Les Cahiers de recherches criminologiques

CAHIER NO 9

NOUVELLES TECHNOLOGIES ET JUSTICE PÉNALE
NEW TECHNOLOGIES AND PENAL JUSTICE

XXXVIIIe Cours international de criminologie

Marc LeBlanc
Pierre Tremblay
Alfred Blumstein
(1988)

LES CAHIERS DE RECHERCHES CRIMINOLOGIQUES
CENTRE INTERNATIONAL DE CRIMINOLOGIE COMPARÉE
Université de Montréal
Case postale 6128, Succursale Centre-ville
Montréal, Québec, H3C 3J7, Canada
Tél.: 514-343-7065 / Fax.: 514-343-2269
cicc@umontreal.ca / www.cicc.umontreal.ca

XXXVIIIe Cours international de criminologie
38th International Course in Criminology

NOUVELLES TECHNOLOGIES ET JUSTICE PENALE
NEW TECHNOLOGIES AND CRIMINAL JUSTICE

sous la direction de
under the direction of

Marc LeBlanc
Université de Montréal

Pierre Tremblay
Universités McGill et Montréal

Alfred Blumstein
Université Carnegie Mellon

Montréal, 1988

Sous les auspices de
Under the Sponsorship of

Société internationale de criminologie
Ecole de criminologie et Centre international de criminologie comparée de l'Université de Montréal

Avec la contribution
With the contribution

Ministère de la Justice, Canada
Ministère du Solliciteur Général, Canada
Ministère de la Justice, Québec
Ministère du Solliciteur Général, Québec
Université de Montréal

TABLE DES MATIERES

TABLE OF CONTENTS

TABLE DES MATIERES

PRESENTATION

En 1967, le Département de criminologie de l'Université de Montréal a organisé le XVIIe Cours international de criminologie sur le thème de "La criminologie en action"; il inventoriait les apports possibles de la criminologie au système de justice pénale (Szabo, 1968)[1]. Une année plus tôt, aux Etats-Unis, The President's Commission on Law Enforcement and Administration of Justice[2] publiait le rapport de son groupe de travail sur la science et la technologie; celui-ci proposait un bilan exhaustif des technologies qui pourraient être utilisées dans le système de justice pénale. Depuis cette date, d'une part, les développements ont été nombreux dans le domaine des technologies et, d'autre part, il y a eu une profusion de tentatives pour les incorporer aux opérations du système de justice pénale. Toutefois les bilans qui ont été réalisés jusqu'ici, en particulier aux Etats-Unis, portaient sur des technologies spécifiques; ce que nous proposons, c'est un bilan qui couvre plusieurs domaines technologiques et qui porte une attention particulière aux controverses que les diverses technologies suscitent ou qu'elles risquent de soulever.

Les actes de ce Cours proposent un bilan de trois catégories de technologies:

- les technologies d'identification des individus (tests de sang, et d'urine; analyse des empreintes digitales, vocales et moléculaires, ...);

- les technologies de surveillance électroniques (en particulier incarcération à domicile) et visuelles (vidéo des interrogatoires policiers, des procès, ...);

1- Szabo, D. (1968). Criminologie en action: bilan de la criminologie contemporaine dans ses grands domaines d'application: Montréal, Presses de l'Université de Montréal.

2- The President's Commission on Law Enforcement and Administration of Justice (1967). Task Force Report - Science and Technology. Washington D.C., U.S. Government Printing Office.

- les technologies de soutien, en particulier les possibilités qu'offrent les ordinateurs (micro et macro) pour les opérations policières, judiciaires et correctionnelles et les stratégies de cueillette et de traitement des informations relatives aux crimes et aux criminels.

Non seulement ce Cours voulait-il inventorier les technologies disponibles, mais il a évalué la portée de l'assimilation de ces technologies par le système de justice pénale. Dans cette perspective, les thèmes suivants ont été traités: quels sont la croissance et l'impact des nouvelles technologies? Quels sont les contextes dans lesquels une nouvelle technologie est adoptée et diffusée? Quels en sont les impacts politiques, sociaux et économiques à court, moyen et long terme de ces technologies? Quels sont les risques pour les droits de la personne? Quelles en sont les implications pour les procédures pénales?

Remerciements

La tenue de ce Cours et la diffusion des conférences n'auraient pu se matérialiser sans la contribution de divers organismes et de nombreux individus.

Remercions d'abord la Société internationale de criminologie qui a accepté ce Cours sous son patronage. Ce Cours n'aurait pu être tenu sans les contributions substantielles des Ministères de la Justice et du Solliciteur général du Québec, de l'Université de Montréal et surtout du Centre international de criminologie comparée.

Remercions aussi tous les conférenciers qui ont su intéresse et stimuler les participants. Aussi, il faut noter la contribution essentielle des participants qui par leurs questions et commentaires ont rendu le Cours si vivant.

Remercions aussi le personnel de soutien, secrétaires et étudiants, qui ont garanti le succès de ce Cours sur le plan de son organisation. En particulier, soulignons le travail diligent de Mmes Marie Miville Dechene, Marie-Christine Cohen et Nicole Pinsonneault.

PREMIERE PARTIE

PART I

BILAN ET PERSPECTIVES

OVERVIEW AND PERSPECTIVES

Science and Technology in Support of Criminal Justice

Alfred Blumstein
School of Urban and Public Affairs
Carnegie Mellon University
Pittsburgh, Pennsylvania 15313

I. Roles of Technology

Most people, when they think of the role of science and technology and its contributions to the criminal justice system, think of the many ways in which highly developed forensic techniques have been applied to develop evidentiary proof or identification based on subtle physical evidence, especially when associated with notorious cases. These have certainly been the most dramatic incidents involving technology.

The much more pervasive effects, however, are those associated with more fundamental improvements in the operation of the criminal justice system. Technology can enhance considerably the collection of information through various kinds of surveillance: This includes overt surveillance using video cameras in public areas as well as covert surveillance using concealed receivers.

The most pervasive role of technology in the society generally over the past decade has been the use of computers for processing collected information. The criminal justice system, which deals to such a large extent with the processing of information has participated in that revolution, but not at all as fully as it might have. This undoubtedly reflects some limits

resulting from the lesser level of technical sophistication in the system, and also the ambivalence about pushing information technology to its potential limits.

Advanced information processing, in combination with various mathematical and computer planning models have been used to develop improved methods for consideration of alternative tactics and strategies for improved resource allocation and for increased efficiency in the operation of criminal justice agencies, particularly police. These developments have capitalized on new management technologies developed for other purposes as well as the enhanced data bases possible with computerized records. All of this have led to greater use of technologies associated with organizational control and performance.

II. A Twenty-Year Perspective

This conference represents a personal landmark for me. It comes just 20 years after the publication of the work of the President's Commission on Law Enforcement and Administration of Justice[1]. That Commission was created by President Lyndon Johnson in 1965. That was a time when the United States was building its spaceship to land men on the moon, and so it was also a time when the nation saw great hope from the promised contributions of science and technology. In resonance with that atmosphere, the Commission decided that it wanted to establish a

[1]President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society, Government Printing Office, Washington, D.C. 1967.

task force on science and technology, feeling confident that "if science and technology can get a man to the moon, then certainly it must have some important contributions to make in the realm of controlling crime".

The Commission clearly faced a difficult choice in the staffing of that task force. They were either going to choose a lawyer or criminologist and try to develop within that person expertise and awareness of the methods and perspectives of science and technology, or alternatively to seek someone who knew something about science and technology, and give him access to the experts at the Commission who knew all about criminology and the criminal justice system. Clearly the latter course was the only feasible one, and so I was recruited as the Director of that task force.

That was an important and exciting time in my own experience. It is always very exhilarating to move into an area in which you know nothing, and to have the opportunity to learn from the true experts who are so well steeped in the knowledge, the theory, and the practice of that field. One important role of the stranger in such a setting is the opportunity it provides to call attention to the missing "emperor's clothes." The novice is free to ask the astonishingly naive questions about issues that remain imbedded presumptions by those who are immersed in the field. More than others would have liked to hear it, we raised the question of "how do you know" in response to many assertions and presumptions that were part of the conventional wisdom.

Our task force on science and technology, which varied between 5 to 10 staff members over its 18-month life, worked with the other task forces (the major ones were on police, on courts, on corrections, and on assessment of crime). In doing so, we were able to raise a number of such fundamental questions, to propose research strategies, and to identify means by which the tools of technology - but much more importantly the methods and knowledge-development approaches of science - might be used to generate improvements in their operations.

It is intriguing to reflect on some of the changes that have come about in the past 20 years and also on how much has not changed. One normally thinks 20 years as an extremely long interval for the development of technology. Certainly, as an example, the developments in computer technology over the past 20 years have been most impressive - from the large mainframes that had less memory and were slower than the $1,000 personal computers that everyone uses today. But aside from their entry of computers into the criminal justice system, the changes brought about by technology have been less than profoundly dramatic.

In part, this results from the fairly advanced state of relevant technology 20 years ago. That was a time when the technology was readily available for doing almost everything that one might want to do. The only real issue of concern was what was

worth buying rather than what could be done technically. Prices have come down somewhat, but not dramatically. Equipment has become somewhat more miniaturized, but hand-held radios were widely available 20 years ago.

The one striking technological advance has been the introduction of automatic fingerprint identification. In 1967 when the task force report was issued[2], the one problem that had no technical solution - that was not technologically feasible- was automatic fingerprint recognition. That problem has finally been overcome in the last few years, partly due to faster computing speeds and partly due to improved algorithms for processing digitized fingerprint images.

The much more profound changes to the criminal justice process are those associated with the change in the knowledge base about crime and the criminal justice system. In the United States in 1967, the only source of date about crime was that reported by the police to the FBI and published annually under J. Edgar Hoover's "authorship", the Uniform Crime Reports. Those annual reports were regarded very skeptically, especially by the research community, largely because people were convinced that there were profound biases in police recording and reporting practices and in arrest practices. Many dismissed the police reports of increasing crime rate as simply a heavy handed attempt to generate larger police budgets; also, many dismissed the large racial differences in arrests as simply attributable to

---

[2]President's Commission on Law Enforcement and Administration of Justice, Task Force Report: Science and Technology, Government Printing Office, Washington, D.C., 1967

police discrimination against blacks.

The changes in the availability of rich data have been dramatic. A major step forward involved the introduction of the U. S. National Crime Survey, with semi-annual interviews of a panel of about 100,000 citizens asking them about their victimization experience. Having this second data source provided an alternative lens with which to view the obscure crime phenomenon. Even though neither lens is fully satisfactory, and each has its own distortions, having the two lenses provides the opportunity for mutual confirmation and calibration as well as for identifying and isolating sources of error in each. These two sources have been augmented by a third kind of source through various self-report studies. The National Youth Survey, conducted by Delbert Elliott and his colleagues, for example, has provided self-report information on almost 2000 youth drawn from in a national probability sample. These data, collected for research purposes, are more limited and more specialized than the other two series, but they do provide an indication of materials that could represent a third independent and very different lens that could be used for calibration of the other two.

