Chapter 2

New Technology for Investigation, Identification, and Apprehension

In most cases, a suspect enters the criminal justice system as a result of investigation and apprehension by the police. Since the beginnings of organized police work in the early 19th century, technological advances have widened the net cast by police investigations and have improved the ability to identify offenders and capture suspects. Now new technologies are providing police with powerful new capabilities. By improving the abilities of local and State law enforcement agencies to cooperate across jurisdictions, these new technologies may also decrease their dependence on Federal law enforcement agencies.

MOBILE COMMUNICATIONS

The municipal police, as an institution, are a relatively modern invention. They date from 1829, when Sir Robert Peel, then the British Home Secretary, won approval from Parliament for the creation of a metropolitan police force.[1] In the American colonies cities had watchmen who patrolled streets at night to secure life and property and to care for the lights. It was 1844 before the first metropolitan police force was formally organized, in New York. Other major American cities quickly followed suit.[2]

The police walked prescribed beats, isolated from headquarters and without means of communications. Commanders had difficulty supervising their men and responding to emergencies. The establishment of telegraph networks in the 1850s linked police districts to headquarters and, eventually, the beat patrolman to his station house. The call box was initially simply a signaling lever indicating the presence of the officer at his prescribed post. Telephones were put in call boxes in 1880 for two-way communications between the officer on the street and his station house. With the introduction of the automobile and the radio in the early 1900s, an officer was able to cover a substantially larger beat, increase the frequency of patrol, and respond to calls for service.

While much of today's police work is done from an automobile, many large departments also use motorcycles, airplanes, and helicopters. Most departments use both car radios and hand-held walkie-talkies, giving officers substantially more freedom of movement and greater security. Many have also installed mobile digital terminals in police cars. Linked to automated databases, these terminals enable the officer to query drivers' license files and other relevant information systems.[3] Computer-assisted dispatching systems let dispatchers keep track of where officers are and efficiently assign cars to calls.

These technologies have raised some constitutional issues related to a subject rights during apprehension and arrest when an ar-

[1] R.B. Fosdick, *European Police Systems (New* York, NY: The Century Co., 1915). The English police were subsequently referred to as "Peelers" or "Bobbies" in reference to the author of the bill from which they originated. L.A. Radelet, *The Police and the Community* (Beverly Hills, CA: Glencoe Press, 1973).

[2] E.H. Sutherland, *Criminology* (Philadelphia, PA: J.B. Lippincott, 1924), pp. 186-187. Also see Law Enforcement Assistance Adrninistration, Two *Hundred Years of American Justice: An LEAA Bicentennial Study* (Washington, D. C.: U.S. Government Printing Office, 1976). Chicago established its police force in 1851, followed by New Orleans and Cincinnati in 1852, Boston in 1854, and Baltimore and Newark in 1857. J. Rubinstein, *City Police (New* York, NY: Farrar, Straus & Giroux, 1973).

[3] Other systems include the National Crime Information Center (NCIC), which is operated by the Federal Bureau of Investigation (FBI). See G. Lyford and U. Wood, Jr., "National Crime Information Center: Your Silent Partner, " *FBI Law Enforcement Bulletin, No. 52,* March 1983, pp. 10-15 for a discussion of the NCIC system.

resting officer has used computer-provided data that proved to be wrong or obsolete. These questions will be considered further in chapter 5 on constitutional issues related to quality of criminal history records.

