Chapter 5

Other Surveillance Issues: Electronic Physical, Electronic Visual, and Electronic Data Base Surveillance

Chapter 5

Other Surveillance Issues

SUMMARY

Electronic Physical Surveillance

Maintaining physical surveillance of individuals is, traditionally, one of the most expensive and risky surveillance techniques used by law enforcement agencies and others. Portable telecommunications devices are now offering a viable substitute in many cases. For example, electronic beepers emit a radio signal that can be monitored in order to track the movements of a car or piece of property to which a beeper is attached. Also, electronic pagers—increasingly used by busy executives, repair personnel, doctors, and the like-can be intercepted to reveal information that may be useful in determining the subject's location and activity.

OTA found that Federal investigative authorities are making extensive use of beepers for conducting electronic physical surveillance of persons and goods, but limited use of paging monitors. OTA also found that legislated policy on beepers and pagers is ambiguous and incomplete, although the U.S. Department of Justice believes that at least some beeper and pager surveillance applications require a search warrant under judicial interpretations of fourth amendment protections.

Based on criteria used to determine the threat to civil liberties-nature of information, nature of place or communication, scope of surveillance, surreptitiousness of surveillance, and pre-electronic analogy-electronic physical surveillance appears to fall somewhere in the middle. The investigative and law enforcement interest appears to be significant-especially for beepers.

OTA identified three options for congressional consideration: 1) legislate one policy for all forms of electronic physical surveillance; 2) formulate separate policies for beepers and pagers; or 3) do nothing at this time.

Electronic Visual Surveillance

Electronic visual surveillance through the use of cameras is an alternative to physical surveillance. In the past, however, the size, cost, and technical requirements of cameras have limited their effectiveness and usefulness. But the latest generation of cameras is smaller, cheaper, and easier to operate. There already is a significant level of video surveillance of public places, such as the use of closed circuit TV in banks, building lobbies, retail stores, and the like. In addition, video surveillance of private places is used for investigative and law enforcement purposes.

OTA found that electronic visual surveillance-whether in public or private places—is not covered by current Federal law, including Title III of the Omnibus Crime Control and Safe Streets Act. The U.S. Department of Justice does voluntarily comply with some provisions of Title III. Even under Department of Justice guidelines, electronic visual surveillance of private places is considered legitimate and does not require a warrant if one party has consented to the surveillance, even if that party is an undercover agent or informer.

Electronic visual surveillance appears to pose a substantial threat to civil liberties, espe cially if conducted in private places and with audio surveillance. The law enforcement interest varies depending on the stage of investigation.

OTA identified five congressional policy options for addressing visual surveillance:

- legislate that such surveillance is prohibited as an unreasonable search under the fourth amendment;
- subject electronic visual surveillance to a higher standard than currently exists

under Title III for bugging and wiretapping;
- treat electronic visual surveillance in the same way as electronic audio surveillance;
- apply a lower standard; and
- do nothing.

Data Base Surveillance

As computerized record systems and data communication linkages become widespread, the potential for computer-based surveillance of the movements and activities of individuals also increases. Various Federal agencies already maintain computerized record systems that could be used as part of a data base surveillance network. Four examples of such systems are: the National Crime Information Center (FBI), Treasury Enforcement Communications System (Treasury), Anti-Smuggling Information System (Immigration and Naturalization Service—INS), and National Automated Immigration Lookout System (INS).

Federal agencies believe that these and other systems are essential to carrying out their authorized responsibilities. However, the systems could include files on any definable category or type of persons, and could be interconnected with numerous other computerized systems.

Based on the results of the Federal Agency Data Request, OTA identified 85 computerized record systems used for law enforcement, investigative, and/or intelligence purposes with, collectively, about 288 million records on 114 million persons. The Departments of Justice and Defense have by far the largest number of systems and records. None of the agencies responding provided statistics on record quality.

Based on a review of technology and policy developments, OTA found that:

- It is technically feasible to have an interconnected electronic network of Federal criminal justice, other civilian, and perhaps even military record systems that would monitor many individual transactions with the Federal Government and be the equivalent of a national data base surveillance system.
- The legal and statutory framework for national computer-based surveillance systems is unclear.
- A central policy issue with respect to computer-based surveillance systems is designing and implementing a mechanism to simultaneously: 1) identify and authorize those applications that have a substantial law enforcement or intelligence value; 2) minimize any adverse impacts on individual rights from authorized use of the systems; and 3) protect against unauthorized and/or expanded use of the systems and the substantial impacts on constitutional rights that might result. Establishment of a data protection board is one option that warrants consideration.
- Other available options, not necessarily mutually exclusive with establishing a data protection board, include: placing data base surveillance applications under Title III of the Omnibus Crime Control Act; requiring congressional approval of specific data base surveillance systems (e.g., by statutory amendment or approval of House and Senate authorizing committees); establishing general statutory standards for surveillance applications; strengthening Office of Management and Budget (OMB) and/or agency oversight roles with respect to data base surveillance; and maintaining the status quo.

PART I: ELECTRONIC PHYSICAL SURVEILLANCE

Introduction

In the past, physical surveillance has generally required around-the-clock agents with backups at various points and has entailed a high risk of detection by the party under surveillance. Monitoring by portable telecommunications devices, or tracking devices, provides a much less conspicuous way of following the physical activities of an individual, a car, or an item, Monitoring by portable telecommunications devices is relatively risk-free in terms of detection. Physical surveillance can be more efficient with the use of portable telecommunications devices. However, electronic tracking may cost more because surveillance can be carried out for a longer period and because of the staff necessary to monitor the information received.

Electronic physical surveillance does raise questions about the rights of individuals under surveillance and the responsibilities of investigative agencies. The availability of new electronic physical surveillance devices to law enforcement agencies is likely to have significant effects on the investigative process. Before the invention of such devices, it was generally assumed that an individual who was engaged in illegal activity was suspicious and was, therefore, aware that someone might be watching. It was also assumed that governmental agents would not invest the resources to watch someone unless they were quite certain that criminal activity would take place. Therefore, it was not thought necessary to legislate restrictions on investigative physical surveillance.

However, these assumptions can no longer be made in an environment that has been changed so dramatically by portable telecommunications devices. It is now easy to attach a beeper to a car or item and follow its movements. Pagers also offer opportunities for monitoring activities. Interception of information destined for pagers that can receive numeric or alphanumeric data could be revealing about the recipient's location or activities. While simple tone-only pagers offer no real surveillance potential, more sophisticated pagers with the ability to receive messages are likely to become commonplace in the next few years. Future paging technology may also be able to function as an electronic mail or data communications terminal. Because of these technological changes, it is necessary to consider whether legislative action is needed to determine when such devices can or should be used for monitoring purposes.