The state of theory in 1967 was as weakly founded as the data sources. There were certainly a rich array of competing theories, but none of them was empirically grounded and none provided clear testable and refutable hypotheses. Of course, all made reasonable sense and were reasonably consistent with

intuition - provided one were sufficiently flexible in the interpretation of the imbedded constructs. On the other hand, none seemed to provide important new insights that had not already been widely believed. It was clear to those of us coming from the perspectives of science however, that this state of theory was not very satisfactory. It was clear that empirically grounded theory could not be developed very well until better data could be collected, and better constructs derived from those data.

Since the use of computers was growing rapidly, one of the dominant concerns of the time was that these new machines would collect all minutia of data about every individual, link them all together, and lay us all bare to the predations of the most inquisitive gossip. The concerns were sufficiently deep that at least half the time of the discussions between the task force on science and technology and its policy advisory group was devoted to developing methods and procedures that would assure that the intrusion of individual privacy would be limited. It was during that time that the construct of an index was developed, very much like the one being implemented in the United States today.

There were some technologies that were available and were being discussed at the time, but that were removed from the task force's agenda on policy grounds. These were usually dictated by other concerns over issues of individual privacy. Some of these have come to represent very attractive technologies today.

In 1967, for example, there was already considerable discussion about the prospect of mounting an electronic monitor on an individual convicted offender, and using that device to track the individual in the community rather than have him languish in prison at a high cost. There were arguments that this might even represent more effective control then prison, and could certainly be far less expensive. That period was at the height of the Warren Court, with its growing emphasis on due process and individual liberties, and so such technologies were viewed to be unacceptably invasive of individual privacy. Today, however, at a time of severe prison crowding, they are viewed as an important means of solving the prison crowding problem.

The principal recommendations of the task force related not so much to the provision of elegant gadgetry or even to major R&D efforts for achieving them. Rather, the task force emphasized the importance of contributions that would derive from the processes of science and from the methods of systems analysis for analyzing and improving the operation and the performance of the criminal justice system. I think subsequent developments have reflected those perspectives. Important advances have been made in learning the effects of the various actions of the criminal justice system on crime and in finding improved methods for linking the parts of the criminal justice system in terms of assessing their impacts on each other. R&D on fingerprint technology continued along with computer development generally and has produced that one major technological advance. Forensic

technology has continued to capitalize on general improvements in laboratory instrumentation and has provided incremental benefits through more sophisticated techniques for identifying smaller quantities of physical evidence with decreasing ambiguity .

The most important development in the operation of the criminal justice system has been that which follows from the introduction of computers, an effect similar to all other facets of society. Many new areas of research have been opened up. Computers have permitted the collection and detailed analysis of large samples of victim reports to learn about victimization, large numbers of criminal histories to learn about criminal careers, and to follow large numbers of released offenders to learn about the factors affecting recidivism. It has also permitted improved allocation of resources by police, courts, probation offices, and other criminal justice agencies, all of which have very limited resources to be applied to problem areas that required differential coverage by region or by individual. Computers have also made available large data bases of wants and warrants and of missing persons and property - as represented by the NCIC for example. This technology was just beginning to become available 20 years ago.

The major technological advance has been that associated with automatic fingerprint identification systems (AFIS). That kind of capability was impossible twenty years earlier, and its introduction in recent years represents a major new development

that has considerable possibility for having a significant impact on the criminal justice system. The major influence will be the potential for solving crimes by using the latent fingerprints left at a crime scene to searching through a large number of candidate suspects. This increases the likelihood of solving the crime when a suspect is not in hand - an extremely difficult problem today. It will also provide a basis for rapid and error- free taking of fingerprints with advanced technologies. This will provide the opportunity to build up larger ten-print fingerprint files that can then be searched more effectively and efficiently with prints in hand.

Another important new development is that associated with the growing availability and system integration of personal electronic monitors. Recent use of these devices has been spurred by the crowding in prisons and jails and the need to find alternative means for dealing with relatively low-risk individuals in the community. An electronic monitor (an unremovable ankle or wrist bracelet), connected electronically through the telephone network to a central surveillance center, can be queried to assure that the individual to whom it is attached is at the appropriate location, which has a fixed receiver or transmitter to which the electronic monitor is electronically linked. Thus, this form of restraint, which is obviously not restraining in a literal physical sense but only through the threat of further sanction if it is not obeyed, represents a limited form of punishment. It is used predominantly

by confining the individual to his home outside of normal working hours. While this may be an "unusual" form of punishment, it is increasingly recognized as far less "cruel" than would be the conventional use of imprisonment in even the most accommodating institution.

Throughout the past period there have been major advances in biotechnology and in electronic instrumentation, thereby providing capability for careful analysis of smaller and smaller segments of physical evidence left at a crime scene. An ultimate extension is reflected in the growing capability at analyzing the nuclear material associated with individual residues to develop a unique DNA match that then provides unique identification of each individual. Developing a data base of individual DNA codes, however, is far more remote than a very large data base of individual fingerprints, so this technology is particularly appropriate when a limited set of suspects is in hand.

III. Changing Pressures for Protection of Privacy

One of the continuing tensions associated with the use of technology by the criminal justice system is that associated with the concern over the degree to which technological approaches might compromise individual privacy. Those compromises may involve aspects of surveillance, dissemination of individual information to multiple interested parties, use of technological means for control or observation of movements, and other means by which the forces government are endowed with stronger means

for exercising control over the individual.

Twenty years ago, when there was considerable slack within the crime control system (U. S. prisons for example, had an incarceration rate well below half of their current rate) and the crime problem was only beginning to become of concern (the UCR crime rate was well below half its current rate). As the system has been increasingly stressed and the public has imposed greater demands for crime-control effectiveness, the balance between protecting individual privacy and becoming more effective at crime control has tended to shift toward the latter. This shift has been accompanied by a growing recognition and accommodation to a society that in many ways is becoming increasingly comfortable with computers. More often, they are viewed as familiar friends rather than hostile threats in the hands of unfeeling technocrats.

All of these influences have led to greater willingness to invoke technological approaches that might formerly have been viewed as unacceptable. This is partly because the threat has been found to be less severe than had been anticipated, and also because the benefits were more urgently desired. Indeed in the area of criminal record information, legislation of the late 1960s and early 1970s, in some jurisdictions, precluded the computerization of criminal record information In the current era, that has been replaced by court decisions that require open access to criminal justice record information. The threat that

was expected to be repelled by precluding use appears to have been replaced by a requirement for open and ready access. It appears unlikely, therefore, that these trends will be reversed to any significant degree now that the technological opportunities have become so widely available and used.

IV. Some Future Prospects

The following papers at the conference will address a number of important developments in the use of technology for the criminal justice system. The breadth of the perspectives considered highlight the many ways in which technology can intersect and improve the criminal justice system. The potential is considerable because the technology will be advancing regardless of the choices made by the criminal justice system. The choices, rather, are much more those in which the system wants to share, and which ones it wants to avoid. If the past is any indication, then it is reasonable to anticipate that an early desire to avoid is likely to be overcome at some future time when needs for the technology make its attractiveness exceed the concerns that may be raised about it.

There is little that the criminal justice system is likely to want to do or to be able to do to impede the advance of the technologies. The issues will be predominantly those associated with the application, the forms of the application, and wise and effective use. These are issues that all participants in and observers of the criminal justice system must deal with in an intelligent and informed way, both in moderating the uses as well as in appropriately enhancing their effectiveness.

Médecine légale et criminologie face aux problèmes des technologies nouvelles et de leur emploi en criminalistique(*)

Giacomo Canepa

1. Introduction

Au nom de la Société Internationale de Criminologie, j'ai l'honneur de prendre la parole, à l'occasion de la séance d'ouverture de notre 38ème Cours International, pour remercier avant tout les organisateurs de l'Université de Montréal, notamment l'Ecole de criminologie et le Centre international de criminologie comparée, ainsi que les directeurs du Cours M. Marc LeBlanc et M. Alfred Blumstein.

Le sujet central du Cours ("Nouvelles Technologies et Justice Pénale") et le commentaire de ce thème que nous avons lu dans le programme se rapportent justement à un Cours précédent: au 17e Cours international ("La criminologie en action") que le Département de criminologie de cette Université, sous les auspices de notre Société, avait organisé en 1967 à Montréal sous la direction de Denis Szabo.

(*) Professeur titulaire, directeur de l'Institut de Médecine Légale et du Centre international de criminologie clinique, Université de Gênes (Italie). Président de la Société internationale de criminologie.

Pour ce qui concerne les liaisons historiques et conceptuelles existantes entre le Cours actuel et le Cours précédent, sur ce point je dois vous exprimer un commentaire tout à fait personnel, qui a été le résultat de mon expérience de participation directe au Cours de 1967 en tant que rapporteur.

Je me souviens que M. Marvin Wolfgang, dans son rapport sur la prédiction des développements futurs de la criminologie, avait fait référence à une distinction en trois systèmes fondamentaux (personnalité, société, culture) en soulignant que:

1) tout individu est un organisme biologique, un porteur de valeurs culturelles transmises, un membre d'un groupe social;

2) le développement historique de la criminologie démontre que la recherche s'est occupée d'abord du système de la personnalité, ensuite de la société et enfin de la culture.

Suivant la doctrine des cycles historiques on pouvait prévoir en 1967, d'après Wolfgang, une fois épuisée la troisième phase ("la culture"), un retour à la première étape de cette évolution de la recherche ("la personnalité").

Vingt ans après on peut vérifier l'exactitude de cette prédiction: une section des travaux du 25ème anniversaire de l'Ecole de Criminologie de Montréal (1985) a été dédiée à la personnalité; à la personnalité est dédiée une partie considérable des travaux de ce Cours International.

En effet l'analyse des technologies nouvelles et de leur application aux systèmes de justice pénale, thème du Cours actuel, concerne une série considérable de problèmes de médecine légale, soit d'une science qui reconnaît dans la personnalité humaine l'objet fondamental de ses études.

A la médecine légale et à ses laboratoires se rapportent

directement les technologies d'identification de la personnalité individuelle (tests de sang, d'urine, de sperme, analyses vocales et moleculaires, etc.). A la médecine légale en tant que science déontologique de la personne humaine, de ses devoirs et de ses droits, se rapporte l'utilisation des autres technologies (surveillance électronique, vidéo, détection du mensonge, ordinateurs, etc.), dont l'application aux systèmes de justice pénale soulève plusieurs questions concernantes les droits de l'homme et la conduite morale dans les domaines dee l'activité professionnelle et de la recherche scientifique.

Afin d'éclaircir ces problèmes j'aborderai avant tout la question de la médecine légale et de sa définition suivant une orientation théorétique et épistémologique qui puisse consentir une systématisation du domaine de son activité. Ensuite j'aborderai le problème des rapports entre médecine légale, criminologie et criminalistique suivant la perspective des questions posées par les travaux de ce Cours international.

2. La définition de médecine légale

A l'heure actuelle la médecine légale risque de se fragmenter en petits morceaux de sous-disciplines, qui vont perdre toute leur signification si elles ne sont plus liées à l'unité conceptuelle de la discipline-mère (Roche, Roche et Diamant-Berger).