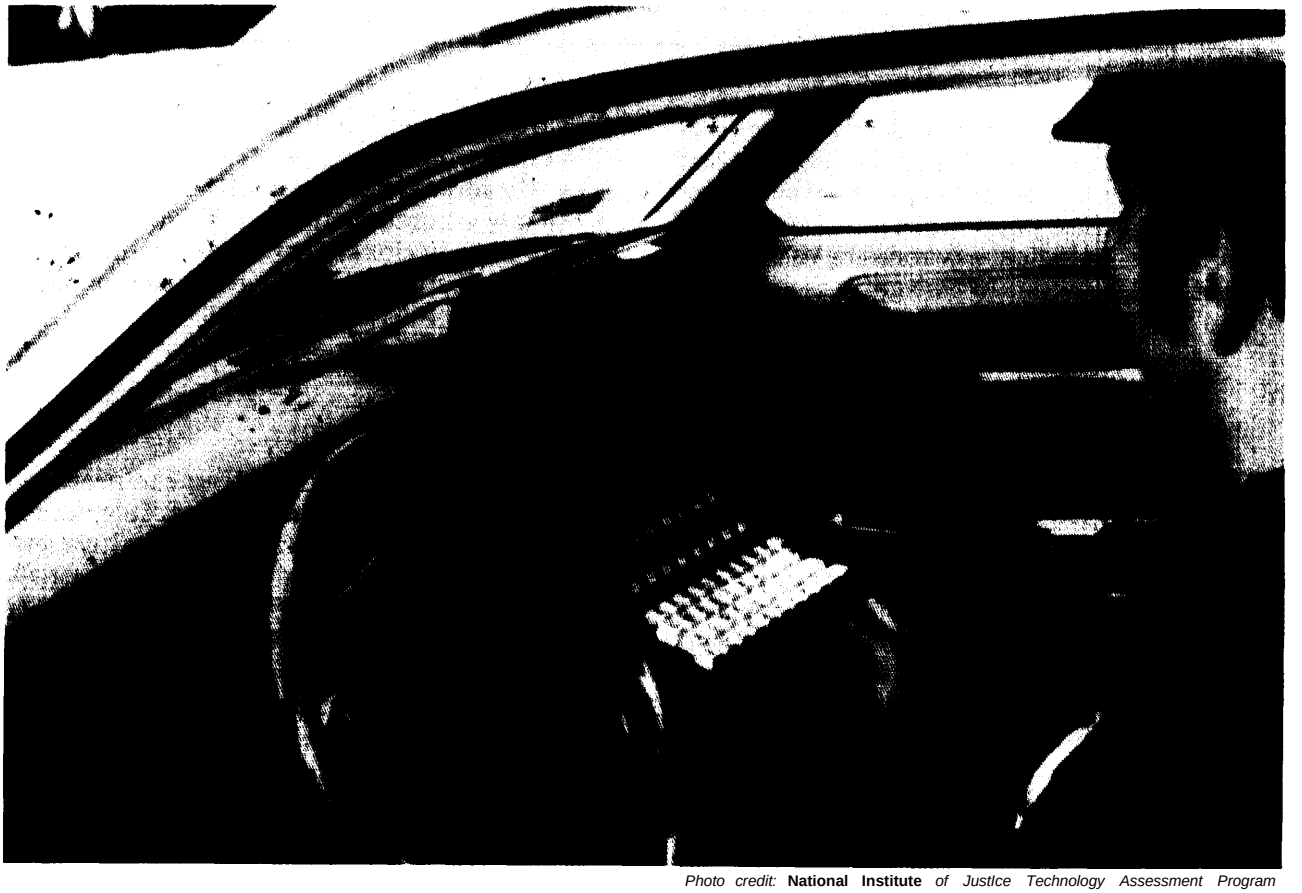


Photo credit: **National Institute** *of Justice Technology Assessment Program*

Digital terminals in police cars allow instant access to computerized databases.

ELECTRONIC SURVEILLANCE

In the last two decades, advances in imaging technology, remote sensing, telecommunications, computers, and related technologies have greatly increased the capability for surveillance of people and their activities. Electronic surveillance includes both sensing techniques and techniques for aggregating and comparing computerized records to reveal additional information about an individual. The Fourth Amendment guarantee of "the right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" has required, and will in the future require, frequent reexamination and reinterpretation in the context of these new means of surveillance, by both Congress and the Federal Courts.[4]

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 extended the existing statutory and judicial principles regard-

[4] Information in this section not otherwise cited comes from the report, U.S. Congress, Office of Technology Assessment, ***Federal Government Information Technology: Electronic Surveillance and Civil Liberties, OTA-CIT-293*** (Washington, DC: U.S. Government Printing Office, October 1985.)

ing privacy to surveillance technology, but at that time this technology still consisted largely of telephone taps and concealed microphones. It now includes many far more sophisticated technologies that can be used to:

1. identify an individual's location or track an individual's movements;
2. monitor and record actions, such as dialing of telephone numbers or automated transactions;
3. listen in on communications or to intercept digital communications;
4. visually monitor behavior; and
5. test or measure reactions and emotions (polygraph testing, voice stress analysis, brain wave analysis, etc.).

Electronic surveillance technologies already in use by Federal law enforcement or intelligence agencies, and by some State and local agencies, include at least the following:[5]

- closed-circuit television;
- light vision systems and image intensifiers;
- parabolic microphones;
- miniature transmitters;
- electronic beepers;
- telephone taps and recorders;
- pen registers;
- computer usage monitors;
- electronic mail monitors;
- cellular radio interception;
- satellite beam interception;
- pattern recognition systems; and
- intruder detector systems working on vibrations, ultrasound, infrared radiation, etc.

Pen registers are devices that are attached to a telephone line to record the dialed pulses by sensing the changes in magnetic energy, thus allowing the interceptor to identify the telephone numbers being called. Parabolic microphone can tremendously amplify sound. Lasers can be used to amplify window vibrations and convert them to audible sound. Night observation devices use infrared radiation or intensify ambient light (e.g., from stars) to the visible spectrum. Image intensifiers allow individuals to be recognized at 100 meters (325 feet).[6]

The surveillance technologies most frequently used bylaw enforcement agencies are undoubtedly still wiretaps and 'bugs, or hidden microphones. In 1986, Federal and State judges approved 754 requests for electronic surveillance, out of 756 that were submitted. This was a drop of 4 percent over the previous year and 6 percent fewer than in 1984.[7] This does not include the 573 wiretaps conducted under the Foreign Intelligence Surveillance Act in 1986.[8]

Wiretapping has been a subject of constitutional challenges for 60 years. The Supreme Court ruled in a 5-4 decision' in 1928 that wiretapping was not contrary to the U.S. Constitution because there was no physical trespass and no search or seizure of physical belongings, and because voice communications projected outside one's house were not protected. Bills were then introduced in Congress to restrict wiretapping, but none passed. Six years later, Congress remodified the 1927 Radio Act. Section 605 of this 1934 Communications Act said that "no person not being authorized by the sender shall intercept any communications and divulge the contents. " Congress may not have intended that prohibition to apply to law enforcement, but the Su-

[5] In 1985, OTA sent a Federal Agency Data Request to all major components within the 13 cabinet-level agencies and to 20 independent Federal agencies, asking about use of surveillance technology, as well as other electronic technologies, The National Security Administration and the Defense Intelligence Agency within the Department of Defense were excluded because the data request results were to be unclassified.

