needed, particularly for video, for better intelligence. It is essential that they be developed in a way that ensures the integrity of the product (including maintenance of an audit trail).

Acceptability of digital evidence

The primary source of digitally acquired evidence is theoretically the computer memory chip or hard disk. However, it seems unreasonable to expect that the chip or disk would be bagged for evidence when a digital copy is identical in every respect to the original. In *Garton* v. *Hunter* (1969, 2 QB 37), Lord Denning made a statement about the "best evidence," as follows:

> That old rule [defining the primary source of evidence] has gone by the board long ago. The only remaining instance of it that I know is that if an original document is available in your hands, you must produce it. You cannot give secondary evidence by producing a copy. Nowadays we do not confine ourselves to the best evidence. We all admit relevant evidence. The goodness or badness of it goes only to weight, and not to admissibility.

In England and Wales, if an original document no longer exists, copies or even copies of copies are admissible as evidence (*R* v. *Wayte* [1938] 76 Cr App Rep 100). It is irrelevant that the original was destroyed by the person who sought to introduce the copy as evidence. There have been rulings in Australia to the effect that the first copy made on transportable media becomes the best evidence.

The best guarantee of authenticity is correct handling procedures and a well-documented provenance. If anything, digital evidence is capable of providing a better provenance than an analog recording. Assuming it is possible to demonstrate to the court that the handling procedures and protocols are as good as or even better than for analog recordings, the risk of rejection is low. Extra weight could be accorded to evidence that has used authentication techniques and whose handling and security can be documented.

Automated facial identification

There is a great deal of interest in a range of applications for automatic facial identification technology, including incorporating it into public CCTV systems to identify offenders. The technology has been a long time in the development stage but now a number of vendors are selling it. There is a good deal of "hype" about the performance of this technology, but not much data are available yet from field trials. What has emerged thus far about performance suggests this is a technology to keep an eye on:

- Currently, the technology does not work reliably on "uncontrolled" images (for example, those from public CCTV systems or cameras at football matches), because the image is usually too small and the lighting and angle of view vary considerably.

- The technology works fairly well on "controlled" images (for example, where access is gained via a combination of a PIN and an auto facial ID) and should work in conjunction with mugshot database comparisons.

Vehicle crime

The UK government has set as a high-priority policy goal the reduction of vehicle crime by 30 percent over the 5-year period from 1999 to 2004. To achieve this goal, the Home Office has drawn up a strategic plan that brings together the following agencies and interests:

- Home Office Crime Targets Task Force.
- Association of Chief Police Officers.
- Vehicle manufacturers.
- Insurance industry.
- Department of Environment, Transport and Regions.
- Department of Trade and Industry.

The areas in which technology can contribute are as follows:

- Increasing the security of new vehicles (by installing factory-fitted security devices, including immobilizers and alarms).

- Increasing the security of older vehicles (by retrofitting security devices and using visible vehicle identification numbers).

- Marking parts (to determine whether components are stolen).

- Developing better standards for vehicle locks and windows.

- Securing license plates (assigning unique identifiers to deter theft, prevent uninsured vehicles from being driven, and recover stolen vehicles).

- Sharing best practices via the Internet.

Property tracking

Property crime accounts for more than 90 percent of all crime recorded in the UK. This fact has spurred manufacturers to produce tracking, identification, and tagging systems for crime prevention in addition to stock control. They are now looking to "total asset visibility" (also called "chipping of goods") using new, highly miniaturized property tags. Industry is considering investing heavily in this technology to benefit from better management of assets throughout the supply chain. This development will spawn a vendor base of tag suppliers, systems integrators, and related software.

The police can benefit because the technology aids in recovering and identifying stolen goods. To maximize benefits, the police need to influence the direction in which tag technology is moving. The key policy goal is the establishment of national and international standards for tags so that a single tag reader can read all types of tags produced.

Now is the time to pursue the opportunity to influence industry. The Home Office is accelerating an industrywide initiative on chipping of goods so that manufacturers, logistics providers, retailers, and police agencies can be involved in developing the technology, testing it, and gaining user confidence in it.

Notes

1. The Lord Chancellor's role is the administration of justice in England and Wales. The office is responsible for managing the courts; appointing judges, magistrates, and other judicial officeholders; and administering legal aid. It also has oversight of a varied program of government civil legislation and reform in such areas as family law, property law, defamation, and legal aid.

2. "Type approval" refers to the requirement of Home Office approval before a particular type of equipment can be put into operational use.

Commentary by Jennifer M. Granholm
Attorney General, State of Michigan
Lansing, Michigan

Criminal Use of Technology

The issues discussed in the paper by Caliber Associates are appropriate and comprehensive from the standpoint of identifying new technologies that may be useful in traditional law enforcement. However, the paper does not address new technologies used by criminals or the technologies and practices that law enforcement needs to respond to them. An example of such a new technology is the Internet, which presents challenges because of the anonymity of users and the difficulty of tracing them. Fortunately, there are also high-tech tools available to help law enforcement respond, to ensure the public is protected.

The Internet creates opportunities that never before existed for like-minded criminals to find each other, congregate in chatrooms, and seek social reinforcement in their antisocial behavior. The effects of this phenomenon have not yet begun to be understood or even measured. The Internet also creates a vast pool of potential victims, and can transform what is merely a local scam into a crime that is potentially international in scope. In light of this new technology, the imperatives for law enforcement are to develop legal processes capable of regulating unlawful conduct on the Internet and to devote resources necessary for training and equipment. New legal processes must be developed to overcome the jurisdictional problems and meet the investigative challenges raised by the Internet. In developing these processes, we must also protect privacy, from both unconsented and commercial use of personal information and from criminal theft of such information.

Deployment Issues

From the standpoint of applying new technology, the most important issues are affordability and training. Budgetary realities mean that criminal justice agencies cannot even consider acquiring a new technology unless financial resources are available to pay for it. Training is also crucial because it will have a synergistic impact on the acceptance, interoperability, and deployment of the technology in a manner that respects civil liberties, including the right to privacy, and takes into account safety and other liability issues. Specifically, policymakers must make it a national priority to provide funding for training investigators in the areas of computer forensics (the retrieval of digital evidence stored on computers) and network investigations (the tracking of criminals using Internet tools and the interpretation of such network evidence as server logs).

The Role of the State Attorneys General

As the chief legal officer of the State, the Attorney General is uniquely positioned at the intersection of the criminal and civil administration of justice, interacting with the courts, the corrections system, and the executive branch of government. This perspective enables the

Attorney General to have a very broad perspective on law enforcement needs and to understand how those needs affect the rest of the government and the public.

With respect to technology, the office of the Attorney General should serve as a laboratory of experimentation and creativity. Different technologies can be tested in the widely differing circumstances of each State. This decentralized approach is the best way to tailor technology to the needs of each State, rather than relying on an overall "master plan."

Role of the Federal Government

The Federal Government should be responsive to the States and local governments by listening to their needs and helping to meet them. It can do so by helping fund technologies and training, particularly through pilot projects designed at the local level and based on locally identified needs. The vast information-gathering and -processing capacity of the Federal Government should be used to help State and local governments obtain complete, up-to-date information that can help them make policy development decisions. The Federal Government should recognize the principle of subsidiarity in policy development, giving precedence to bottom-up solutions.