La réalité de ce processus est dénoncée par certaines terminologies qui sont utilisées d'habitude dans le langage commun et qui, à mon avis, dénoncent des erreurs conceptuelles: par exemple "droit médical" au lieu de "déontologie médico-légale", "psychiatrie légale" au lieu de "médecine légale psychiatrique".

On pensait jadis qu'un problème médico-légale pouvait être résolu, en cours d'expertise, par la collaboration entre le juge et le spécialiste d'une discipline médicale particulière: le juge avec l'obstétricien (à propos d'un avortement), le juge avec le spécialiste en traumatologie (à propos de coups et blessures), le juge avec le

gynécologue (à propos d'un viol), le juge avec l'hématologiste (pour le diagnostic de taches de sang), le juge avec le clinicien psychiatre (à propos d'un défaut mental).

Cette vision unilatérale, autrefois en vigueur dans la pratique légale et encore persistante à l'heure actuelle en certains pays (par exemple, anglo-saxons), a été depuis longtemps une source remarquable d'erreurs judiciaires. Mais un autre critère s'est imposé graduellement d'une façon presque universelle.

Ce critère, qui est la source originale même de la médecine légale et le noyau central de sa raison d'être, exige la connaissance préalable et essentielle des problèmes médicaux nécessaires pour la compréhension et pour l'interprétation de la norme juridique.

Cette problématique a assumé une véritable autonomie, dans le sens qu'elle ne fait pas partie ni du domaine du droit ni du domaine de la médecine clinique (Canepa, 1983).

La médecine légale est une science qui étudie la personnalité dans ses rapports avec le droit. Par conséquent, l'objet de ses études (la personnalité) est le même de la médecine clinique. Ce qui permet de différencier la médecine légale de la médecine clinique est la finalité (pas l'objet, qui est le même) de son activité: la thérapie et la prévention sont les finalités de la médecine clinique; l'évaluation juridico-sociale est le but de la médecine légale. Deux orientations existent au niveau de l'activité médico-légale:

1) L'évaluation des normes juridiques concernant la personnalité afin de rendre possible leur application pratique (collaboration du médecin légiste avec le juge).

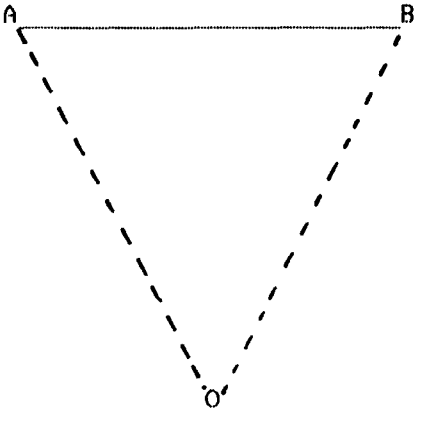
2) L'évaluation de ces mêmes normes afin de les modifier pour les rendre, dans les législations futures, plus adéquates aux connaissances scientifiques (collaboration du médecin légiste avec le législateur).

pçLe but de la recherche médico-légale va s'identifier dans une finalité d'évaluation juridico-sociale. Cette finalité peut être exprimée, en synthèse, dans un rapport bien défini: le rapport "personnalité et droit".

L'analyse de ce rapport, qui est la base conceptuelle de la médecine légale, nous permet de dégager deux principes fondamentaux:

1) La personnalité, qui est à l'origine du comportement et concerne l'individu considéré non seulement comme un "organisme biologique" (Wolfgang), mais aussi comme un porteur de valeurs culturelles transmises et comme membre d'un groupe ou système social (Canepa, 1971).

2) La situation juridique, où la personnalité est insérée, qui peut être exprimée par la figure géométrique d'un triangle (Carnelutti) suivant le schéma suivant:



Dans ce schéma sont représentés deux sujets (A, B), liés entre eux par un "rapport" juridique c'est-à-dire par la loi (ligne continue), qui manifestent un "intérêt" (ligne dessinée au trait) pour un objet déterminé (O).

Les études de médecine légale, qui portent sur la personnalité

dans les différents domaines du droit (pénal, civil, de sécurité sociale), sont finalisées à évaluer:

1) Les qualités de la personnalité en tant que sujet de droit (A, B).

2) Les lésions de la personnalité en tant qu'objet de droit (O).

Il s'ensuit que toute la médecine légale peut être configurée en rapport à la "situation juridique" (en matière pénale, civile et de sécurité sociale), étant donné que ses recherches visent à l'examen de la personnalité humaine placée dans une situation juridique déterminée, c,est-à-dire à l'évaluation d'une série de problèmes qui peuvent être présentés dans la synthèse suivante, qui représente le contenu même de la médecine légale dans ss différents domaines (Canepa, 1983):

I- EN MATIERE PENALE:

1) qualités

- capacité criminelle
- imputabilité (responsabilité)
- dangerosité sociale

2) lésions

- avortement
- infanticide
- coups et blessures
- délits sexuels
- homicide

II- EN MATIERE CIVILE:

1) qualités

- capacité juridique
- capacité civile
- capacité au mariage
- capacité à tester

2) lésions

- dommage corporel des enfants
- dommage corporel des adultes
- dommage corporel des vieux

III- EN MATIERE DE SECURITE SOCIALE:

1) qualités

- aptitude
- capacité de travailler
- capacité de gain

2) lésions

- maladie
- accident du travail
- maladie professionnelle

J'avais déjà formulé ces orientations conceptuelles il y a quelques années en référence à la médecine légale, (1953, 1966, 1976), en tant que "science interdisciplinaire de la personnalité dans ses rapports avec le droit".

En effet toute recherche ou méthodologie utilisée en médecine légale (clinique, nécroscopique, de laboratoire) se rapporte à des questions juridiques qui concernent la personnalité ou ses traces: même l'autopsie et la criminalistique médico-légale, qui visent à la reconstruction d'un homme vivant (son identité, les causes de sa mort, etc...); soit une "personnalité".

Cette orientation, qui se rapporte aussi au concept de médecine légale "humaine" (Franchini), poursuit la finalité essentielle de souligner l'importance et l'unité de la médecine légale en tant que science autonome, dont l'enseignement est fondamental pour la formation culturelle et professionnelle non seulement des médecins, mais aussi des juristes, magistrats ou avocats.

Le schéma unitaire de la médecine légale, que nous avons proposé pour sa définition et pour son contenu analytique, offre à notre considération la coexistence de trois perspectives fondamentales:

1) Une perspective évolutive, au cours de la vie de l'homme.

2) Une perspective comparative, en tant que schéma applicable aux divers systèmes juridiques, abstraction faite des différences que ces systèmes présentent dans les divers pays.

3) Une perspective évaluative, pour l'interprétation des lois en vigueur ("médecine légale judiciaire"), aussi que pour leur réforme en vue de la formulation des législations futures ("médecine légale juridique").

3- Les rapports entre médecine légale, criminologie et criminalistique

Une partie considérable de la criminologie dépend des concepts et des évaluations de la loi pénale; par conséquent son objet (la criminalité) ne peut être déterminé que des principes tirés de l'évaluation légale et sociale. Les auteurs s'accordent sur ce point et, à cet égard, Hurwitz affirme qu'une connexion rigoureuse avec la criminalité dans le sens légal est une conditions nécessaire préalable pour que la criminologie puisse disposer d'une série d'"expériences contrôlables".

Dans les mêmes conditions se trouve la médecine légale, dont les études roulent sur la personnalité dans ses rapports avec le droit (civil, pénal et de sécurité sociale) et qui de la personnalité examine:

1) les qualités, en tant que sujet de droit;

2) les ménomations, en tant qu'objet de droit.

Les problèmes de la criminologie présente des aspects communs avec les problèmes de la médecine légale dans le domaine du droit pénal.

La criminologie étudie ces aspects médicaux mais elle étend son intérêt au-delà de la médecine légale. Enfin la médecine légale offre à la criminologie un des thèmes de ses études, c'est-à-dire la partie de médecine légale qui se rapporte à la personnalité en tant que sujet de droit pénal.

Il a été nécessaire de poser avant tout le problème des rapports entre médecine légale et criminologie. Ce problème nous permet de poser une autre question concernant la criminalistique et ses rapports avec la médecine légale et la criminologie: une question qui, à mon avis, doit être étudiée sour la même perspective.

Nous avons déjà souligné que la médecine légale peut être configurée en rapport à la situation juridique (en matière pénale, civile et de sécurité sociale), étant donné que ses recherches visent à l'examen de la personnalité humaine, placée dans la situation juridique, c'est-à-dire à l'examen des "qualités" de la personnalité (en tant que sujet de droit); et des "lésions" de la personnalité (en tant qu'objet de droit).

Les recherches médico-légales se rapportent à la personnalité ou à ses traces, aussi l'autopsie et l'examen des tâches, qui visent en tout cas à la reconstruction d'un homme vivant (la cause de sa mort, son identité, etc.), c'est-à-dire d'une personnalité. Cette orientation se rapporte aussi au concept de "Médecine Légale Humaine", illustré par Franchini à l'occasion du Congrès International de Vienne.

Il y a de plus le problème de l'identification de la personnalité qui se rapporte au sujet mais aussi à l'objet de droit: en effet, ce problème médico-légal se présente à notre considération:

1) en ce qui concerne les qualités de la personnalité: en pénal (identité du délinquant et de ses traces), en civil (identité du père dans les procès de filiation, identité de l'hériter en matière testamentaire, etc.;

2) en ce qui concerne les lésions de la personnalité: en pénal et en civil (identité de la victime, etc.).

Par conséquent, tout le domaine de la médecine légale peut être configuré par rapport à trois aspects fondamentaux de la personnalité: identité, qualité et lésions.

La considération du premier aspect (l'idendité) comprend tous les problèmes médico-légaux de l'identification.

Ici nous trouvons la liaison avec le criminalistique, qui s'occupe des problèmes médico-légaux de l'identification de la personnalité en matière pénale, susceptibles d'être examinés par les procédés de laboratoire. La criminalistique s'occupe aussi des procédés de laboratoire qui concernent l'identification des traces non biologiques dans les situations d'intérêt juridico-pénal: cet aspect est complètement au dehors de la médecine légale.

En conclusion, la criminalistique, qui n'est pas une discipline autonome et qui relève (en ce qui concerne les aspects biologiques) de la compétence des laboratoires des Instituts de Médecine Légale, peut être définie comme suit: elle s'occupe des procédés de laboratoire qui concernent l'identification de la personnalité et de ses traces et aussi l'identification des traces non biologiques dans les situations d'intérêts juridico-pénal (Canepa, 1966).

Les considérations exposées nous permettent de conclure, que le problème de l'identification biologique de la personnalité dans le domaine pénal (soit de l'auteur que de la victime, c'est-à-dire en tant que sujet ou objet de droit pénal) relève de la compétence de la criminalistique biologique, qui fait partie de la médecine légale.

Ce problème présente un intérêt évident aussi dans le domaine de la criminologie, notamment de la recherche criminologique, appliquée aux enquêtes sur des cas criminels.

L'étude des rapports entre médecine légale et criminologie nous consent d'esquisser une véritable "criminologie médico-légale" au niveau de trois perspectives fondamentales: l'identité. les qualités et les lésions de la personnalité en tant que sujet ou objet de droit pénal.