[6] Steve Wright, Program of Peace and Conflict Research, University of Lancaster, United Kingdom, "New Police Technologies: An Exploration of the Social Implications and Unforeseen Impacts of Recent Developments, " ***Journal of Peace Research,*** vol. XV, No. 4, 1978, pp. 5302-322.

[7] "Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications for the Period Jan. 1, 1986 to Dec. 31, 1986, " prepared by the Statistical Analysis and Reports Division of the U.S. Courts, Washington, DC 20544, p. 2.

[8] This information was supplied by congressional staff, to update figures contained in U.S. Congress, House of Representatives, ***Implementation of the Foreign Intelligence Surveillance Act,*** Report 98-738, May 9, 1984, 98th Cong., 2d sess., app. C. In 1983, 549 FISA Court orders were obtained.

[9] *Olmstead* v. *United States, 277* U.S. *438.*

preme Court held in 1938 that it prohibited all wiretapping, even by Federal officials.[10] Bills to allow law enforcement wiretaps with procedural safeguards passed both houses, but did not clear a conference committee before thesession ended. In spite of the Court's ruling, the Justice Department, construing Section 605 differently from the Court, continued to use wiretaps.

Finally, in 1967,[11] the Supreme Court ruled that wiretapping was a "search" under the Fourth Amendment. The Court further held that it maybe "unreasonable" if the subjects have a "reasonable expectation of privacy" in the area or in the activity under surveillance. As to how such an expectation is to be established, the Court has adopted a two-part test based on Justice Harlan's concurring opinion in that case: that the person has exhibited an actual (subjective) expectation and that society is prepared to recognize it as reasonable. This appears to mean that one's privacy is protected if one closes a telephone booth door before speaking (demonstrating an expectation of privacy) but not if one is talking on an unenclosed telephone in a public office. However, the Court also said that the Fourth Amendment "protects people, not places. " This may have been intended to avoid the tie to physical trespass in the 1928 decision, but its full meaning is not clear.

The Court also left unanswered the question of how the Katz decision would apply to other forms of electronic surveillance. The courts have tried to extend the principle of a "reasonable expectation of privacy. " This becomes more and more tenuous in the context of remote sensing devices, but the courts generally have continued to assume that certain places such as residences and yards should have a higher level of protection than other places.

Wiretapping by law enforcement and national security agencies can be done only under certain procedural safeguards, set out in Title III of the 1968 Omnibus Crime Control Act. This law prohibits electronic tapping of conversations except under a court order, when consented to by one participant in the conversation,[12] for certain necessary telephone company monitoring, and (under later amendment) in surveillance allowed by the Foreign Intelligence Surveillance Act of 1978. The court orders must be requested by high-level prosecutors, be related to one of a specified list of crimes, rest on probable cause to believe that a crime has been committed by the target of the surveillance, and be necessary because other kinds of investigation would be ineffective, among other procedural requirements. State officials are also allowed to wiretap under State legislation modeled after the act and for the investigation of specified crimes.

The Foreign Intelligence Surveillance Act of 1978 set standards for use of electronic surveillance in collecting foreign intelligence and in counter-intelligence activities within the United States. It covers not only wiretapping of voice communications, but taps of teleprinters, telegraphs, facsimile machines, and digital communications. The 1978 law also covers radio intercepts and other monitoring devices, such as closed-circuit television and vehicle trackers. In these categories, protection against surveillance is limited to circumstances in which a person has a reasonable expectation of privacy and a warrant would be required if surveillance were conducted for law enforcement purposes.

Two recent Supreme Court cases involved surveillance by means of new technology. In Dow Chemical Co. v. *United States, 1986,* the company contested an action of the U.S. Environmental Protection Agency (EPA). The agency, refused permission to make an on-site inspection of a chemical facility, hired a commercial aerial photographer to make pictures from within lawful navigable air space, without benefit of a search warrant. The Court held

[10] *Nardone* v. *United States*, 302 U.S. 379.
[11] *Katz* v. *United States* 389 U.S. 347, 360.

[12] The Massachusetts Supreme Court recently ruled that the State constitution requires a warrant for electronic surveillance of a private home even when one party to a conversation has consented to its recording and transmission. ***Commonwealth v. Blood*, 507 N.E.** 2nd 1029 (Mass. **1987).** This is an example of more stringent safeguards under a State constitution than under the U.S. Constitution, a not unusual occurrence.

that this was not a search prohibited by the Fourth Amendment, because the commercial facility was analogous to an open field rather than a personal dwelling (in terms of the expectation of privacy) and because EPA was using a "conventional" camera that merely enhanced human vision.

In *California v. Ciraola, argued* the same day, the Court held that the Fourth Amendment was not violated by observation and photography (without a search warrant) of marijuana growing in the garden of a private house, which was enclosed and shielded by fences. The owner of the garden had shielded it from some views, but not from "a public vantage point" where police officers had a right to be, thus the expectation of privacy was not reasonable.

These two cases appear to make the "reasonable expectation of privacy" a function of rapidly changing technology. They seem to say that given more and more powerful surveillance technology there will be fewer and fewer places or circumstances in which one could reasonably expect privacy and in which, therefore, one would be protected against unreasonable searches and seizures, or against surveillance without a search warrant. This makes it likely that there will be further challenges to determine the limits to which surveillance may constitutionally go.