Background

Before analyzing policy issues and policy options, a brief review of the technological development and potential of portable telecommunications devices will be presented to provide a context for the policy discussion.

Pagers

Electronic paging became a possibility in 1949 when the Federal Communications Commission (FCC) allocated three bands of radio frequencies for mobile communications. Those licensed to use these frequencies were considered radio common carriers. Electronic paging did not become popular until the 1960s when the FCC allocated more frequencies, and doctors and traveling salespeople began to use them to stay in touch with the office. In the 1980s, the use of electronic pagers expanded as lawmakers, lobbyists, repair personnel, business executives, and parents began to realize their potential as a means to stay in touch. The number of pagers in use has grown significantly and is expected to increase. In

1976, there were an estimated 424,000 pagers; in 1982, an estimated 2.2 million.[1] Arthur D. Little, Inc., expects that by 1990, 10 million people will carry personal mobile message machines.[2] Arthur D. Little anticipates that public systems will carry 80 percent of paging traffic, and private systems 20 percent.[3]

A number of pagers are available today, and others are in the development stages.[4] Tone-only pagers, which beep or vibrate to inform the wearer to call in, are still the most popular. There are also tone-voice pagers that give the wearer a 12-second voice message. A newly marketed pager uses a 10- or 12-digit liquid crystal to display messages. Such pagers could be used to convey information to the wearer, ranging from phone numbers to stock information to a patient's medical history to a coded message. A device that is presently being developed is the voice-retrieval system for paging. With this pager, the caller's voice message is stored digitally and is retrieved when the subscriber is ready to receive the message. The voice message is broadcast over a regular FM signal or an FM subcarrier signal, as is the case for cellular phones. Another pager in development that is thought to have great market potential is the alphanumeric pager, which displays alphabetical as well as numerical information. Some companies are developing pagers that could print hard copy, thus transforming pagers into pocket data terminals.

As the technology develops, the cost of pagers and the subscription fees are dropping. The size and attractiveness of pagers are also adding to their marketability .-Moreover, the FCC is taking action to expand the market for pagers. Recent FCC decisions will more than quadruple the frequency spectrum available for paging. More paging channels have been allocated to the Private Carrier Paging Service, and paging can also be provided now over FM subcarriers.[5]

A potentially significant effect of recent FCC decisions is the creation of regional and national paging networks. In January 1982, the FCC allocated new frequencies in the 900 MHz band to radio common carriers to develop local and wide-area paging. In May 1982, the FCC set aside one channel at 900 MHz for nationwide paging and two channnels for either regional or national paging, depending on consumer interest. In May 1983, the FCC made all three channels available for nationwide paging. In April 1984, the FCC, on the basis of a lottery, awarded licenses for these three channels. It is expected that a nationwide paging network will be in full operation in 1986.[6] The nationwide networking systems will use satellites and terrestrial phone systems to transmit signals.[7]

Paging radio technology also has enabled the development of automatic vehicle location (AVL) systems. By using the Long Range Navigation system (LORAN-C) of the Department of Transportation, it is possible to locate vehicles based on radio signals sent from the vehicle, to a transmitter, to a base station. With the use of an intelligent modem, information on the location of the vehicle can be communicated to a central points

Beepers

Beepers, also known as "bumper beepers" or "bird dogs, " are electronic transmitters that generate a series of pulses and are used as a tracking device, frequently by law enforcement agencies for covert operations. A series of pulses is transmitted every 2 seconds. Beepers are about 4 inches long and 2 inches

[1] Penny Pagano, "Thousands Heed Beeps From Pagers, " *The Los Angeles Times,* Oct. 20, 1984.

[2] Nell Henderson, "Beepers Said to Link Legions of Area's Workaholics, " *The Washington Post,* Oct. 22, 1984.

[3] Telocator Members Told That Paging to Prosper in the Future," *Telocator Network of America Bulletin,* Sept. 28, 1984.

[4] For a more detailed description of the various pagers and the technology involved see: John G. Posa, "Radio Pagers Expand Horizons, " *High Technology,* March 1983, pp. 44-47, and "Special Report– RCC, " *Broadcasting,* Oct. 4, 1982.

[5] "Telocator Members Told that Paging to Prosper in the Future," op. cit.

[6] "Nationwide Paging, " Information sheet distributed by Telocator Network of America.

[7] F.C.C. Moves Toward National Paging System, " *The New York Times,* Aug. 20, 1984.

"Bob Jane, *'The 'Landsmart' AVI. System, " *Telocator.* August 1983.

wide with a thickness of three-fourths of an inch. Three U-shaped magnets on the bottom of the beeper are covered by a metal "keeper plate" which is sheathed over the magnets when not in use. The metal plate is removed and magnets exposed to attach the beeper to a bumper, underneath a dashboard, or to any metal protrusions. Cars, ships, trucks, and metal containers can be tracked using beepers.

Self-contained batteries supply the power source for beeper transmissions. A remote receiver is used to pick up signals. This receiver can be located in a car, an airplane, or a helicopter, From the air, a helicopter traveling 6,000 feet above the ground can pick up signals within a 250-mile diameter. From the ground in a metropolitan area, a vehicle can pick up signals within a distance of approximately 1 mile.

The beeper receiver can pick up three types of information, The first is directional information that determines the position of a vehicle and the direction it is heading. The second indicates whether a vehicle is stationary or moving. The third involves the relative distance to the vehicle being tracked.

The FCC sets regulations on beeper frequency levels, power ratings, and the like and is involved in the authorization and licensing process for law enforcement use of beepers. The results of the OTA Federal Agency Data Request indicated that 13 Federal agency components currently use beepers, with two other agency components planning such use.

Findings and Policy Implications

1. OTA found that Federal investigative authorities are making extensive use of beepers for conducting electronic physical surveillance of persons and goods, but limited use of paging monitors. Legislated policy for beepers and pagers is ambiguous and incomplete.

The OTA Federal Agency Data Request and discussions with representatives of the Departments of Justice, Treasury, and Defense indicate that investigative authorities are making extensive use of portable telecommunications devices in conducting physical surveillance of persons or goods. Beepers are often attached to vehicles or goods, e.g., shipments of guns, drugs, or materials used in the manufacture of illegal substances. Monitoring of paging devices is not yet a major surveillance technique, in part because they are not thought to be used extensively by persons engaged in illegal activities, except for drug dealers,' and because the geographic range of use is narrow. Both of these features are presently changing. Paging devices would clearly meet the needs of anyone who was trying to make connections to buy or sell goods, or to indicate that a meeting was to take place. Once investigative authorities perceive that paging devices are being used in this way, there will be interest in monitoring them. The development of a nationwide paging system will also make paging devices more attractive to a variety of customers, and also to investigative authorities as a way of monitoring long-distance movements and transactions.