4- Conclusions

Je pense que, sur la base des considérations exposées, il est possible présenter le domaine très vaste de la médecine légale concentré dans un schéma en trois sections:

1) L'identification de la personnalité;
2) Les qualités de la personnalité;
3) Les lésions de la personnalité.

Cette division en trois sections doit être précédée par une introduction générale qui touche les problèmes suivants:

- histoire et définition de la médecine légale;
- les formes de l'activité médicale et les normes qui règlent cette activité pour ce qui concerne les devoirs, les pouvoirs et les droits (étique et déontologie médicale dans le domaine de l'activité professionnelle et scientifique).

Le Cours international qui va commencer propose un bilan actuel de plusieurs catégories de technologies nouvelles, appliquées aux systèmes de justice pénale.

La plupart de ces technologies présentent un intérêt qui concerne en même temps la médecine légale, la criminologie et la criminalistique.

Afin de fournir des exemples concrets de cette approche interdisciplinaire, avec mes collaborateurs je présenterai deux rapports:

1) un rapport en collaboration avec M. Francesco De Stephano, qui concerne l'identification individuelle de la personnalité (problème médico-légal et criminalistique) au moyen de l'étude des régions répétitives et hypervariables du DNA humain, appliquée aux expertises sur les taches de sang, ainsi que aux expertises visant à l'attribution ou à l'exclusion de la paternité;

2) un rapport en collaboration avec M. Marco Lagazzi, qui concerne le problème éthique des nouvelles technologies génétiques (problème de médecine légale et déontologie).

Je vais conclure sur ces points en soulignant encore une fois la conception de la médecine légale en tant que "science interdisciplinaire de la personnalité dans ses rapports avec le droit". Il s'agit d'une conception qui rentre dans la tradition européenne continentale, bien différente de la conception propre à la tradition anglaise, réductive, du médecin légiste en tant que "pathologist" (soit, médecin des cadavres...).

La conception élargie et extensive, que je propose, de la médecine légale en tant que science interdisciplinaire de la personnalité dans ses rapports avec le droit, se base sur les critères suivants:

1) la solution des problèmes d'expertise, concernant l'étude de l'homme et de son intégrité bio-psychologique, exige surtout une compétence et une préparation médico-légale, étant donné que c'est la médecine légale qui a enseigné et qui enseigne comment l'on doit étudier et approfondir, au niveau de chaque discipline de spécialisation clinique, les questions juridiques qui résultent de l'application du droit en vigueur aux problèmes médico-biologiques.

2) Pour paraphraser une célèbre affirmation Kantienne on pourrait dire que le jugement de l'expert médico-légal, qui manque de contenu technique et spécialisé, est "vide"; mais ce jugement, s'il manque de référence aux normes juridiques en vigueur, est "aveugle".

La médecine légale nord-américaine, au niveau plus qualifié, a finalement abandonné la conception restrictive anglaise (suivant laquelle la médecine légale se réduit à la "pathologie légale"). Cette évolution positive est bien évidente dans les traités de médecine légale nord-américaines (Curran, Mac Garry et Petty) et va reproduire une concep-

tion qui, à l'origine, était déjà présente dans l'ouvrage fondamentale de Paolo Zacchia, qui remonte au XVII siècle.

"Rebus medicis sub specie juris": une phrase latine, qui synthétise efficacement l'essence spécifique de la médecine légale et son contenu spécialisé. Ce qui représente le point de départ pour bâtir l'unité épistémologique de la médecine légale, en tant que science interdisciplinaire de la personnalité et de ses rapports avec le droit.

Cette orientation consent de mettre en évidence des liaisons très étroites avec la criminologie et la criminalistique, que j'ai pensé de signaler et de souligner au début de ce Cours International, auquel je souhaite le plus grand succès, avec les compliments aux meilleurs organisateurs.

BIBLIOGRAPHIE

Canepa, G.: II concetto di personalità nei suoi aspetti filosofici, biologici e medico-legali, 108-113. Ed. Ateneo, Roma, 1953.

Canepa,G.: Les problèmes de la criminalistique et de la criminologie au point de vue de la médecine légale. Acta medecinae legalis et socialis, vol. 19, p. 63, 1966.

Canepa, G.: L'épistémiologie et la recherche criminologique. Revue de droit pénal et de criminologie, vol. 51, p. 761, 1971.

Canepa, G.: Les bases épistémologiques et pratiques de l'unité de la médecine légale. Journal de médecine légale. Droit médical, vol. 26, p. 571, 1983.

Carnelutti, F.: Teorica Generale del diritto (p. 110). Ed. Foro Italiano, Roma, 1946.

Curran, W.J.; M.C. Garry; Petty, C.S.: Modern Legal Medicine, Psychiatry and Forensic Science. F.A. Davis Company, Philadelphia, 1980.

Franchini, A.: Médecine légale cadavérique et médecine légale humaine. Acta Medicinae Legalis et Socialis, vol. 25, p. 85, 1962.

Hurwitz, S.: Criminologica (p. 24). Ed. Macri, Firenze, 1954.

Roche, L.; Diamant-Berger, O.: Médecine légale et Droit médical. Journal de Médecine Légale, Droit médical, vol. 25, p. 647, 1982.

Roche, L.: Médecine sociale et droit de l'homme. Enseignement de droit et d'éthique médicale à la profession médicale. Journal de médecine légale, droit médical, vol. 25, p. 661, 1982.

Szabo, D. (textes réunis par): "Criminology in action". Presses Universitaires de Montréal, Montréal, 1968.

Wolfgang, M.: The viable future of criminology, in "Criminology in action" (p. 109), Presses Universitaires de Montréal, Montréal, 1968.

Zacchia, P.: Questiones medico-legales (IV ed.). Tipographia Joannis Piot, Avenione, 1955.

NEW TECHNOLOGIES IN CRIMINAL JUSTICE: AN OVERVIEW[1]

BY

DAVID J. ROBERTS

DIRECTOR
RESEARCH AND STATISTICS PROGRAM
SEARCH GROUP, INC
925 SECRET RIVER DRIVE, SUITE H
SACRAMENTO, CALIFORNIA 95831

INTRODUCTION

In the early part of this century, when automobiles and radios were first being introduced into police work, August Vollmer, a noted police reformer of the day, commented on the impact of this new technology:

> [W]ith the advent of the radio equipped car a new era has come. . . . Districts of many square miles . . . are now covered by the roving patrol car, fast, efficient, stealthy, having no regular beat to patrol, just as liable to be within 60 feet as 3 miles of the crook plying his trade—the very enigma of this specialized fellow who is coming to realize that a few moments may bring them down about him like a swarm of bees—this lightning swift "angel of death."[2]

Although we now know that Vollmer was a bit optimistic in his assessment, new technologies have found increasing application in criminal justice, often with dramatic results.

---

[1]Much of this presentation is drawn from D.J. Roberts, J.A. Ryder, T.F. Wilson, *New Technologies in Criminal Justice: An Appraisal* [A Report to the Office of Technology Assessment, U.S. Congress.] Sacramento, CA: SEARCH Group, Inc., Draft, June 8, 1987).

[2]National Commission on Law Observance and Enforcement, Report No. 14, *The Police* (Washington, D.C.: U.S. Government Printing Office, 1930), pp. 90-98, quoted in J. Rubinstein, *City Police* (New York: Farrar, Straus and Giroux, 1973), at p. 20.

The purpose of this course, then, is to provide an overview of the new technologies which are finding application in criminal justice, to evaluate the technical capabilities and operational consequences of their application, and to examine some of the legal and ethical controversies which arise when these technologies are applied.

Judith Ryder, Tom Wilson and I recently wrote a report on New Technologies in Criminal Justice for the Office of Technology Assessment of the United States Congress.[3] In that report we reviewed a broad range of technologies which have a current or potential application in criminal justice. To organize our efforts somewhat we divided the justice system into four principal domains:

- Investigation and Identification;
- Decisionmaking in Criminal Justice;
- Correctional Supervision and Treatment; and
- Information Processing and Communications.

The purpose of my presentation today is to assess the general capabilities of these technologies and to discuss the broad implications of their use in society. In my discussion I use an expansive definition of technology which includes the innovative use of information, such as data on career criminals, to support law enforcement applications (such as the repeat offender project of the Washington, D.C. Police Department) career criminal prosecution programs, and the development of bail, sentencing and parole guidelines.

INVESTIGATION AND IDENTIFICATION

Within the domain of investigation and identification we have seen the emergence of several new technologies which offer significant new capabilities to criminal justice

[3]See D.J. Roberts, J.A. Ryder, and T.F. Wilson, *supra* note 1.

agencies. Perhaps one of the most exciting and operationally significant technology is the introduction of Automated Fingerprint Identification Systems (AFIS).

Automated Fingerprint Identification Systems

The newest generation of Automated Fingerprint Identification Systems (AFIS) has revolutionized fingerprint identification technology in the 1980's.[4] The heart of AFIS technology is the ability of new computer equipment to scan and digitize fingerprints, 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 compare a new fingerprint with massive collections prints on file in a matter of minutes and can make identifications that previously were possible only through a time-consuming and error-prone process of manual comparison.

AFIS technology 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) of latent prints against very large fingerprint files. Thus, AFIS technology has significantly improved the efficiency of the criminal identification process and has added an important new crime-solving capability to the law enforcement arsenal.

What is perhaps most extraordinary about these new systems is the sophistication and intricacy of the scanning and mapping algorithms, which convert the unique spatial relationship of a fingerprint's characteristics, called minutiae—the ridge endings, bifurcations, and additional ridge direction and contour information—into a digitized

---

[4]See T.F. Wilson, "Automated Fingerprint Identification Systems," *Law Enforcment Technology* (August-September 1986), pp. 17-48; T.F. Wilson and P.L. Woodard, *Automated Fingerprint Identification Systems (AFIS): Technology and Policy Issues* (Washington, D.C.: U. S. Department of Justice: Bureau of Justice Statistics, forthcoming); and *Proceedings of a SEARCH National Conference on Automated Fingerprint Identification Systems*, Kansas City, Missouri, February 26-28, 1986. (Sacramento: SEARCH Group, Inc., forthcoming).

representation of the fingerprint. In a ten-print to ten-print search on good quality inked impressions, the computer plots the spatial relationship of 90 or more minutiae points for each finger—a number high enough to distinguish the uniqueness of that print from all others and to make it virtually certain that the computer will be successful in matching the candidate prints with the prints in the file. Latent prints have less minutiae data for the scanners to map. Nevertheless, working with only 15 to 20 minutiae points the systems can score matches. One law enforcement agency reported a hit made on a partial latent print which yielded only eight minutiae points.[5]

In preparing fingerprints to be searched, the system allows the technician to enhance the prints, correcting for breaks in the fingerprint pattern caused by blood, dirt, scars or burns. The system can even provide an evaluation of the quality of the print, disqualifying inferior prints. This print enhancement capability is especially important in searching latent prints, since it enables an experienced technician to fill in missing or blurred portions of print fragments to produce more useful images for the computer to work with.