The Electronic Communications Privacy Act of 1986[13] was enacted to extend protection from electronic surveillance to voice and data digital communications, electronic mail and messaging services, and cellular phones, thus expanding Title III protections. Nevertheless, there may already be surveillance technologies not covered by statute, especially when they do not technically require interception of existing communications systems.

[13] Public Law 99-508, Oct. 21, 1986, 100 Stat. 1849-1855.

COMPUTERIZED DATA MATCHING

Computer matching is the computerized comparison of two or more sets of electronic records to search for individuals who are included in both or all sets. It is used in many government agencies to detect fraud, waste, and abuse; for example, the collecting by one person of overlapping or redundant government benefits, where this is not legitimate.[14]

The National Crime Information Center (NCIC) is a criminal justice information database administered by the FBI and used by 64,000 local, State, and Federal agencies. It holds over 19 million records related to convicted, wanted, unidentified, and missing persons, as well as descriptions of stolen articles, vehicles, guns, and license plates. In 1987 the NCIC's Advisory Policy Board (APB) considered proposals to broaden the database in redesigning the NCIC system, to include records of misdemeanors and juvenile offenses, photographs and artist sketches of persons under investigation, DNA patterns, and some other kinds of investigative information.[15] The APB rejected or narrowed some proposals because of their civil liberties implications, but approved concepts for tracking files for subjects of investigations related to drugs, murders, or kidnappings. This would be a major departure since NCIC has so far been a public record system.

[14] U.S. Congress, Office of Technology Assessment, ***Federal Government Information Technology: Electronic Record Systems and Individual Privacy,*** OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

[15] A memorandum on "Proposed Expansion of NCIC" was sent to "interested parties" requesting comments on these proposals, on June 11, 1987, by Congressman Don Edwards, Chairman of the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, U.S. House of Representatives. In response to this memorandum, staff members of OTA'S Communication and Information Technologies Program prepared a Staff Paper on "Issues Relevant to NCIC 2000 Proposals," Nov. 12, 1987, for use of the Hon. Edwards' Subcommittee in considering the Advisory Panel proposals. Results of the NCIC Advisory Policy Board meeting on Dec. 9-10, 1987, when proposals were evaluated, were summarized in a memorandum to Interested Parties, Dec. 16, 1987, from Chairman Edwards.

Proposals were also considered, but rejected, for linking the NCIC with databases operated by the Internal Revenue Service, the Social Security Administration, the Securities and Exchange Commission, the Immigration and Naturalization Service, and the Bureau of Alcohol, Tobacco, and Firearms. These proposals, if accepted, would have allowed wide opportunities to aggregate information about almost any individual through computer matching. The APB did approve on-line linkages to the files of the Bureau of Prisons, the FE I criminal history files, the Canadian motor vehicle registration files, the files of the Canadian version of NCIC, and the "modus operandi" files of the FBI's Violent Criminal Apprehension Program. These linkages should improve the usefulness of NCIC to law enforcement officers without raising serious new concerns about privacy and civil liberties.

The APB-approved proposals must be accepted by the FBI Director, and then will become part of the "user requirements" for redesign of NCIC computers and software in the next 2 years, subject to congressional oversight.

It is probably impossible for statutory law on privacy and civil liberties to keep up with the rapid development or improvement of surveillance technologies and computer data management technologies. Thus Congress and society will be forced by recurring challenges to reexamine and reinterpret the application of Fourth Amendment protections as technology continues to change.

DNA TYPING

DNA (deoxyribonucleic acid) is the basic genetic material, found in every cell of the body. DNA itself is made up of four nucleotides, arranged in two long strands. The order in which the four nucleotides fall along the strand of DNA varies. The chemical structure of the nucleotides (labeled A, G, C, and T) are the same in every person, but the nucleotides are sequenced in a different pattern in each individual; only identical twins have been found to share common DNA patterns. Molecular biologists have developed a test in which the DNA is examined and mapped to determine the sequencing of nucleotides as a method of personal identification.[16] This is called DNA typing; by analogy it is sometimes spoken of as DNA fingerprinting.

Dr. Alec J. Jeffreys, of the University of Leicester in England, working with two other scientists from the British Home Office's Forensic Science Service, first adapted DNA typing for police use. The test quickly proved useful in determining paternity. In the United States, one of the several companies offering DNA paternity tests reports that it has performed 5,000 of them since 1982.[17]

The technique was quickly used in criminal cases. In a multiple rape-murder case in England, a suspect was cleared when DNA typing of his blood and of semen taken from the victims' bodies proved that he could not have been the rapist.[18] Police then urged all men in the community between the age of 13 and 30 to provide a blood sample for analysis. Their theory was that about 60 percent of the samples provided could be eliminated by simple blood tests, and the rest would be subjected

[16] Peter Gill, "A New Method for Sex Determination of the Donor of Forensic Samples Using a Recombinant DNA Probe," *Electrophoresis*, vol. 8, 1987, pp. 35-38. Peter Gill, Joan Lygo, Susan Fowler, and David J. Werrett, "An Evaluation of DNA Fingerprinting for Forensic Purposes," *Electrophoresis*, vol. 8, 1987, pp. 38-44. Barbara E. Dodd, "DNA Fingerprinting in Matters of Family and Crime," *Nature*, vol. 318, Dec. 12, 1985, pp. 506-507.