Pagers

Presently, there is no formal executive, legislative, or judicial policy with respect to the interception of pagers for investigative purposes. According to the Justice Department, the protections afforded pagers depend on the type of pager. The interception of "tonal pagers, " emitting only a sound, does not require either a warrantor court order. Title III does not apply because it is not an aural communication; the Foreign Intelligence Surveillance Act (FISA) does not apply because paging is not a data communication. The interception of a display pager is not covered by Title III because it is not an aural interception, but would be covered by FISA because it conveys information in digital form. The Department of Justice's policy is that interception of tonal pagers involves a sufficient invasion of privacy that a court order should be secured prior to interception. Additionally, the Department of Justice believes that users of display pagers have a reasonable expectation of privacy based on the fourth amendment,

"Interview with Maureen Killian, Department of Justice, Sept. 4, 19H5.

and that a search warrant should be obtained under Rule 41 of the Federal Rules of Criminal Procedure. The interception of "tone and voice pagers" would, the Justice Department believes, require a Title III warrant because aural communication is involved.[10]

Beepers

The use of beepers for surveillance purposes has been the subject of two Supreme Court cases. In *United States v. Knotts, 103 S.* Ct. 1081 (1983), the Court ruled that the warrantless monitoring of a beeper was not a search or seizure under the fourth amendment, because there was no reasonable expectation of privacy as the movements being tracked were all public. A year later, in *United States v. Karo, 104 S.* Ct. 3296 (1984), the Court ruled that using a beeper to trail a container into a house and to keep in touch with it inside the house did violate the fourth amendment. The Court found a legitimate expectation of privacy in the house, and what it considered an equally legitimate expectation of privacy that anything coming into a house would do so without a Government surveillance device. The Justice Department policy on the use of beepers follows the Supreme Court's holding, i.e., a warrant is required if a beeper is potentially going to invade someone's privacy. The Department of Justice advises agents to get a warrant for any use of beepers beyond use on a car.[11]

2. Based on the dimensions used to determine the threat to civil liberties as introduced in chapter 2, electronic physical surveillance falls somewhere in the middle. The governmental investigative interest appears to be significant—especially for the use of beepers.

The nature of the information obtained by electronic physical surveillance depends on the device used. The information divulged by portable telecommunications devices varies with the device. Beepers only yield limited information on the location and movements of individuals, cars, or items. Voice pagers and display pagers disclose the content of a message, however brief and cryptic the message might be. Beepers and tonal pagers do not disclose the number of individuals in a location or the activities in which they are engaged.

Electronic physical surveillance does not discriminate between public and private areas, and can be considered intrusive when it allows the monitoring of movements in private areas. Investigative agents who are conducting the monitoring can minimize the intrusion by turning off their devices when parties or objects enter private places.

Electronic physical surveillance casts a narrow net in that it does not involve people who are not specifically under surveillance, unless they are passengers in a car.

It is difficult for an individual to determine whether a beeper has been attached to a car or article. Beepers are easily concealed because of their size. Some may be detected with a metal detector or other sensor; however, one would have to be looking for a beeper in order to find it. It is almost impossible for an individual to detect whether a signal or message that has been transmitted to a pager has been intercepted. It would be relatively easy to warn individuals who subscribe to paging services that the signals and messages received can be monitored by others.

The closest pre-electronic analogy to electronic physical surveillance of public places is physical surveillance on foot or by automobile, while the analogy to surveillance inside private premises is to police undercover work. There has been limited restriction on the use of undercover agents. If they are too aggressive, their case may be dismissed because of entrapment. In general, undercover agents have not been considered an infringement on one's expectation of privacy because an individual is thought to assume the risk of his or her involvement with others. Congress has recently been considering whether such a risk is realistic or if there needs to be some guidance for the types of roles or relationships in which un-

[10] See John Keeney, U.S. Department of Justice, Statement Before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee, Sept. 12, 1984.

[11] Remarks, Fred Hess, Criminal Division, U.S. Department of Justice, OTA Workshop, May 17, 1985.

dercover agents can engage. Although police undercover work is the closest historical analogy, it may not apply in the same way to electronic physical surveillance because it is based on the assumption of risk. It would be difficult to argue that one assumes the risk that one's movements are always being monitored by a beeper. It would not be as difficult to assume that, if one was carrying a pager, one's activities may be monitored. However, use of pagers may decline if this assumption were widely held.

The governmental interest in using electronic physical surveillance will once again vary with the purpose of the investigation, the degree of suspicion, and whether or not other means have been attempted to secure similar information. Use of beepers and interception of pagers occur in all types of investigations, although they are probably used most often in law enforcement investigations. Electronic physical surveillance is used at all stages of an investigation, but is probably most useful in building a record for probable cause. Electronic physical surveillance is more effective and may be less costly than techniques that are less technologically sophisticated.

The accountability of authorities for use of electronic physical surveillance devices is generally fairly low. They are considered tools of routine investigative use, and can usually be authorized by the agent in the field. If a question of privacy invasion is raised by the use of surveillance devices, then authorization should be obtained from agency headquarters. It is possible to build in a method of accountability, such as authorization by a bureau head for a limited period of time with review and reauthorization possible, and standards of accountability based on the stage of investigation and governmental interest.

3. OTA identified three options for congressional consideration with respect to policy on electronic physical surveillance: a) fashion one policy for all forms of electronic physical surveillance; b) design separate policies for beepers and pagers; and c) do nothing at this time.

Option A.–Fashioning a policy for all forms of electronic physical surveillance is an attractive option in that it is not dependent on specific technological devices and, therefore, will set standards and principles for the future as well as the present. However, given the differences in types of portable telecommunications devices and the different ways in which they are used, it may be difficult to design a comprehensive policy for this area.

Option B.—Although pagers and beepers are similar in that they allow more efficient and less detectable surveillance of physical movements, from a policy perspective they are markedly different in that a beeper needs to be attached by investigative authorities, while a pager is used by an individual. This contributes to the degree of suspicion that an individual has about the possibility of being monitored. People who carry pagers can be made aware of the potential for surveillance that these devices allow. The possibility that one's movements may be monitored by a beeper is more remote for most people. Because of differences in the active involvement of investigative authorities and in the possible awareness of targets of surveillance, it may be necessary to treat beepers and pagers separately. At this time, the differences in the type of information that can be gathered by monitoring beepers and pagers would also seem to dictate separate legislation for each.