Equally sophisticated are the search algorithms used in the new AFIS systems to convert the minutiae data and ridge direction and contour data extracted by the scanner into a unique binary code that the computer can use in searching its files. The search algorithm determines the degree of correlation among the location, angle and relationship of the minutiae of the search print and the minutiae patterns of file prints. The computer is not actually comparing fingerprint images in its search; it is conducting a mathematical search that will provide a candidate list of those binary codes in the file most similar to the binary code used in the search.

The mathematical search is carried out by an AFIS system component called a matcher, which can search a candidate print (a rolled, ink impression of a suspect's prints

[5]Interview with Sergeant Kenneth Moses, Crime Scene Investigations, San Francisco Police Department, March 29, 1985.

or the latent print found at the crime scene) against the file prints at a rate of 500 to 600 prints per second. Matchers operate in parallel, each taking a portion of the data base. As file size increases, matchers may be added so that there need be no diminution of searching speed. Average searching time is, however, relative to a number of factors including the number of matchers employed, the time spent in preparing and enhancing the prints and entering demographic data to limit the number of prints to be searched, and the time the candidate prints wait in the system's queue (temporary memory storage) prior to the search process. Search time for a ten-print search (rolled print to rolled print comparison) in a file of under 500,000 prints is a matter of minutes. For a latent search, the search time averages about one-half hour.

During the search for a mathematical match, the computer uses a scoring system that assigns points to each of the criteria used in the match. The technician defines the parameters of the search and sets a threshold score above which he has assurance that a match has produced a hit. At the conclusion of the search, the system reads out the candidate list of matches, the number of which was defined by the technician as a search parameter. Based on parameters set in the scoring system, the score of the candidate in the number one position, if high enough, indicates that the match is probably a hit. If the score is low, it means that the system has chosen the selected number of candidates most similar to the search print, but there is little probability of a hit. The optimal functioning of an AFIS would produce a hit on the candidate in the number one position every time and the score would be high enough to leave no doubt as to the match. For the 10-print search, fingerprint experts are reporting that in 98 percent of the prints that are matched, the candidate's score met the threshold and was in the number one position.[6] This level of accuracy, which is made possible by the large number of minutiae available from rolled prints, eliminates the necessity of comparing the search prints with the file prints of the

[6]*Proceedings of a SEARCH National Conference on Automated Fingerprint Identification Ssytems.* Kansas City, Missouri, February 26-28, 1986 (Sacramento: SEARCH Group, Inc., forthcoming).

other candidates on the list. If all of the candidates fall below the threshold score, then there is a high probability that the candidate's prints are not in the system. Nevertheless, some AFIS systems have policies calling for review of selected candidate prints in such cases, as an added precaution against missed identifications. For example, some jurisdications have a policy which requires comparison of the search prints with the file prints of the candidate in the number one position if there is a sizable differential between the scores of the number one and two positions.[7] For latent searches, where there are fewer minutiae to work with, comparisions may be made on as many as three to five candidates. Such policy determinations, in general, factor technical performance, cost, time, and the priority given to particular kinds of crimes.

Finally, it is important to note that an 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 it does not replace, the fingerprint expert.

Biometric Security Systems

In addition to AFIS, we are also witnessing important advances in a variety of biometric security systems which may ultimately affect our lives in ways we have only begun to realize.

Recent advances in microchip design are increasingly being used in devices which verify the identity of persons seeking access to controlled or classified data or secured areas. This new technology includes devices that read fingerprints, palm prints, hand

[7]The California Department of Justice's CAL-ID statewide AFIS, for example, has adopted the above policy and others based on careful study and testing of its AFIS performance relative to candidate position and hit frequency.

geometry, voice, and retinal blood vessel patterns.[8] One of the early and commercially successful devices to verify identity was Identimat, a product of Stellar Systems Inc., a San Jose, California company. The device measures the spatial geometry of the hand (i.e., the length, curvature and webbing between fingers) in order to verify the identity of the person. The device works by having the user insert a card, containing the authorized individual's hand geometry data magnetically encoded, and then placing his or her hand in the four slots of the machine's surface to verify that the geometry of the hand in the slots is identical to the one stored on the card. The individual hand geometry data can also reside within a microcomputer linked to the machine, thus obviating the need for a separate card. The device is currently used in a variety of applications, ranging from nuclear facilities, government installations, banks, automatic teller machines, and even the cafeteria of a major university.

Direct Readings

Other biometric devices read individual fingerprints or palm prints directly from an individual's hand. Both Identix and Fingermatrix manufacture products which allow identity verification by reading individual fingerprints. These systems allow the operator to review the fingerprint on an accompanying screen to determine the quality of the print, thus averting the collection of poor quality fingerprints. The system can be used to create the standard ten-print fingerprint cards which are generally used by police departments and the FBI, allowing faster processing and eliminating the mess and smudging of traditional inked prints. Mitsubishi Electric is presently designing a system which will utilize palm prints, in a manner similar to the hand geometry system designed by Stellar Systems, but without the user card.

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

Retinal Scanning

Another innovative strategy in identity verification relies on the pattern of the blood vessels of the retina. Easily seen behind one's pupil, the patterns appear to be unique to each individual. EyeDentify Inc., has developed a device into which an individual peers through a raised set of opera glasses attached to a machine with a keypad station. The eye camera scans an area of the retina with a safe, low-level infrared light, which is fed back to a photo sensor. The resulting waveform is then digitized into computer language, computer processed, and stored as a signature template. On subsequent attempts to gain entry by the individual, the machine compares the eye signature with the authorizations on file.

DNA Fingerprinting

Another area of technological advance which promises important contributions in criminal justice as well as the civil justice systems is DNA Fingerprinting. British scientists have recently developed a test in which the deoxyribonucleic acid (DNA), which is contained in every cell of the human body, is examined to determine the sequencing of nucleotides as a method of identification.[9] The actual sequences of nucleotides are the same in all persons, but the number of sequences and the pattern of those sequences varies with each individual. It is this variation that scientists believe will be useful in establishing individual identification. Preliminary tests indicate that the nucleotides are sequenced in a pattern nearly unique to each individual; only identical twins have been found to share common DNA patterns, and scientists hope subsequent advances will help distinguish unique traits between twins.

---

[9]P. Gill, A.J. Jeffreys and D.J. Werrett, "Forensic Application of DNA 'Fingerprints'" *Nature* 318 (December 1985), pp. 577-579. Also see P. Gill, J.E. Lygo, S.J. Fowler and D.J. Werrett, "An Evaluation of DNA Fingerprinting for Forensic Purposes" *Electrophoresis* 8 (1985), pp. 38-44; P. Gill, "A New Method for Sex Determination of the Donor of Forensic Samples Using a Recombinant DNA Probe" *Electrophoresis* 8 (1985) pp. 35-38; and B. E. Dodd, "DNA Fingerprinting in Matters of Family and Crime" *Nature* 318 (December 1985), pp. 506-507. L.K. Altman, "The Ultimate Fingerprint" *New York Times*.

The test to apply DNA chemical sequencing was first reported by Dr. Alec J. Jeffreys, of the University of Leicester, who, working with two other scientists from the British Home Office's Forensic Science Service, adapted the test for criminological uses. Experts believe the test will be useful in rape and homicide investigations, where blood or semen evidence can often be retrieved. The test should also prove useful in the civil justice system for determining paternity.

Forensic specialists in the United States are also studying the application of this new technology to criminal justice. One of the major problems challenging the routine use of this test in homicide and rape cases is the relatively large amount of blood or semen required in order to conduct the test. Scientists working at the FBI, however, are hopeful that they will be able to overcome this difficulty, and they view the procedure as one which will have great potential in law enforcement investigations.[10]

Artificial Intelligence

One area of innovation which we view as having significant potential application in criminal justice is the use of artificial intelligence. Artificial Intelligence (AI) is a relatively new discipline within computer science, which after 30 years of research and development in universities and the private sector has begun to yield commercially available products.[11] While there is much disagreement about the definition of artificial intelligence, the common element that distinguishes AI from other computer disciplines is the attempt to imbue

---

[10]Interview with Dr. Bruce Budowle, Forensic Specialist, Crime Laboratory, Federal Bureau of Investigation, February 17, 1987.

[11]For a comprehensive review of artificial intelligence, see A. Barr and E. Feigenbaum, *The Handbook of Artificial Intelligence, Volumes 1-3* (Stanford, CA: HeurisTech Press, 1982). Also see R. Forsyth and C. Naylor, *The Hitch-Hiker's Guide to Artificial Intelligence* (London: Chapman and Hall/Methuen, 1986); H.C. Mishkoff, *Understanding Artificial Intelligence* (Indianapolis, IN: Howard W. Sams & Co., 1985); W.B. Gevarter, *Intelligent Machines: An Introductory Perspective of Artificial Intelligence and Robotics* (Englewood Cliffs, NJ: Prentice-Hall, 1985); D. Peat, *Artificial Intelligence: How Machines Think* (New York: Baen Enterprises, 1985); and P.H. Winston and K.A. Predergast, eds. *The AI Business: Commercial Uses of Artificial Intelligence* (Cambridge, MA: The MIT Press, 1984) [hereinafter cited *The AI Business*].

computers with traits associated with human mentation—specifically those associated with human understanding and intelligence.

The four predominant artificial intelligence research and development applications that have made significant progress are Natural Language Processing, Computer Vision, Expert Systems, and Problem Solving and Planning.

Expert Systems

Expert systems are computer programs that embody human expertise in a particular domain (area of expertise) of knowledge. They are, in a figurative sense, the cloning of an expert's methods of problem solving.[12] Expert systems, at least at present, do not replace experts; rather, they act as assistants who give advice to experts and to those who do not have access to experts. Expert systems emulate the thinking processes of the best experts on their best days. Experts are human and in the course of their daily work they are subject to memory lapses, distractions, and other interferences and failings of their reasoning processes. More important, experts age, retire and die, all of which may result in an irretrievable loss of the expertise. In the process of transferring an expert's knowledge to a computer, however, the experts are given the opportunity to carefully articulate, examine and test their rules and methods for problem solving, thereby capturing their best information.

Expert systems are distinguished from *database management systems* by their ability to apply reason to the knowledge in their databases. *Database management systems* store declarative knowledge, or facts, in their data bases and can retreive those facts rapidly. In contrast, expert systems contain both declarative knowledge and procedural knowledge, which allows them to apply the reasoning processes of human experts to the declarative knowledge. For example, a *database management system* could store and

[12]R. Davis, "Amplifying Expertise with Expert Systems," in Winston and Prendergast, eds., *The AI Business*, see note 11, p. 18.

rapidly retrieve all of the symptoms of various illnesses, while an expert system would be able to diagnose a specific illness from the various symptoms, suggest a method of treatment, and explain the steps used in arriving at the solution.[13]

In recent years we have seen growing development in the application of AI in criminal justice, primarily in the area of expert system. Examples of expert systems in criminal justice include:

- *Criminal profiling for serial murder and rape.* Under development by the FBI's Behavioral Science Investigative Support Unit, National Center for the Analysis of Violent Crime, FBI Academy, Quantico, Virginia.[14]

- *Serology Analysis.* Under development by the California Department of Justice.

- *Organized Crime and Labor Racketeering.* Called "Big Floyd" and "Little Floyd." Developed by the FBI's Technical Services Division.

- *Narcotics Interdiction.* Under development by the FBI's Technical Services Division.