[17] "Admission of DNA Fingerprints Prompts Queries," *The National Law Journal*, Jan. 18, 1988. In a recent case in England, DNA typing was used to establish maternity. British authorities denied entry into Britain to a Ghanian boy, basing this action on their doubt that the woman claiming to be his mother was in fact his mother. DNA typing "confirmed the relationship because the minisatellites detected by the (DNA) probes are so hypervariable that the chance of a sister of the alleged mother sharing all the maternal specific bands of the child" was extremely remote. See B.E. Dodd, op. cit., footnote 16.

[18] Anthony Schmitz, "Murder on Black Pad," *Hippocrates, vol. 2, No.* 1, January/February 1988, pp. 48-58.

to DNA typing. As the police hoped, however, it was not necessary to examine the DNA of 1,600 men. Even though in England these blood samples could only be acquired on a voluntary basis, one man, in order to clear himself, persuaded a friend to give blood in his place and under his name. The police were tipped off, and the man later confessed to the murders.

In England genetic typing is accepted as conclusive evidence.[19] Its status in the United States is less clear-cut at this time. In a recent case in Florida, a judge admitted DNA "fingerprints" as evidence in a rape case. Scientists testified that semen found in the cervix of the rape victim was "a perfect match" to that of the accused, who could not be identified by the victim and had offered an alibi. The accused man was convicted.[20] DNA prints have also been admitted as evidence by judges in Oklahoma, Florida, New York, and Pennsylvania. According to an Associated Press account, most of the defendants who have been confronted with such evidence have pleaded guilty .21

Experts believe the test will be useful in rape, homicides, and other investigations where blood or semen evidence can often be retrieved. There are problems, however, with DNA typing for police investigations. One of them is that it now takes about 2 weeks. In addition, a relatively large amount of blood or semen is required, which is a difficulty in using the test in homicide and rape cases. In a recent rape case in the District of Columbia, which had to be retried 5 years after the first trial and conviction, a semen sample which had been collected from the victim's body at the time of the crime proved to be both too small and too deteriorated from aging, to be useful.[22] Federal Bureau of Investigation scientists hope that they will be able to overcome these limitations with further development of the technique.

No case involving DNA evidence has yet reached the Supreme Court. Courts have ruled that blood extraction can be compelled, by a warrant, for the purpose of criminal investigations if there is a showing of probable cause. In other words, given the proper procedures using a DNA probe might not necessarily be "an unreasonable search and seizure" under the Fourth Amendment, nor would it necessarily constitute self-incrimination under current precedents.[23] However, as an earlier OTA report has pointed out,

> . . . (t)he more personal or intimate the information that is gathered, the more intrusive the surveillance technique and the greater the threat to civil liberties.[24]

In June of 1987, the Advisory Policy Board of the FBI's National Crime Information Center considered a proposal that records kept by NCIC and used in tracking people who have been accused of crimes or who are missing, be expanded to include the capability for storing, transmitting, and matching the DNA characteristics of these persons, but this proposal was rejected.[25]

---

[19] According to recent news reports; see "having Holmes in the Dust, " Newsweek, Oct. 26, 1987, p. 81.

"'Admission of DNA Fingerprints Prompts Queries," *The National Law Journal* (Associated Press), Jan. 18, 1988; the case cited is *State v. Andrews*, CR87-1659 (Fla. Cir. Ct.).

[21]" Admission of DNA Fingerprints Prompts Queries, " *National Law Journal,* Jan. 18, 1988, p. 42. See also, Kirk Johnson, "DNA 'Fingerprinting' Tests Becoming a Factor in Courts, *The New York Times*, Feb. 7, 1988, p. 1; Alan Dershowitz, "Crime and the Stuff of Life," *Washington Times*, Dec. 8,1987, p. F3; and Janny Scott, "Blood, Semen Tests Likely To Have Greater Use in Court, " Los *Angeles Times, Nov.* 22, 1987, pt. 2, p. 1.

[22] Lee Hockstader, "DNA 'Fingerprinting' Inconclusive in Scott Trial," *The Washington Post,* Feb. 16, 1988, p. All.

[23] *Schmerber v. California*, 384 U.S. 757, 86 S. Ct. 1826, 16 L. Ed. 2nd 908 (1966).

[24] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, 1985), p. 22.

[25] Edwards, op. cit., footnote [illegible]

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS

On February 20, 1978, 48-year-old Miriam Slamovich, a survivor of Nazi concentration camps, encountered a burglar in the bedroom of her San Francisco home. The intruder panicked and shot Mrs. Slamovich in the face. She died a month later. The crime scene investigators assigned to her case had little hope of finding the murderer—Officers Ken Moses and Walter Ilhe had no leads or suspects, only fingerprints left on the windowsill and bedroom window of Mrs. Slamovich's home.[26]

Returning to the police department, Moses and Ihle began the tedious and frustrating process of comparing the latent prints with the thousands of rolled fingerprints cards on file. The odds of finding a match in a database with more than 300,000 prints were remote, but over the next 6 years the officers faithfully spent thousands of hours trying, driven by rage that Miriam Slamovich could survive the brutality of the concentration camps, only to be fatally shot in her own home by an intruder.