It may also be necessary to treat pagers in a discriminate fashion depending on the amount of information that the pager receives. This option would be consistent with the present policy opinion of the Department of Justice.

Option C.–Congress could wait to act until the technology progresses, especially in terms of the development of a nationwide paging network. In formulating legislation for the proper boundaries on police undercover work, Congress may want to consider the parallels between traditional physical surveillance and electronic physical surveillance and design policy that is consistent for both.

PART II: ELECTRONIC VISUAL SURVEILLANCE

Introduction

As cameras have become smaller and easier to activate from a distance, they have become more attractive as a tool for watching people and recording their activities. The evidence that can be obtained from electronic visual surveillance, especially if accompanied by audio surveillance, is as complete as investigative authorities could expect. But there are questions about the intrusive nature of electronic visual surveillance, and the circumstances under which its use is appropriate. Electronic visual surveillance, more than any other form of electronic surveillance, reminds people of the specter of Big Brother watching at all times and in all places.

There is presently a great deal of electronic visual surveillance of public places. Banks have cameras running continuously to monitor both the interior teller counters and also the outside automatic teller machine areas. Airports use electronic visual surveillance in a number of places to ensure the security of the passengers and equipment. Many large department stores, as well as all-night convenience stores, use electronic visual surveillance to deter and detect shoplifting and to compile a visual record of activity. Many cities use closed circuit television to survey street corners in high crime areas, subway platforms, and entrances to public buildings. The Federal Government uses electronic visual surveillance at various Federal buildings to monitor people coming and going. Some employers, especially factory owners and those who maintain large clerical pools, use electronic visual surveillance to monitor the activities of workers.

The motivation for this electronic visual surveillance is a heightened concern for security; the result is that people are becoming more and more accustomed to being watched as they carry out their public life. As cameras become smaller, and easier to install and to monitor, their attractiveness as a means of monitoring activities in private places becomes greater. Previously, one could take actions to ensure an expectation of privacy in a private place, e.g., locking the doors and closing the curtains. But, in the absence of legal standards, the only effective barriers against electronic visual surveillance are the limitations of the technology and such limitations are few.

Electronic visual surveillance of public places is not specifically addressed by Federal statutes, although the assumption is that it is legitimate. Electronic visual surveillance of private places is not presently addressed by Federal laws. The Department of Justice has developed policy guidelines on the use of electronic visual surveillance in private places. These guidelines are regarded as requirements for Department of Justice bureaus (FBI, INS, and DEA) and advisory for other Federal investigatory agencies (Bureau of Alcohol, Tobacco and Firearms and Customs). Electronic visual surveillance of private places where one party has consented to the surveillance, even if that party is an undercover agent or informer, is assumed to be legitimate. The Supreme Court has not ruled on the many questions that are raised by using electronic visual surveillance. For example, if Government agents wish to observe private behavior with the assistance of video cameras or closed-circuit TV, must they get a court order as they would for the use of electronic eavesdropping equipment? Can a court, without specific statutory authority, give authorization for new types of searches or does this overstep the legitimate boundaries of judicial policymaking?

No one has accurate data on the extent of the use of visual surveillance, but there is general agreement inside and outside the investigative community that it is increasing. The Department of Justice has indicated that it has used electronic visual surveillance 18 times in the past year for investigative purposes. Other Federal agencies, such as Treasury and Defense, use video surveillance routinely to monitor the traffic at ports of entry or at buildings containing sensitive materials.

The ease with which video surveillance of private places can be used is in dispute. Some argue that the installation and changing of film make its use prohibitive unless there is easy access to the building or room on a regular basis. For example, video surveillance was used successfully in monitoring the activities of the FALN group in Chicago,[12] but the group met in a "safe house" and thus it was easy for law enforcement agents to gain access. Others argue that the miniaturization of cameras and the use of film that is triggered by activity make it easy to install and maintain video equipment. In support, they cite numerous technological developments and an R&D trend that indicates cameras and film will become more attractive for investigative purposes.

Electronic visual surveillance of private places is most often used when one party consents to the surveillance and can either install and monitor the camera or make it possible for others to do so. Under this circumstance, no Title III warrant or judicial intervention is necessary. However, such enhancement of what an undercover agent or informer can witness and testify to may be significantly more intrusive than an agent acting alone, and on that basis might be required to have some form of judicial authorization.

Background

Before analyzing policy issues and policy options, a review of electronic visual surveillance developments will be presented to provide a context for the policy discussion.

The early literature on modern surveillance techniques warned of the great potential offered by hidden television and video cameras. [13] In the 1960s, this was viewed as a threat rather than a reality because the size and sophistication of cameras made it difficult to install, conceal, and maintain them for surveillance purposes. A number of developments have eliminated such problems. [14]

Miniature television cameras equipped with a "charge-coupled device' rather than the traditional bulky television tubes are widely available at reasonable prices. Closed-circuit cameras also make use of this technology and thus can be easily installed. Technological advances have refined the sensor in the charge-coupled device and have made it even smaller and more powerful. It is predicted that miniature cameras will soon be on the market. These cameras could be concealed in anything from a briefcase, to a lamp, to a plant. It would thus be easy for an agent who has even brief access to an area under surveillance to install a miniature camera, leave, and return later to retrieve the film.

Fiber optics also permits the concealment of small cameras with the lens located at the surveillance site and the camera located at a distance. This is possible because of a "light pipe, " a bundle of thin, transparent fibers, which conducts light and visual images from a lens to a camera. With these devices, an agent need only enter the premises once, to install the lens; film changing and retrieval can be done at a distance.

Low light level television technology makes it possible to see in the dark. Such devices have been used in several cities to detect street crime. Infrared television cameras also make it possible to see in the dark by detecting infrared radiation with a camera that *is* sensitive to such radiation or by detecting infrared radiation and converting it to electrical images. The systems can then produce a detailed black and white picture.

The major advance in the area of visual technology in the 1980s is the development of machine vision systems. Such systems combine video and computer technologies to allow computerized analysis of what is being captured

[12] See *United States v. Torres* (**No. 84-1077,** decided Dec. 19, 1984).

[13] See: Alan Westin, *Privacy and Freedom* (New York: *A theneum*, 1967) and Samuel Dash, R. F, Schwartz and Robert Knowlton, *The Eavesdroppers {New* York: Da Cape, 1959).