- *Counterterrorism.* Under development by the FBI's Technical Services Division.

- *Name Searching System for Various FBI Data Bases.* Under development by the FBI's Technical Services Division.

Components of Expert Systems

Most expert systems are developed to solve specific problems. There is no one standard expert system. There are, however, three principal components common to most expert systems: a *knowledge base*, an *inference engine*, and a *user interface.*

The *knowledge base* may be defined as the component of an expert system that contains the system's declarative and procedural knowledge. It is the expert's knowledge

---

[13]Examples of operating medical diagnostic expert systems are MYCIN, CASNET, and INTERNIST. Descriptions of these systems are provided in Barr and Feigenbaum, *The Handbook of Artificial Intelligence*, see note 11, Volume 2, pp. 184-223.

[14]Interview with W. Tafoya, Behavioral Science Investigative Support Unit, Federal Bureau of Investigation, January 5, 1987; interviews with W. Tafoya, D. Icove and R. Rabussen, Behavioral Science Investigative Support Unit, Federal Bureau of Investigation, January 15, 1987. For discussion of criminal profiling and the expert system being developed by the FBI, see J.E. Douglas and A.E. Burgess, "Criminal Profiling: A Viable Investigative Tool Against Violent Crime," *FBI Law Enforcement Bulletin* 55, (December 1986), p. 9; D.J. Icove, "Automated Crime Profiling," Ibid., p. 27.

of a particular domain and his heuristics (rules of thumb), which provide a procedure for attempting to solve a given problem. The *inference engine* is that component which controls the system's operation by selecting the rules to use, accessing and executing those rules, and determining when a solution has been found. The inference engine also functions as the control structure or rule interpreter. The *user interface* is the component of an expert system that allows bidirectional communication between the system and its user. Most user interfaces utilize another AI technique, that of *natural language processing*.

The development of an expert system begins with a working partnership between a knowledge engineer and a domain expert to build the knowledge, i.e., the database of declarative and procedural knowledge. The knowledge base may be the expertise of one or more experts in a given field. This is a complex process, sometimes requiring as many as six years to capture and translate the expert's knowledge into the expert system's knowledge base. The dominant form of knowledge representation in today's expert systems is the rule-based production system. In a rule-based expert system, the knowledge engineer integrates the declarative knowledge of the domain expert with the procedural knowledge in the form of heuristic *if-then* statements. The expert system may also contain rules that do not pertain to the domain; these are called meta-rules, which specify under what conditions a certain rule in the knowledge base should be followed instead of another.

An example of an if-then, rule-based expert system in medical diagnosis is MYCIN. The knowledge base contains scientific data linking symtoms to illnesses in the following manner:

IF 1) the infection is primary-bacteremia, and
2) the site of the culture is one of the sterile sites, and
3) the suspected portal of entry of the organism is the gastrointestinal tract,

THEN there is suggestive evidence (.7) [probability] that the identity of the organism is bacteroids.[15]

[15]Ibid., p. 187.

The inference engine is constructed to act on a particular domain or knowledge base, although there are expert shells that supply an inference engine to more than one domain, if the domains are similar in structure. One of the key features of expert systems is that they speed searching and eliminate paths known to result in dead ends. It is the inference engine that provides the "reasoning" component of the expert system, selecting and executing the applicable rules and deciding when a suitable solution has been found. Problem solving in rule-based systems is usually executed by relating elements of knowledge into branches represented by if-then statements: if A, then B; if B, then C; or, if not A, then D. Each branch opens the possibility of choices and directions in problem solving. The inference engine is the decisionmaking component determining which branches to follow and which to eliminate in the problem solving process.

The user interface allows communication between the user and the expert system. The user presents the problem to the expert system, the expert system responds with its problem solution, and, if asked to do so, with its reasoning process. Because most domain experts normally are not computer experts, most expert systems are designed to be user friendly, using ordinary English by means of an AI component called a natural language processor.

Characteristics and Benefits of Expert Systems

Expert systems are distinguished by at least the following characteristics:

- Expert systems capture the expertise and problem solving methods of an expert or experts, thereby preserving institutional knowledge for the future and allowing it to be transferred to other users.

- Expert systems have faultless memories, capable of storing enormous amounts of information; they do not forget anything that is put in their knowledge base.

- Expert systems have the ability to "reason"—that is, they utilize rule-based procedures to select and make decisions on the elements of a new problem based upon prior knowledge captured by the system. The decision-making results in a solution to the problem.

- Expert systems can explain their reasoning process, showing the path of their decisionmaking logic.

- Expert systems have the ability to "learn"—that is, they can add knowledge to the knowledge base without the necessity of reprogramming, as in database management systems.

- Expert systems provide a means for testing and validating the knowledge base by examining real cases against the system. As such, they provide an iterative process of formulating and validating knowledge.

Expert Systems in Criminal Justice

Through their ability to institutionalize knowledge, and to disseminate rare investigative expertise, expert systems have the potential to benefit criminal justice operations enormously. Experts in fields such as criminal profiling,[16] forgery, arson, serial murder and rape investigation may have accrued as many as 30 years of experience in problem solving. When those experts leave their criminal justice agency, they take their expertise with them, causing the agency to begin replacing that expertise--a costly process which may take another lifetime to accomplish. Moreover, expert systems extend the range of the expert beyond a particular institution. Small agencies with less experienced or no experts may benefit from transferrable expert system programs that can assist in investigative problem solving.

Expert systems may also benefit the criminal justice community economically. While they are expensive to develop, they can supplement the work of criminal justice agencies in times of fiscal restraints, personnel cutbacks and hiring limitations.

The FBI views artificial intelligence as an opportunity to capture institutional knowledge, and the systems being developed by the Bureau are extensive. Expert systems are particularly critical to the investigative work of the FBI because frequently, the most effective investigators are promoted out of investigation and into management positions. This deprivation of highly trained investigators is compounded by early retirement and

[16]For a general discussion of criminal profiling, see B. Porter, "Mind Hunters," *Psychology Today* (April, 1983), pp. 44-52.

other attrition factors. In addition, the Bureau relies heavily on the expertise of local law enforcement officers, who, after being trained and participating in the Bureau's narcotics and drug interdiction program, return to their own jurisdictions, draining the FBI of valuable human resources.

Although the FBI is currently working inhouse on the development of AI applications, they have also used outside agencies to help develop systems, including the Institute for Defense Analysis. The Institute worked with the Bureau in developing "Big Floyd," a labor racketeering expert system, which is able to access and utilize the data contained in more than 3 million records in the FBI's Organized Crime Information System. The program, which derives its nickname from Floyd Clark, head of the Criminal Identification Division, is a very large relational database based on an "entity relation model." Relevant statutes, such as RICO are also in the system. The system allows an investigator to start with a person or organization, look at the statutes and their constituent parts, and ask questions such as: "Do I have enough evidence to charge this person/organization?" The program will analyze all data pertaining to an offender/organization and come to a conclusion. If there is not sufficient evidence, the program will suggest, for example, the kind of additional information that is needed and will suggest that, given the various relationships between individuals in the database, Subject "X" is likely to have data which may implicate the suspect in various crimes. The program will also suggest strategies for "turning" X into an informant.

DECISIONMAKING IN CRIMINAL JUSTICE

A considerable amount of research in criminal justice has recently focused on the longitudinal sequence of offenses which comprise an offender's "criminal career."[17] Most notable among this body of research of course is the work of Dr. Alfred Blumstein, who recently concluded several years of research with the National Academy of Sciences. A consistent finding of this body of research is the existence of a small core of recalcitrant and very active offenders who are responsible for a disproportionately large share of crime.[18] These findings have significant policy implications, particularly when considered in light of the burgeoning prison populations which today confront most states.[19]

In an effort to achieve the greatest crime reduction benefits in the most cost effective way, two innovative strategies for the apprehension and prosecution of persistent offenders have recently emerged. The Repeat Offender Project (ROP) of the Washington, D.C. police department is an example of law enforcement offender targeting in which the police sought to concentrate investigative resources on apprehending high-rate, repeat offen-

---

[17]A. Blumstein, J. Cohen, J. Roth and C. Visher, eds., *Criminal Careers and "Career Criminals" Volumes 1 and 2*. (Washington, D.C.: National Academy Press, 1986); A. Blumstein, D. Farrington and S. Moitra, "Delinquency Careers: Innocents, Desisters, and Persisters," in M. Tonry and N. Morris, eds, *Crime and Justice: An Annual Review of Research*, Volume 6 (Chicago, IL: University of Chicago Press, 1985); P. Greenwood, with A. Abrahamse, *Selective Incapacitation* (Santa Monica, CA: Rand Corp., 1982); J. Chaiken and M. Chaiken, *Varieties of Criminal Behavior* (Santa Monica, CA: Rand Corp., 1982); J. Petersilia, "Criminal Career Research: A Review of Recent Evidence," in N. Morris and M. Tonry, eds, *Crime and Justice: An Annual Review of Research*, Volume 2 (Chicago, IL: University of Chicago Press, 1980); J. Petersilia, P. Greenwood and M. Lavin, *Criminal Careers of Habitual Felons* (Santa Monica, CA: Rand Corp., 1977).

[18]Ibid.; M.E. Wolfgang, R.M. Figlio, and T. Sellin, *Delinquency in a Birth Cohort* (Chicago: University of Chicago Press, 1972). Wolfgang et. al. reported that six percent of their cohort of nearly 10,000 males born in 1945 were responsible for over half (52 percent) of the arrests recorded by the boys by their eighteenth birthdays. But see M. Gottfredson and T. Hirschi, "The True Value of Lambda Would Appear to be Zero: An Essay on Career Criminals, Criminal Careers, Selective Incapacitation, Cohort Studies, and Related Topics," *Criminology* 24, (1986) p. 213.

[19]A recent report of the U.S. Bureau of Justice Statistics indicates that the number of prisoners housed in state prisons has significantly outpaced capacity. U.S. Bureau of Justice Statistics, *Population Density in State Prisons* (Washington, D.C.: U.S. Department of Justice: Bureau of Justice Statistics, 1986).

ders.[20] The Major Violator Unit (MVU) of the San Diego District Attorney's Office is an example of a career criminal prosecution program, in which prosecutors sought to target prosecution resources on serious, repeat offenders.[21] Both projects have proven effective.

The Washington, D.C. Repeat Offender Project (ROP)

The Washington, D.C. Repeat Offender Project (ROP) which was established in 1982, created a specialized unit comprised of 88 officers whose responsibility was the proactive[22] apprehension of high-rate, repeat offenders.[23] The unit was organized into seven-member squads, each led by a sergeant.

The ROP project targeted two types of offenders for apprehension: those currently wanted on one or more outstanding warrants ("warrant targets") and those who were believed to be criminally active, though not presently wanted ("ROP-initiated targets"). Both types of offenders were targeted based on "the belief that the person is committing five or more Part I offenses per week."[24] A target committee, composed of three experienced investigators, initially targeted offenders through the use of criminal history record information, though this proved an ineffective and unreliable indicator of criminal

---

[20]For a recent review of other such programs, see W. Gay and W. Bowers, *Targeting Law Enforcement Resources: The Career Criminal Focus* (Washington, D.C.: U.S. Department of Justice, 1985).