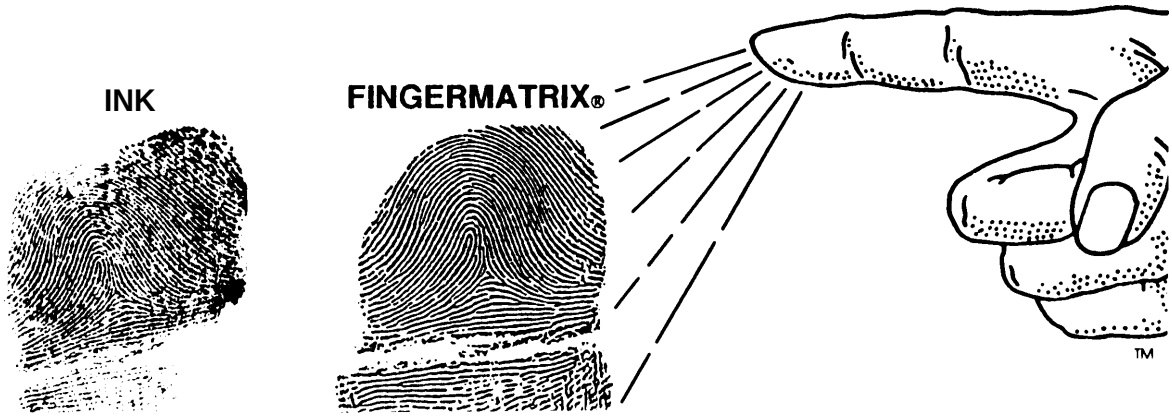
In 1984, the city of San Francisco installed a new Automated Fingerprint Identification System (AFIS). Moses decided to test the latent prints of Mrs. Slamovich's killer, which had been sitting on his desk for 6 years. Once fed into the computer, a match was found in less than 6 minutes. The crime scene prints matched those of Leoncio Saulney, a young computer operator who had once been arrested and booked on a minor trespassing charge. Saulney was arrested, and at first denied ever having been in the Slamovich home; when confronted with the fingerprint evidence, he confessed to the crime and pled guilty to first degree murder.

The newest generation of AFIS has revolutionized fingerprint identification technology.[27] The heart of AFIS technology is the ability of a computer to scan and digitize fin-

[26] This account was provided by the SEARCH Group, Inc., "New Technologies in Criminal Justice: An Appraisal," contractor report prepared for the Office of Technology Assessment, 1987.

[27] There are relatively few publications on AFIS technology. See T.F. Wilson, "Automated Fingerprint Identification Systems," *Law Enforcement Technology,* August-September 1986; U.S. Department of Justice, Bureau of Justice Statistics, *Technology and Policy Issues* (Washington, DC, forthcoming); and *Proceedings of a SEARCH National Conference on Automated Fingerprint Identification Systems,* Kansas City, MO, Feb. 26-28, 1986 (Sacramento, CA: SEARCH Group, Inc., transcript).

Fingerprint Scanner Replaces 90-Year-Old Practice of Inking and Rolling Fingerprints



A proprietary electro-optical system scans and digitizes live fingerprints, eliminating inking and rolling. Ten-print fingerprint cards are generated for standard law enforcement use.

SOURCE: Fingermatrix, Inc., White Plains, NY,

gerprints, to automatically create a spatial geometry or map of the unique ridge patterns and minutiae of the prints, and to translate this spatial relationship into a binary code for the computer's searching algorithm. Making incredibly fine distinctions among literally thousands or millions of prints, an AFIS computer can in a matter of minutes compare a new fingerprint with the massive collections of prints on file and make identifications that previously were possible only through a time-consuming and error-prone process of manual comparison.

This has greatly increased the speed and accuracy of ten-print processing and has made it possible to conduct "cold searches" (i.e., a search where there are no suspects or other identifying information other than the crime scene prints) against very large fingerprint files.[28] The search time in a file of less than 500,000 prints may range from a matter of minutes to about one-half hour.[29]

A somewhat newer development in AFIS is image storage and retrieval, a byproduct of the initial conversion process by which the search print is read into the system in digital form. It allows the digitized fingerprint images to be stored on an optical disk and retrieved later, with the digitized search prints and the retrieved image of the candidate file prints appearing side by side on the operator's screen for comparison. A less costly alternative to image retrieval is a microfilm and microfiche reader.

One AFIS computer cannot search the files of a different manufacturer's AFIS computer, but this is not a big problem. All the AFIS computer needs from another computer is digitized fingerprint image data to make its own search.[30]

Facsimile is used for transmitting fingerprint images from remote sites to the AFIS computer. The facsimile prints must be of high quality to substitute for the inked impressions in the AFIS, but this quality is increasingly available.

Linked photographic and telecommunications technologies are also being used to lift and transmit prints to the AFIS. The use of a remote television camera linked to telecommunications lines is under trial. A device attached to the camera converts the photographic image into digital data and sends the information via modem directly from the crime scene to the AFIS computer at the State central repository. A fingerprint sent by photographic transmission from a crime scene to a central location within a State could be processed instantly, thus allowing an all-points-bulletin to be issued within minutes.

The identification of latent prints by AFIS begins at the crime scene where the fingerprints must be detected and developed.[31] When a finger touches an object, it leaves a residue of water, oils, salt, amino acids, and other chemicals. This latent print will have the ridge patterns and minutiae needed to make comparisons with file prints. However, finger-

[28] Kenneth R. Moses, "A Consumer's Guide to Fingerprint Computers," Identification *News*, June 1986, pp. 5-10.

[29] Proceedings of a SEARCH National Conference on Automated Fingerprints Identification Systems, op.cit., footnote 25. During the search for a match, the computer uses a scoring system that assigns points to each of the criteria set by a technician, who also sets a threshold score above which he has assurance that a match has produced a hit. Thus, AFIS makes no final decisions on identity. While the score may virtually guarantee a hit, only the trained eye of the fingerprint technician will make the final verification. The use of the fingerprint as evidence in court requires the fingerprint technician to prove, by a comparison of measurements and points of minutiae on the latent and file prints, that the prints match. For verification, an AFIS assists, but does not replace, the fingerprint expert.