[14] For a review of the technologies available in the mid-1970s see: David P, Hodges, "Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother'?" 3 *Hastings Constitutional Law Quarterly* 261 (1976).

on the camera. Both the computer hardware, which allows the system to rapidly scan and pick up the coordinates that define the outline of images,[15] and the software, which is derived from artificial intelligence research and enables images to be scanned in relation to preprogrammed patterns, 'G are important to the effectiveness of machine vision systems. Such systems have been used primarily in industry to perform a number of labor-intensive inspection tasks, including: identifying shapes, measuring distances, gauging sizes, determining orientation, quantifying motion, and detecting surface shading.[17]

Although the major market for machine vision systems is thought to be factories, there are other areas in which labor-intensive analysis of films could be done by these systems. '8 One is in defense for verification of treaties or evaluation of reconnaissance films from satellites. [19]Another is in the investigative area where films that are captured through electronic visual surveillance are then analyzed by machine vision systems to differentiate the segments of the film that are relevant to an investigation from those that are not. Use of machine vision systems would drastically reduce what is presently a very labor-intensive part of electronic visual surveillance, and thus might make it more attractive.

Findings and Policy Implications

1. OTA found that electronic visual surveillance is not currently covered by Title III of the Omnibus Crime Control and Safe Streets Act. The U.S. Department of Justice voluntarily complies with some Title III provisions. Some judges have asked for, congressional clarification.

"Marsha Johnston Fisher, "Micro-Based 'Roving' Eye Sifts Motion, " *MISWeek*, Nov. 14, 1984, pp. 1, 42.

[16]Paul Kinnuean, "Machines That See, " *Technology}*, April 1983, pp. 30-36.

'-tJohn Meyer, ''Vision Systems: Technology of the Future at Work Today, " *Computerworld*, May 27, 1985, p. 13.

[18]See: Edith Myhers, "Machines That See, " *Datamation*, Nov. 1983, pp. 90-103, and ''Machine Vision Merges With Process Imaging, " *Electronic Market Trends*, February 1985, pp. 17-19.

"'Da \ 'id Hafemeister, ''Advances In Verification Technology, " Bulletin of the Atomic Scientists, January 1985, pp. 35-40.

The courts have upheld the use of video surveillance for law enforcement purposes in a number of cases. In evaluating the appropriateness of video surveillance, judges have considered the place under surveillance, the evidence already accumulated, and the warrant process used.

In 1981, the Court of Appeals of New York, in *People v. Teicher, 439 N.Y. S.* 2d 846, upheld the use of video surveillance in a case where a dentist was charged with sexually abusing his patients. The judge ruled that the warrant authorizing video surveillance was valid because probable cause was clearly established by the affidavit, the warrant described the place to be searched and things to be seized, the warrant explicitly provided that surveillance be conducted in such a way as to minimize coverage of activities not related to specified crimes, and the warrant gave evidence that there were no less intrusive means for obtaining needed evidence.

In 1981, the Michigan Court of Appeals in *People v. Dezek*, 308 N.W. 2d 652, ruled that a warrant for video surveillance of a restroom in a highway rest area where homosexual activity was suspected was invalid because it did not limit the search to precise and discriminate circumstances.

In December 1984, the Seventh Circuit Court of Appeals handed down the major decision to date on the question of video surveillance, *United States v. Torres.* At issue was the FBI's video surveillance of the Puerto Rican nationalist group FALN for more than 130 hours over 6 months. The Seventh Circuit, in an opinion authored by Judge Richard Posner, held that the courts could authorize electronic video surveillance if they followed the requirements of the fourth amendment's warrant clause, i.e., "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. " In this case, the Government asked for the warrants in conjunction with its application for Title III eavesdropping warrants and followed the Title III requirements. The Court held that:

> A warrant for video surveillance that complies with those provisions that Congress put into Title III in order to implement the fourth amendment ought to satisfy the fourth amendment's requirement of particularity as applied to such surveillance.[20]

The Court went onto state that it did not suggest that compliance with Title III was necessarily required, but said that "we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope. "[21] It is important to note that Judge Posner did not include all of the Title III requirements, i.e., the exclusionary rule, the limitations on which Federal officials could make an application, limits on the severity of the crimes that could be involved, and limits on State and local use.[22]

The Department of Justice policy is to require a warrant analogous to a Title III warrant for electronic visual surveillance that is not in a public place or that is conducted in a nonconsensual situation. The policy is the result of a desire to have evidence as clean as possible, and the view that it is better to get a warrant "just in case" rather than have a judge rule the results of electronic visual surveillance inadmissible at a later date. The Department of the Treasury reports that it follows the Department of Justice guidelines for use of electronic visual surveillance.[23]

Although the present Department of Justice guidelines require a warrant analogous to a Title III warrant for electronic visual surveillance, the Attorney General has delegated the authority to authorize television surveillance to a responsible official within the Criminal Division who may authorize the surveillance if he or she:

> . . . concludes that the proposed surveillance would not intrude on the subject's justifiable expectation of privacy . . . If such official concludes-that the surveillance would infringe on the subject's justifiable expectations of privacy, he shall initiate proceedings to obtain a judicial warrant.[24]

In the case of electronic visual surveillance of public places or places to which the public has unrestricted access, the head of each Department of Justice investigative division has responsibility for issuing guidelines for that division.

In 1984, Representative Robert Kastenmeier introduced the Electronic Surveillance Act of 1984 which, in part, would bring video surveillance under the Title III warrant requirements. In this bill, video surveillance is defined as "the recording of visual images of individuals by television, film, videotape, or other similar method, in a location not open to the general public and without the consent of that individual. '[25] In September 1985, Congressman Kastenmeier introduced a separate bill, the Video Surveillance Act of 1985 that deals exclusively with video surveillance.[2G] Other electronic surveillance activities are covered in the Electronic Communications Privacy Act of 1985, also introduced in September 1985.[27]

2. Electronic visual surveillance appears to pose a substantial threat to civil liberties, especially if conducted in private places and with audio (as well as video). The governmental interest varies depending on the stage of the investigation in which electronic visual surveillance is to be used.

Before examining specific policy options, it is useful to examine the policy implications of electronic visual surveillance in light of the principles that appear to have guided surveillance policy to date. Based on the dimensions introduced in chapter 2, electronic visual surveillance, especially when used in conjunction

'{'United *States v. Torres*, No. 84-1077, p. 17 (7th Cir., Dec. 19, 1984).

[21] Id, at 19.

[22] Remarks made at OTA Workshop, May 17, 1985.

[23] Remarks made at OTA Workshop, May 17, 1985. "Department of Justice, Order No. 985-82, "Delegation of Authority to Authorize Television Surveillance. "

[25] H.R. 6343, sec. 8, 3117, c.