[21]"Symposium on the Career Criminal Program," *Journal of Criminal Law and Criminology* 71 (Summer 1980), pp. 83-123. [Includes papers discussing the objectives of career criminal prosecution programs, selection criteria, the problems with existing prediction devices, and evaluations of operating programs.]

[22]A.J. Reiss, Jr., *The Police and the Public* (New Haven, Conn.: Yale University Press, 1971). Reiss distinguishes *reactive* and *proactive* police organizations as follows: "We have termed the police force a reactive organization when it is mobilized by calls or complaints from citizens, and a proactive organization when it seeks criminal violations on its own initiative." Ibid., p. 88.

[23]S.E. Martin and L.W. Sherman *Catching Career Criminals: The Washington, D.C., Repeat Offender Project* (Washington, D.C.: National Institute of Justice, 1986) [Hereinafter cited *Catching Career Criminals*]. This unit was subsequently reduced to 60 officers. Ibid., p. 9. Also see S.E. Martin and L.W. Sherman, "Selective Apprehension: A Police Strategy for Repeat Offenders," *Criminology* 24, (1986) p. 155 .

[24]Ibid., p.8. Part I offenses refer to the Index crimes of the Uniform Crime Reporting (UCR) program of the FBI. Federal Bureau of Investigation, *Crime in the United States: 1985* (Washington, D.C.: U.S. Government Printing Office, 1986) p. 331. The Index is comprised of murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, and auto theft. In 1978, arson was added to the Index, though it is separately accounted. Ibid.

activity. The officers subsequently used information obtained from other police units and street informants as the basis of their work, having established a rich set of criteria for targeting offenders and unique styles of investigation:

The unit received daily lists of major violators wanted by the department, criminal records of recent arrestees, daily crime reports from other districts, and specially prepared weekly printouts listing offenders wanted on numerous warrants. While the squads initially used lengthy surveillance of targets as their primary tactic, they later developed a variety of investigative and undercover techniques.

Following a 26 week experiment, data were compiled and an analysis of the effectiveness of the ROP project was performed. The findings indicate an increased likelihood of arrest, prosecution, conviction and sentence to confinement for ROP-targeted offenders. In addition, ROP arrestees generally had significantly longer criminal history records and were typically charged with more serious offenses than a comparison group of arrestees.[25] Overall police productivity, as measured by the gross number of arrests per officer, decreased during the project. This finding, however, must be weighed with the quality of arrests made by the ROP officers.

San Diego District Attorney's Major Violators Unit (MVU)

In July 1975, the San Diego District Attorney initiated the Major Violators Unit (MVU) project, aimed at identifying serious, repeat robbery offenders and prosecuting them to the full extent of the law. The program was initiated in response to massive increases in robberies (up 260% between 1968 and 1974) in the San Diego area. The unit was staffed by six senior deputy district attorneys, a research analyst, and three clerical

[25]Ibid., pp. 11-13.

support personnel. Unlike other criminal career prosecution programs, the San Diego MVU project was designed to concentrate solely on habitual robbery offenders.[26]

The broad goals of the program were 1) the early identification of serious, repeat robbery offenders, 2) vertical prosecution and reduced caseloads, 3) reduced plea bargaining, 4) increased convictions, and 5) appropriate prison sentences.

Identifying the serious robbery offender was aided by applying the following criteria:

- the suspect is under arrest for committing three or more separate robbery offenses; or
- the suspect is under arrest for robbery and within the last 10 years has been convicted of one or more of a series of specified serious offenses; or
- the prosecutor uses his discretion to accept a case involving great bodily harm or a defendant with several prior felony convictions.[27]

The MVU unit instituted a *vertical prosecution* technique which allowed a single prosecutor to handle cases throughout the prosecution, from arrest to final disposition.[28] Prosecutors assigned to the MVU unit handled a reduced caseload (8 cases per attorney compared to 22 cases per attorney in the Superior Court Division), allowing them to devote personal attention to a variety of tasks which might otherwise have been handled by others. The MVU attorneys attended bail hearings with the intent of having bail set high; maintained personal contact with witnesses, in order to encourage them to testify at trial; handled their own pretrial motions; assisted probation offices in preparing presentence investigations, including calculating a recommended sentence; prepared a prison statement

---

[26]"Symposium on the Career Criminal Program," see note 21. This discussion of the San Diego program is drawn largely from D. Whitcomb, *An Exemplary Project: Major Violator Unit, San Diego, California* (Washington, D.C.: U.S. Government Printing Office, September 1980) [Hereinafter cited *Major Violator Unit.*] Also see West's Ann. Penal Code §§999b-h, regarding California's career criminal statute.

[27]Whitcomb, *Major Violator Unit*, see note 26, p. 56.

[28]It is not an uncommon occurrence for several different deputy prosecuting attorneys to handle a single case throughout the course of a prosecution. This may occur as a result of the significant volume of cases routinely handled in large prosecutors' offices and the fact than an attorney is required to be present at various stages of the criminal justice process. Since the prosecuting attorney who handled the preliminary hearing of a particular offender may be involved in another proceeding when the offender's trial is scheduled, another prosecutor may be called upon to handle the case at trial.

for offenders sentenced to prison, expressing their perception of the offender's character and rehabilitative potential; and attended probation revocation proceedings when the crime committed qualified the defendant for MVU prosecution.

The MVU project adopted a tough plea bargaining policy of "descriptive pleading." The prosecutor was to review the nature of the current offense and the offender's criminal history, and select a configuration of charges which best described the offense and which, if proven, would obtain the optimal penalty. Defendants who desired to plead guilty were required to plead to the top (most serious) felony count or, in mulitple count cases, to more than one felony count, or the prosecutor would try the case. If the case went to court, the defendant ran the risk of being convicted of each of the original charges.

In addition to identifying the most serious robbery offenders, personally handling the cases throughout prosecution, and adopting a firm stance in plea and charge negotiation, the unit's prosecutors also sought lengthy sentences for those convicted. Two principal tactics were used by prosecutors in seeking lengthy sentences: applying enhancements[29] wherever possible, and seeking consecutive sentences rather than concurrent sentences.[30]

The results of an evaluation indicate substantial success in achieving the objectives of the project. Bail for MVU defendants was typically set at $20,000-$25,000, compared to $5,000-$10,000 for comparable defendants charged before the project started. The unit obtained high conviction rates for MVU defendants (90 percent were convicted either by guilty plea or were found guilty at trial) as well as high incarceration rates (virturally every MVU conviction resulted in incarceration). The unit also produced lengthy sentences for

[29]Enhancements are extended sentences authorized by California statutes for crimes involving firearms, great bodily harm, repeat offenders, and other similar aggravating circumstances. See West's Ann. Penal Code §1170.1; §12022; §12022.5.

[30]See West's Ann. Penal Code §§4501; 4501.5; 4502; 4503; 4532; 1170.1; 12022; 12022.5; 12022.6; 12022.7.

those convicted; an average sentence of 8.8 years for MVU defendants compared to 4.6 years for a comparable pre-project cohort.[31]

Decisionmaking Guidelines

In addition to projects that aid law enforcement and prosecutors in dealing with the chronic offender, recent years have also witnessed the emergence of innovative tools to aid practitioners in the complex process of decisionmaking when predictions of future behavior must be made. Setting bail, sentencing, releasing from prison and admitting to parole are discretionary decisions which necessarily involve the prediction of behavior. In setting bail the judge must consider the likelihood that a defendant will appear at trial. In sentencing, the judge may evaluate the danger an offender poses to society as well as his rehabilitative potential. Similarly, correctional officials and parole boards must also evaluate the likelihood that an offender will return to crime upon his release from prison.

In an effort to aid judges and correctional and parole officials in making these consequential and difficult decisions, an innovative decisionmaking tool has recently emerged. Parole, sentencing, and bail guidelines have attempted to bring structure, rationality, and consistency to correctional and judicial decisionmaking. It would not be overstatement to observe that these projects have revolutionized decisionmaking in criminal justice.

---

[31] D. Whitcomb, *Major Violator Unit*, see note 26, pp. 31-52.

OFFENDER SUPERVISION AND TREATMENT

A variety of alternatives have emerged in recent years in an attempt to divert from prison those offenders who can safely and successfully be treated in the community. Among the range of frequently used alternatives are fines, probation, suspended sentences, restitution and community service. Other innovative alternatives that may contribute to solving the dilemma of prison crowding while remaining sensitive to public safety, include electronic monitoring and the use of drug therapy for alcoholic and sex offenders.

Electronic Monitoring

The concept of electronically monitoring the geographic location of parolees and probationers is not entirely new. In 1964, Dr. Ralph Schwitzgebel, a member of Harvard's Science Committee on Psychological Experimentation, described a system of "electronic parole" whereby a portable transceiver device could monitor a parolee's location 24 hours a day.[32] Parolees, mental patients and researchers in Cambridge and Boston, Massachusetts volunteered to wear the tracking devices to assist the developers in their research between 1964 and 1970.[33] A patent was issued for the device in 1969.[34]

---

[32]R.K.Schwitzgebel, R. L. Schwitzgebel, W. N. Pahnke, and W. S. Hurd, "A Program of Research in Behavioral Electronics," *Behavioral Science* 9 (1964) pp. 233-238. Schwitzgebel's tracking device, called a Behavior Transmitter-Reinforcer (BT-R), consisted of two containers, one holding batteries and the other, a transmitter that automatically emitted uniquely coded radio signals. Each container was approximately the size of a thick paperback book, weighing about a pound. The transceiver had a transmitting range of a quarter of a mile and a receiving range of two miles. Information from the transceiver was received and recorded at a central base station. The device could be connected to a sensor resembling a wristwatch, enabling it to transmit the wearer's pulse rate. The wearer could also press a button to send beeps to the receiver, and register beeps sent from the receiver in reply.

[33]The subjects in a 1969 study ranged from an offender with over 100 arrests and eight years of incarceration to a young businessman with no criminal history. R.K. Gable (formerly Schwitzgebel), "Application of Personal Telemonitoring to Current Problems in Corrections," *Journal of Criminal Justice* 14 (1986) p. 168.

[34]Ibid. p.176. *R.K. Schwitzgebel and W. S. Hurd (1969). Behavioral supervision system with wrist carried transceiver. Patent No. 3,478,344.*

Almost immediately, the electronic tracking device generated publicity and sparked much speculation of potential applications. Possibilities included adding a microphone (to transmit whatever the wearer heard or said), and a walkie-talkie;[35] transmitters that might broadcast signals from sensors recording blood alcohol levels or other physiological data;[36] and brain monitors to determine if the wearer was asleep, alert or emotionally agitated.[37] Researchers also contemplated implanting electrodes in the body to stimulate the wearer's heart, brain or other organs for medical purposes. Meyer suggested the creation of a system which would combine individual, personally worn transponders, with transceiver units strategically placed in buildings and alongside streets designed to track offenders.[38]

The development of electronic monitoring devices made few advances until the early 1980's when national prison crowding "created [such] an unprecedented demand for diversion that market conditions were attractive enough to encourage the private sector to make the technology commercially available."[39] Rapid advances in communications technology and data management expanded the feasibility of using personal telemonitoring systems for correctional purposes. Microcomputer circuitry made it possible to create a portable and less conspicuous device capable of transmitting information over telephone lines and today, new developments in telemonitoring are occurring rapidly.