[30] National Bureau of Standards, *Proposed American National Standard Data Format for the Interchange of Fingerprint Information* (Washington, DC: National Bureau of Standards, Apr. 7, 1986). On Aug. 25, 1986, the American National Standards Institute accepted the standard entitled "Data Format for the Interchange of Fingerprint Information" (ANSI/NBS/ICST-1-1986), developed by the Institute for Computer Sciences and Technology of the National Bureau of Standards (NBS). This NBS standard will probably pave the way for the sharing of fingerprint data among law enforcement agencies in a form that can be utilized by all AFIS systems.

[31] For a general reference on classification, pattern interpretation, latent fingerprint lifting techniques, and other aspects of fingerprint identification work, see U.S. Department of Justice, Federal Bureau of Investigation, *The Science of Fingerprints: Classification and Uses* (Washington, DC: U.S. Department of Justice, 1977),

prints often can not be made visible on certain surfaces. The traditional method of carbon dusting powder requires relatively fresh prints with ample amounts of residue. Powder works well on glass and hard surfaces, but not on paper, fabric, or other porous surfaces that absorb the moisture and salts left by the fingers. Manual identification of those prints meet with little success.

Today, however, a revolution is taking place in the detecting and "lifting" of latent prints, with the use of chemicals and lasers. For example, ninhydrin, an oxidizing agent, activates the amino acids and makes the ridge patterns visible. It works effectively on surfaces such as paper. Other chemicals restore moisture to faint prints, making them more visible. Cyanoacrylate, which is common household "super glue, " attaches itself in its gaseous state to fingerprint chemicals, turns them white, and hardens them. It works well even on fabric and plastic.[32]

Lasers are being used to detect fingerprints on surfaces on which dusting or the use of chemicals has proven ineffective. An intense flood of blue laser light can detect fluorescence in the chemicals found in fingerprint residue, even in very small quantities. The FBI used a laser to detect a fingerprint of a Nazi war criminal on a postcard after 40 years.[33] Lasers are now used mostly in the laboratory, but smaller, more portable units are being tested at crime scenes.

As fingerprint matching becomes a more powerful tool of criminal identification and as matching from large files becomes faster and easier, there will be increasing pressure to expand the files of law enforcement agencies. This is likely to lead to controversies over whether fingerprints that were collected for other purposes should be included in the files. Government employees, military personnel, and juveniles may be routinely fingerprinted for reasons having nothing to do with crime. Congress or the courts may be asked to decide whether this violates the constitutional right to privacy.

The use of fingerprints collected for purposes not related to criminal justice raises the issue of voluntary consent; without this consent the use would be a "search" under the Fourth Amendment. In *Davis v. Mississippi*,[34] fingerprints collected in the course of an unlawful detention were held to be inadmissible in court. The question may also be raised as to whether, under the 14th Amendment's requirement of due process, it would be necessary to tell people that their fingerprints, voluntarily given in another context, were to be used in a criminal investigation.

The broader question, which also applies to the biometric identification systems discussed below, is whether the new technology is making everyone subject at all times to an electronic search even where traditional police searches would require a warrant issued on the basis of probable cause.

[32] Henry C. Lee and R.E. Gaenssien, "Cyanoacrylate, 'Super Glue' for Latent Fingerprints," *The Identification Officer*, spring 1985, pp. 8-11.

[33] T.F. Wilson and P.L. Woodard, U.S. Department of Justice, Bureau of Justice Statistics, ***Automated Fingerprint Identification Systems–Technology and Policy Issues*** (Washington, DC: U.S. Department of Justice, forthcoming), p. 5.

[34] 394 U.S. 721 (1969).

BIOMETRIC SECURITY SYSTEMS

Recent advances in microchip design are being used in devices that verify the identity of persons seeking access to controlled or classified data or to secured areas. They include devices that read fingerprints, palm prints, hand geometry, and voice and retinal blood vessel patterns.[35] One of the early commercially suc-

[35] For general discussions of contemporary biometric technology see M. Thompson, "In Search of Security's Future," *Security World*, vol. 23, January 1986, pp. 26-32; and M. Thompson, "The Newest Wave: Biometric Security, *Security World*, vol. 22, February 1985, pp. 39-43.

cessful devices measures the spatial geometry of the hand (i.e., the length, curvature, and webbing between fingers). Hand geometry data can be stored within a microcomputer attached to the device or on a separate card. The device is currently used in nuclear facilities, government installations, banks, automatic teller machines, and even the cafeteria of a major university.

Other biometric devices read individual fingerprints or palm prints directly from an individual's hand. Some systems can create the standard ten-print fingerprint cards generally used by police departments and the FBI, allowing faster processing and eliminating the mess and smudging of inked prints. A system now under development will use palm prints.

Another innovative strategy relies on the pattern of blood vessels in the retina of the eye, which can easily be seen behind the pupil. The blood vessel pattern appears to be unique to each individual. With one device, for example, a camera scans the retina with a safe, low-level infrared light, which is fed back to a photo sensor. The resulting waveform is then digitized, computer processed, and stored as a signature template for subsequent comparisons.