[26] See H.R. 3455, Video Surveillance Act of 1985 and U.S. Congress, House of Representatives, Congressional *Record*, Extension of Remarks, Sept. 30, 1985, p. E-4269.

[27] See H.R. 3378 and S. 1667, Electronic Communications Privacy Act of 1985; U.S. Congress, House of Representatives, *Congressional Record*, Extension of Remarks, Sept. 19, 1985, p. E-4128; and U.S. Congress, Senate, Congressional *Record*, Sept. 19, 1985, p. S-11795.

with audio surveillance, poses a great, if not the greatest, threat to civil liberties.

The nature of the information that is gained with electronic visual surveillance is very personal. The information is quite complete, including the content of movements, facial expressions, and nonverbal communications, as well as conversations if audio is used.

Video surveillance can be usefully applied to surveillance of any area. The present controversy is focused on the surveillance of private places. Electronic video surveillance is capable of penetrating the most private places, where curtains are drawn and doors are locked, without leaving a trail.

The scope of a video or closed circuit TV camera is broad. All persons and activities that come in camera range will be filmed. Depending on the area under surveillance, it is likely that a number of people unrelated to the investigation will be covered. In this case, the more private the area to be monitored, the narrower the scope of the surveillance. The scope of the surveillance might be minimized by the use of machine vision systems that could scan the film for the targets of the surveillance or for certain types of motions.

Given the miniaturization of video and TV cameras, it is very difficult for an individual to detect electronic visual surveillance. Again, one would have to suspect that he or she was the target of an investigation and would have to look carefully to locate a hidden camera. Additionally, the present policy of allowing electronic visual surveillance without a warrant if one party has consented raises very serious questions about how the concept of assumption of risk is applied.

The historical analogy would be to undercover agents, although the use of video surveillance is much more powerful in terms of detail and unimpeachability. While the testimony of an agent or informer could always be questioned and needs corroboration, the film would probably be accepted. It is always possible, however, to edit a film to make it more incriminating and some editing may not be detectable.

The governmental interest in using electronic visual surveillance will vary. Video surveillance would be useful in investigations for any purpose, but, given the threats to civil liberties involved, would probably be difficult to justify for investigations to ensure the proper administration of Government programs and investigations of minor felonies and misdemeanors. Given the difficulties of installing and monitoring and the need to have certain basic information, electronic visual surveillance will most likely be used when there is a high level of suspicion. As it is such an intrusive form of surveillance, it would be very hard to justify its use during the early stages of an investigation. Although electronic visual surveillance is more effective and less costly than less technologically sophisticated techniques, the threat to civil liberties involved would seem to require that other techniques be tried first.

The present rules on the accountability of authorities using electronic visual surveillance are not clear. The Department of Justice guidelines appear to leave officials in the Criminal Division some discretion, in that they have to determine if the surveillance would violate an expectation of privacy and hence require a court warrant. Also unclear is the definition of a public place.

3. OTA identified five policy options for addressing electronic visual surveillance—ranging from prohibiting such surveillance as unconstitutional to doing nothing. In formulating policy, the issues of consensual v. nonconsensual visual surveillance and surveillance of public v. private places need to be given careful consideration.

The five policy options are discussed below.

Option A.–The first option is to legislate a prohibition on electronic visual surveillance be cause Congress considers it an unreasonable search under the fourth amendment. The basis for choosing this policy option might be the assumption or belief that electronic visual surveillance is an inherently unacceptable form of surveillance because: 1) the information it secures is so complete and specific; 2) it can pick up the most private activities in hereto-

fore private places; 3) it captures the activities of people not under investigation; 4) it captures the unrelated activities of the targets; 5) it is very difficult to detect, and 6) its pre-electronic analogy, i.e., undercover agents, is also regarded as intrusive.

Option B.—The second policy option is to regard electronic visual surveillance as more intrusive and invasive than eavesdropping, but not unacceptable in all circumstances. The legislative option then would be to subject electronic visual surveillance to higher authorization standards than exist for bugging and wiretapping under Title III. This option would be especially applicable in four areas. First, new minimization standards or a new concept to restrict the scope of the invasion, in terms of both place and content, might be developed. Additionally, the list of crimes and circumstances for which electronic visual surveillance is considered appropriate might be developed independently of the list for wiretapping. Third, the use of video surveillance might be restricted to only very sensitive and important types of investigations. Lastly, documented exhaustion of other techniques might be required.

Option C.–The third policy option would be to treat electronic visual surveillance in the same way as electronic audio surveillance. The advantages of this are that visual surveillance is generally conducted with audio surveillance so that only one warrant would be necessary, and that Title III is a known and tested procedure. The disadvantage is that the use of both audio and video may pose a greater risk to civil liberties.

Option D.–The fourth policy option would be to apply a lower standard to electronic visual surveillance than to eavesdropping. This would be hard to justify, given the principles that appear to govern the use of surveillance. It could only be justified if video surveillance were being used alone.

Option E.–The fifth option would be to do nothing. The disadvantage of this option is that both Judge Posner's request to Congress to deal with the issue and the questions raised with the existing Department of Justice guidelines would remain unanswered in terms of legislated policy.

PART III: DATA BASE SURVEILLANCE

Introduction

A significant implication of widespread computerized record systems and data communication linkages is the increased potential for computer-based surveillance of the movements and activities of individuals.

In modern society, most persons leave a trail of transactions with various institutions—governmental, retail, financial, educational, professional, criminal justice, and others. Before the widespread use of computer-communication systems, linking various kinds of transactions was very difficult, if not impossible, since transactions were paper based and the cost of matching or linking paper records was prohibitive. In addition, the time delay inherent in paper linkages would negate much of the potential surveillance value.

Computer-based record systems and electronic linkages make it possible to overcome the cost and time barriers associated with paper systems. In theory, the technology permits the instantaneous linkage of a large number of record systems that would capture and consolidate, for example, gasoline credit card transactions, telephone calls, retail credit card transactions, bank card transactions, and transactions with Government agencies. Thus, electronic linkages could be used to conduct surveillance of individuals who are of investigative, law enforcement, and/or intelligence

interest to the Government. This assumes, of course, that the Government agencies would have electronic access to transactional record information.

Background

One example of a Federal computerized record system that could be used for surveillance purposes is the FBI's National Crime Information Center. NCIC maintains an "electronic bulletin board" of, among other things, wanted persons, missing persons, and persons with criminal history records. Law enforcement and criminal justice agencies make electronic inquiries to the bulletin board to ascertain whether particular individuals are listed as wanted or missing or have a prior criminal record.[26] The process of making inquiries about specific persons also generates information about the location and movement of these individuals and, indirectly by followup with the inquiring officials, more detailed information about the nature of a person's activities at a given point in time.