A system for computerized handwriting analysis, currently under development, would analyze a signature using a variety of characteristics such as speed, pressure, and conformation, and compare it with the authorized signature on file. This technology also has great potential in the commercial world, most notably in banking and the use of credit cards, as well as in crime detection.

Voice recognition systems, though under development for many years, are not yet sufficiently accurate for broad commercial or security uses. Because of the great variability in a person's voice over time and the fact that it can be affected by air quality, physical illness, and mental attitude, the systems remain error prone. Nevertheless, interest in this technology continues.[36] At least two companies have developed voice verification applications for use with electronic monitoring systems. There are conflicting reports about error rates with most of these devices and little can be said as yet about their acceptance by courts.

Scanning technology used in criminal investigations as a way of establishing or verifying identity would perhaps be subject to the same challenges as the matching of fingerprints collected for non-crime-related purposes, as discussed above. However, they are intended primarily to secure entry and access, where their use is governed by contractual agreements between employers and employees, and it is not clear how they may be adapted for identification of criminals.

[36]%. M. Menke, "Voice-Recognition Applications Will Increase in 1987," ***Government Computer News,*** vol. 6, No. 1, Jan. 16, 1987, pp. 44-45. Also see R. Hager, "Breakthroughs Said To Be Ahead for Voice Recognition," ***Government Computer News,*** vol. 5, No. 16, Aug. 29, 1986, p. 40.

"LESS-THAN-LETHAL" WEAPONS

Law enforcement officials recognize that there is a dangerous gap in the range of tools available to them.[37] The use of a weapon is necessary in many confrontations, to stop a fleeing suspect, to deal with terrorist and hostage standoffs, to subdue violent or emotionally disturbed persons, and sometimes for riot control. A nightstick may be inadequate, but use of a gun risks unnecessary injury or loss of life and danger to bystanders as well as to the policeman and the suspect. Ideally, policemen should have a range of non-lethal or less-than-lethal weapons appropriate to such situations.

Some progress is being made in developing less-than-lethal weapons, but it has been hampered by a number of factors. Acceptable limits of risk must be set, since any force used against

[37]Material in this section not otherwise cited, relies on Sherri Sweetman, Report ***on the Attorney General's Conference on Less Than Lethal Weapons*** (Washington, DC: U.S. Department of Justice, National Institute of Justice, March 1987).

a person can potentially hurt or kill. Tolerances vary widely among people, especially in relation to size, health, and drug use. Environmental factors can greatly increase the danger to those against whom a weapon is used.

Less-than-lethal weapons will endanger the law officer when they are at least as reliable, accurate, and easy to use as conventional weapons. Their potential for misuse or abusive use must be minimal, and the weapons must be acceptable to both users and the public. One problem in development has been the need to test and demonstrate the usefulness of the weapons on people.

Less-than-lethal weapons currently being used or under development include:[38]

- electrical devices that deliver a disabling but nonfatal shock–the Taser, the stun gun, and the Talon (a glove with an electrical pulse generator in the palm);
- chemical devices that work either on the central nervous system (e.g., tranquilizers) or peripherally on the body (e.g., tear gas or mace);
- impact devices that include the water cannon or fire hose and various launched soft projectiles, such as rubber bullets, soft rubber rings, bean bags, and small water balloons, some of which may also be filled with chemicals such as mace;
- combinations of the above types might include impact devices that deliver a tranquilizing shot; such weapons are now used by conservation officials in the capture of wild animals for inspection, marking, or treatment;
- marking devices, such as pistols that fire a blob of paint for later identification of fleeing suspects or vehicles; and
- miscellaneous other devices such as explosive light and sound grenades for disorienting people, trip devices, and capture nets.

[38] Some but not all of these devices are described in Sweetman, ibid.

Whenever police kill a suspect or bystander in the process of making an arrest or halting a crime in progress, serious questions arise about the possibility of use of excessive force. This is especially true when the person killed was not guilty of crime, or the crime being committed (or suspected) did not involve direct threat to life, or would not merit capital punishment. Less-than-lethal weapons should thus contribute to protection of constitutional values of law enforcement, due process, and rights of prisoners. That assumes, however, that the new weapons will not be used to exert physical force where it would not otherwise be acceptable—for example, to break up or control "mobs" that are really people exercising their constitutional right of assembly and protest, or to "subdue" suspects that are not really resisting arrest.

When and if nonlethal weapons become effective and widely available, a constitutional challenge could arise regarding the use of lethal weapons; in that situation the use of deadly force by police might be challenged as an unjustified deprivation of life, liberty, or civil rights, as deprivation of due process, or as cruel and unusual punishment. A recent Supreme Court case held that deadly force may not be used unless it is necessary to prevent an escape and then only when the officer has probable cause to believe that a suspect poses a significant threat of death or serious physical injury to the officer or to others.[39] Otherwise, the use of deadly force maybe "an unreasonable seizure" under the Fourth Amendment.

[39] For example, the supreme Court ruled in *Tennessee v. Garner*, 471 U.S. 1 (1985) that use of deadly force in making an arrest, without probable cause to believe the suspect was dangerous, violated the Fourth Amendment prohibition on unreasonable seizures. Previously courts had used a complicated standard based on the 14th Amendment Due Process Clause, inquiring whether the force used caused severe injury, that it was grossly disproportionate to the need for action, and that it was so malicious as to shock the conscious. See for follow-up, Martha Middleton, "Fourth Amendment Rights Are Expanded in Arrests," *National Law Journal,* Oct. 5, 1987.