NCIC is, in effect, a computer-based system for locating persons who are listed as wanted or missing or have a prior criminal record. Until 1982, with one exception, NCIC was not used for intelligence purposes, that is, for locating individuals not having a formal warrant outstanding and/or a formal criminal record. The one exception was during the the early 1970s, when the FBI made very limited use of NCIC to keep track of, for example, bank robbery suspects. The objective here was "to enable law enforcement agencies to locate, through NCIC, individuals being sought for law enforcement purposes who did not meet the criteria for inclusion in the NCIC wanted person file. "[29] In other words, NCIC was being used to track individuals who had not been formally charged with a crime and did not have an outstanding warrant for a Federal offense or other extraditable felony or misdemeanor offense.

The early 1970s (actually April 1971 to February 1974) pilot project had not been authorized by Congress. From then until 1982, the FBI rejected all requests or proposals for intelligence use of NCIC. However, in 1982 the Department of Justice and FBI approved a U.S. Secret Service proposal to establish an NCIC file on persons judged to represent a potential threat to Secret Service protectees. That Secret Service file is now fully operational, and includes the names of about 125 persons judged by the Secret Service to represent substantial threats. Apparently, according to FBI Director William Webster, the file has been quite useful in helping the Secret Service to keep track of (i.e., maintain surveillance on) the location and movement of a significant number of these persons.[30]

During the past 2 years, several other proposals for intelligence use of NCIC have been discussed, although none has been approved. For example, suggestions have been made to add new NCIC files on white-collar crime suspects and suspected organized crime associates.

Beyond this, the already existing electronic linkages between NCIC and other Federal law enforcement communication systems (e.g., the Treasury Enforcement Communication System, or TECS) easily could be extended to other Federal criminal justice record systems and even to Federal noncriminal justice record systems.

TECS is a good example of the extensive electronic linkages already in place. TECS includes a wide range of information on persons that are suspected of or wanted for violations of U.S. Customs or related laws, including persons suspected of or wanted for thefts from international commerce, and persons with outstanding Federal or State warrants. TECS includes the same kind of information on sus-

[28] For further discussion of NCIC, see OTA, *Assessment of Alternatives for a National Computerized Criminal History System*, October 1982.

[29] Letter from Harold R. Tyler, Jr., Deputy Attorney General, U.S. Department of Justice, to Senator John Tunney, Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Oct. 29, 1975.

[30] Statement of William Webster, FBI Director, at Oct. 17, 1984, NCIC Advisory Policy Board Meeting.

pects that has proven so controversial when proposed for NCIC. Of course, TECS is not accessible on-line to tens of thousands of State and local law enforcement and criminal justice agencies, as is NCIC. Nonetheless, TECS is accessible to numerous Federal agencies (plus two foreign agencies), as indicated in table 7.

The so-called Border Enforcement System is the major component of TECS. Computerized information from this system is used, among other things, to: assist U.S. Customs and the Immigration and Naturalization Service personnel screen persons and property entering and exiting the United States; alert Customs and INS officers to potentially dangerous persons or situations; provide investigative data to Customs or other agency law enforcement or intelligence officers; and aid in the exchange of data with other Federal, State, or local law enforcement agencies.

As of May 1, 1985, the TECS Border Enforcement System included computerized records on over 2 million persons. Table 8 gives the distribution of the record sources.

One of the TECS users and record sources is INS. INS, in turn, has its own extensive computerized law enforcement, investigative, and intelligence systems, with records on, collectively, several tens of millions of persons. Highlights of several of the INS computerized record systems are presented in table 9.

Again, two of these systems–Anti-Smuggling Information System and National Automated Immigration Lookout System—include information on suspected as well as known violators. And one of the major purposes of these two systems is to monitor the movements of suspected violators.

Other Federal agencies maintain similar computerized record systems. Based on the results of the Federal Agency Data Request, OTA identified 85 computerized record systems operated by Federal agencies for law enforcement, investigative, and/or intelligence purposes. Out of 142 agency components responding, 36 (or 25 percent) reported the use of at least one such computerized system. Collectively, the 85 systems include about 288 million records on about 114 million persons. (Note that some systems may overlap with multiple records on the same persons, and some agencies did not know or did not provide the number of records and persons per system. Nonetheless, the overall results provide the most complete accounting of such systems to date.) The Departments of Justice and Defense have by far the largest number of systems and records. Justice reports 15 systems with, collectively, about 241 million records on 87 million persons. Defense reports 18 systems with about 29 million records on 22 million persons.

Table 7.—Treasury Enforcement Communication System/ Border Enforcement ,System Users

- U.S. Customs Service
- Bureau of Alcohol, Tobacco and Firearms
- Immigration and Naturalization Service
- Federal Bureau of Investigation
- U S. Marshals Service
- Interpol (International Police Organization)
- Drug Enforcement Administration
- El Paso Intelligence Center
- Internal Revenue Service
- U.S. Coast Guard
- U.S. Department of State
- National Narcotics Border Interdiction System
- Royal Canadian Mounted Police

SOURCC U S Customs

Table 8.—Source of Treasury Enforcement Communication System/Border Enforcement System Records

Source	Number of records
U.S. Customs Service	897,963
Immigration and Naturalization Service	32,828
National Narcotics Border Interdiction System	959
National Crime Information Center	220,693
U.S. Coast Guard	2
Internal Revenue Service Inspection	6,102
Internal Revenue Service Criminal Investigation	100,692
Drug Enforcement Administration	114,387
Bureau of Alcohol, Tobacco and Firearms	712,720
Royal Canadian Mounted Police	22,022
U.S. Department of State	19,721
Interpol	49,699
Total	2,177,788 records (on 2,153,888 person)

SOURCE U S Customs as of May 1 1985

Table 9.—Selected INS Computerized Record Systems

Name of record system	Contents	Number of records	Number of persons
Anti-Smuggling Information System (ASIS)	Known or suspected alien smuggling operations	750,000	unknown
Central Index System (CIS)	All aliens and naturalized citizens except temporary visitors	152,000,000	21,000,000
Non-Immigrant Information System (NIIS)	All temporary visitors to U.S.	24,000,000	24,000,000
Student School System (STSC)	All foreign students and schools they attend	*750,000*[a]	687,000
National Automated Immigration Lookout System (NAILS)	Known or suspected violators of INS laws and other Federal statutes	*40,000*	*40,000*

[a]87,000 persons plus 18,500 schools

SOURCE Immigration and Natural ization Service, based on June 1985 response to OTA Federal Agency Data Request

OTA also asked agencies for any statistics on record quality (completeness and accuracy) for such systems. No such statistics were provided by any of the 142 agency components responding. The four specific examples noted earlier illustrate the already extensive development of computerized data base systems operated by Federal agencies for law enforcement, investigative, and/or intelligence purposes. Federal agencies believe that these systems are essential to carrying out their authorized responsibilities. However, the systems are capable of including files on any definable category or type of persons, and are capable of interconnection with numerous other computerized systems. As a result, these systems (and others like them) provide the technical infrastructure of a data base surveillance system.

Findings and Policy Implications

1. It is technically feasible to have an interconnected electronic network of Federal criminal justice, **other civilian, and perhaps even military record systems that would monitor many individual transactions with the Federal Government and be the equivalent of a national data base surveillance system.**

For example, the current Secret Service file on NCIC could be extended so that the list of dangerous persons would be checked against not only NCIC wanted person and criminal history inquiries, but also social security, food stamp, and other kinds of inquiries or record transactions that would indicate the location or activities of listed persons. This scenario could be further extended to include travel and credit card transactions and the like.

Of course, these are hypothetical examples at this point in time, but serve to demonstrate the vast technical potential for computer-based surveillance inherent in record linkages among computerized systems. These kinds of potential applications raise numerous issues, ranging from whether the application would be cost effective and serve a significant, useful, and lawful criminal justice purpose to the possible implications for civil and constitutional rights.

For example, first amendment rights could be violated to the extent a national computer-based surveillance system was used to monitor the lawful and peaceful activities or associations of citizens or if it were to have the effect of discouraging such activities or associations. Fourth amendment rights could be violated if the surveillance amounted to an unreasonable search and seizure of personal information. And, as a final example, fifth amendment rights to due process could be violated if such surveillance was conducted without first establishing probable cause or reasonable suspicion and without serving advance notice on the subject individual.

The possible civil liberties implications would need to be balanced against the Government's interest in, for example, enforcing public laws, maintaining social order, and protecting the national security. Thus, the trade-offs could, indeed, be difficult to balance.

2. The legal and statutory framework for national computer-based surveillance systems is unclear.

The systems would appear to be subject to the Privacy Act and perhaps other statutes, depending on the purpose. Law enforcement investigative record systems are exempt from key elements of the Privacy Act, but other record systems would have to establish that surveillance use is a routine use under the Privacy Act, and all such systems would have to publish notices in the Federal Register and withstand the inevitable congressional scrutiny. This would appear to be quite difficult to do, although computer matching was defined as a routine use, apparently with relatively little difficulty. On the other hand, if the surveillance was directed at, say, foreign terrorist activity, the system might fall under Foreign Intelligence Surveillance Act and be subject to little or no public scrutiny. Data base surveillance does not appear to fall under Title III of the Omnibus Crime Control and Safe Streets Act since there would be no "aural" acquisition.

3. A central policy issue with respect to computer-based surveillance systems is designing and implementing a mechanism to simultaneously: 1) identify and authorize those applications that have a substantial law enforcement or intelligence value; 2) minimize any adverse impacts on individual rights from authorized and/or expanded use of the systems and the substantial impacts on constitutional rights that might result. Establishment of a data protection board is one option that warrants consideration.

One policy option that has been proposed from time to time in the United States and has been implemented in other countries is a data protection board. Such a board was proposed in the 1970s with respect to NCIC, and in particular the computerized criminal history **(CCH)** program As early as September 1970, OMB recommended the establishment of a strong "policy control board' that would report directly to the U.S. Attorney General. The board was to include officials from the FBI, the Law Enforcement Assistance Administration (LEAA), and the States, and represent all elements of the criminal justice community. Comprehensive legislative proposals developed in 1974 included an independent Federal Information Systems Board that was to be responsible for the operation and regulation of a national CCH system. On a broader level, several European countries have established independent data protection boards or authorities that have some oversight authority over law enforcement and intelligence systems, as well as a wide range of privacy-related systems (e.g., social services, health, and education).

The institutional placement of such a board or authority would be important. If it were to be a new board within an existing department, its power might be too dependent on that of the department and its character shaped by that department. Additionally, the department might well have interests that might conflict or interfere with the responsibilities of the board. If it were to be a board reporting to the President, it would have added stature and potential influence, but it might easily be politicized, and its visibility and stature might well change with changes in administrations. If the board were to report to Congress, either directly or through a special joint committee, it would be independent of the executive agencies that have stakes in personal information collection and use. It might be less open to partisan uses, but the board might become too removed from the realities of agency operations.

The responsibilities of such a board or authority are also important. Should the board's jurisdiction be limited to some surveillance applications, all surveillance applications, all law enforcement/intelligence uses, privacy-related applications, and so forth? The broader the responsibilities, the larger the necessary size and budget of the board, or, in the absence of adequate resources, the greater the work overload. On the other hand, a broad mandate may be necessary to gain the necessary political support, thus contributing to a better overall understanding of agency technologies and practices and resulting in more effective oversight and better decisions.

Other questions include the size and composition of the board, process of appointments, scope of authority, and extent of decisionmaking v. advisory, research, and/or information clearinghouse responsibilities.

4. Other available options, not necessarily mutually exclusive with establishing a data protection board, include: placing data base surveillance applications under Title III of the Omnibus Crime Control Act; requiring congressional approval of specific data base surveillance systems (e.g., by statutory amendment or approval of House and Senate authorizing committees); establishing general statutory standards for surveillance applications; maintaining the status quo; and strengthening OMB and/or agency roles with respect to data base surveillance.

One congressional option would be to amend Title III, making data base surveillance subject to the Title III procedural and balancing requirements. Another legislative option would be to amend the enabling statutes of the various individual computerized systems that are or could be used for surveillance purposes (or enact specific enabling statutes where none exist) to require that new surveillance applications must be approved by Congress. The strongest (and most difficult) form of approval would be to require an act of Congress in the form of a further amendment to the enabling statute. Short of that, formal approval of the relevant House and Senate authorizing committees could be required. Alternatively, agencies could be required to give the authorizing committees 60 to 90 or 120 days' formal advance notice, so that an investigation could be conducted and oversight hearings held, if desired.

As an alternative or complement to such congressional notice and/or approval options, OMB'S role could be strengthened by setting up a separate, statutory office within OMB and mandating a minimum staff. However, some of OMB'S other responsibilities may conflict, and it is unclear that such an office located in OMB would or could provide effective oversight. There is also the option of establishing agency staff in the data protection area and/or assigning new responsibilities to the Privacy Officers and/or Inspector General offices.