One of the first successful applications for personal telemonitoring devices was the "GOSSlink" electronic bracelet, a device inspired by the *Spiderman* comic strip. In 1977,

---

[35]Note, "Anthropotelemetry: Dr. Schwitzgebel's Machine" [Hereinafter cited "Schwitzgebel's Machine"], *Harvard Law Review* 80 (1966) p. 403. See *Hearings on Invasions of Privacy (Government Agencies) Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, 89th Congress, 1st Sess., pt. I, pp. 14-63, 323-24 (1965).

[36]R. S. MacKay, "Radio Telemetering from Within the Body," *Science* 134 (October 1961) p. 1196; I. J. Young and W. S. Naylor, "Implanted Two Way Telemetry in Laboratory Animals," *American Journal of Medical Electronics* 3 (January/March 1964), pp. 28-33.

[37]*Schwitzgebel's Machine*, see note 35, p. 404. See D. B. Lindsley, "The Recticular Activating System and Perceptual Integration" in D. Sheer, ed., *Electrical Stimulation of the Brain: An Interdisciplinary Survey of Neurobehavioral Integrating Systems* (Austin, Texas: University of Texas Press, 1961), p. 331.

[38]J. A. Meyer, "Crime Deterrent Transponder System," *Institute of Electrical and Electronic Engineers Transactions on Aerospace and Electronic Systems* 7 (1971), pp. 2-22.

[39]C.M. Friel and J.B. Vaughn, "A Consumer's Guide to the Electronic Monitoring of Probationers," *Federal Probation* 50 (September 1986), p. 3 [Hereinafter cited "Consumer's Guide"].

New Mexico District Court Judge Jack Love became intrigued with a cartoon in which a villain strapped a special bracelet on Spiderman's wrist to track the hero's whereabouts. Judge Love wrote to his state's corrections department, enclosing a copy of the comic strip and a news article about transmitting units that could track cargo and animals. Nothing more came of the idea until a 1982 crowding crisis in the county jail motivated the judge to begin contacting several companies to discuss the feasibility of creating the device.[40]

Judge Love convinced Michael Goss, a computer salesman, to quit his job to design and produce such a device. Goss established National Incarceration Monitor and Control Services (NIMCOS) and developed an electronic bracelet that could be used to monitor probationers. In 1983, after wearing the bracelet himself for three weeks, Judge Love ordered a probation violator to wear the device. Soon, four additional offenders were ordered to wear the monitoring bracelet; two offenders were convicted for drunk driving and two had probation violations that would have resulted in jail or prison sentences.

An appraisal of this electronic monitor, funded by the National Institute of Justice (NIJ), concluded that:

- the equipment operated successfully;
- monitored home confinement was acceptable to local criminal justice agencies;
- the concept did not appear to pose legal problems when used as an alternative to detention;
- compared to detention, monitoring resulted in "substantial savings" to the criminal justice system.[41]

Since Goss' pioneering work in 1983, and the establishment of the first monitoring program in Palm Beach, Florida in 1984, approximately 46 programs in 20 states have

---

[40]*Criminal Justice Newsletter* 15 (March 15, 1984) p. 4.

[41]D. Ford and A.K. Schmidt, "Electronically Monitored Home Confinement," *NIJ Reports*, (Washington, D.C.: U. S. Department of Justice, November 1985) p. 2.

used electronic monitoring devices in probation and parole, pre-sentence probation, work release or house arrest programs.[42]

Programmed Contact Systems

Programmed contact monitoring systems can assume a variety of forms, but basically entail an automated caller programmed to dial the probationer's home randomly or at specific times, to deliver one of several pre-recorded messages.[43] This type of system is frequently used in conjunction with a wristlet encoder device which the probationer inserts into a verifier box attached to the phone. Once inserted, the wristlet sends a signal to the computer which identifies the recipient of the call. If the telephone is not answered, or the bracelet is not inserted into the receiver, the computer notes a possible violation.

Other programmed contact systems use computerized "voice verification" to ensure that the respondent is the actual offender. Voxtron Systems, Inc., for example, has developed the "Provotron Home Confinement System" which utilizes specialized software and speech processing hardware to digitize a person's voice into binary code. When an offender begins the program, voiceprint data is collected for several phrases.

When the automatic calling unit calls an offender, the individual is asked to repeat a selection from the phrases which were originally recorded. If the spoken voice matches the voiceprint, the system may advance to a second "test"; the Provotron system has an option which requires the monitored offender to repeat a series of digits, using a telephone's touchtone keys. The intent is to test manual dexterity for indication of drug or alcohol use.

---

[42]The implementation of electronic monitoring programs is expanding rapidly, making a true count very difficult. NIJ reported these program figures in December 1986 and plans an extensive survey of all these programs in February 1987. Previously, in January 1986, the Texas Criminal Justice Policy Council conducted a 6-month feasibility study on electronic surveillance and house arrest as alternatives to incarceration, surveying 10 programs located in 7 states. See J.B. Vaughn, *Potential Applications for Electronic Monitoring and House Arrest in the State of Texas* (Huntsville, Texas: Sam Houston State University, July 1986) [Hereinafter cited *Potential Applications*]. In addition, in October and November 1986, EMT Group, Inc. surveyed 20 programs in 12 states. T. Armstrong, G. Reiner and J. Phillips, *Electronic Surveillance: An Overview* [Draft Report] (Sacramento, California: The EMT Group, December 1986).

[43]Armstrong, et. al., *Electronic Surveillance: An Overview*, see note 42, p. 2.

Continuously Signalling Systems

Continuously signalling systems usually consist of three components:

(1) a transmitter device worn by the offender around the ankle, neck or wrist, which transmits an encoded signal at regular intervals over a range of approximately 200 feet;

(2) a receiver/dialer unit located in the offender's home that detects signals from the transmitter and periodically reports to a central computer; and

(3) a control computer located at the controlling criminal justice agency that accepts reports from the receiver unit over telephone lines, compares them with the offender's curfew schedule and alerts correctional personnel to unauthorized absences.[44]

The device may be strapped above the ankle with a rubberized watch-type strap that is reportedly tamperproof; an electronic circuit within the device detects tampering and sends an alarm to the receiving unit.[45]

Operational Programs

Palm Beach County, Florida began two electronic monitoring programs in December 1984. The first of the currently operating programs in the country, the Palm Beach programs involve probationers and work-release offenders from a minimum security facility. The work release program is under the auspices of the County and the probation program is administered by PRIDE, Inc., a non-profit corporation that since 1977 has provided misdemeanant probation services for the county.[46]

The Palm Beach County Sheriff's Department implemented the first law enforcement application of electronic monitoring. The technology complements a work release program which allows midemeanants and nonviolent felons to work in the

---

[44]Ford and Schmidt, "Electronically Monitored Home Confinement," see note 41, p. 2.

[45]G. Kennedy, Control Data Corporation, Minneapolis, Minnesota. Interview conducted April 11, 1985, reported in R. v. del Carmen and J. Vaughn, "Legal Issues in the Use of Electronic Surveillance in Probation," *Federal Probation* 50, (June 1986), pp. 60-61 [Hereinafter cited "Legal Issues"].

[46]For a detailed description of the Florida programs, see Ford and Schmidt, "Electronically Monitored Home Confinement," see note 41, pp. 2-4; Vaughn, *Potential Applications*, note 42, pp. 38-41.

community during the day. After a period of adjustment (30-60 days), selected work release inmates are allowed to complete their sentences on monitored home confinement.[47] The program is designed for post-conviction work release inmates, with the average offender under house arrest for 60 days.

Offenders must have a home, a phone and be willing and able to pay a $9.00 daily fee. A transmitter is fitted to the offender's ankle and a sergeant accompanies the offender home to install the receiver unit. Each week the individual must report to the County stockade to pay the weekly fee and have the monitor checked. The sergeant who is assigned to each case also makes regular, unannounced visits to the offender's home and job site. As of July 1986, a total of 139 inmates had been under home arrest, with only three revocations.[48]

Costs and Benefits

Electronic monitoring is obviously more expensive than traditional probation programs, but the program is less expensive than prison confinement. Costs include the computer equipment, personnel and operational cost. The benefits in allowing certain offenders to be incarcerated in their own homes include the economic benefits of an offender's continued employment and ability to support himself and perhaps a family (thereby insuring tax revenues and relieving the state of welfare costs), and reducing the state's need to build additional prison cells. There are also important social benefits in allowing an offender to retain family and community relations.

---

[47]Individuals with any record of violence, sexual misconduct or drug abuse are ineligible for the program. Approximately 60 percent of participants are non-violent felons and 40 percent are misdemeanants.

[48]Vaughn, *Potential Applications*, see note 42, p. 39.

Depo-Provera

Treatment of sex offenders traditionally takes several forms: mental health therapy, psychotherapy, life skills training, behavior modification, and hormonal manipulation. Increasingly, programs involve a combination of methods and techniques, and almost always include some form of counseling and peer group treatment.[49] These treatment modes are considerably less intrusive than other strategies, which use a variety of aversive conditioning techniques, including electric shock treatments, shame-aversion, and covert sensitization.[50]

One promising, albeit controversial, treatment for use with certain sex offenders is hormonal manipulation through the injection of antiandrogen progesterone, i.e., chemical castration. Used in Europe for many years, hormonal manipulation has only recently been used in the American criminal justice system.

Found in varying levels in both males and females, testosterone is the sex hormone that produces male characteristics and is responsible for the male sex drive. Research has indicated that male sexual behavior is related to many variables, only one of which is the serum level of testosterone. Nevertheless, variations from the normal range of testosterone concentration are frequently associated with changes in behavior; a reduction in the hormone due to castration may reduce sexual interest and activity and an injection of testosterone to androgen-deficient men can increase sexual activity.[51]

---

[49]D.J. West, "Sex Offenses and Offending," in M. Tonry and N. Morris, eds., *Crime and Justice: An Annual Review of Research, Volume 5*, (Chicago: University of Chicago Press, 1983) p. 216. Comprehensive surveys of programs in the United States include E.M. Brecher, *Treatment Programs for Sex Offenders*, (Washington, D.C.: U.S. Government Printing Office, 1978); B. Delin, *The Sex Offender* (Boston: Beacon Press, 1978). Also see *Report on Nationwide Survey of Juvenile and Adult Sex-Offender Treatment Programs and Providers* (Syracuse, New York: Safer Society Press, 1986). [Hereinafter cited *Nationwide Survey Sex-Offender Treatment Programs.*]

[50]M. Serber and J. Wolpe, "Behavior Therapy Techniques," in H.L.P. Resnick and M.E. Wolfgang, eds., *Treatment of the Sex Offender* (Boston: Little, Brown and Company, 1972) pp. 59-64.

[51]J. Kelly and J. Cavanaugh, "Treatment of the Sexually DangerousPatient," *Current Psychiatric Therapies* 21, (1982), p. 103 [Hereinafter cited "Sexually Dangerous"].

The first clinical use of antiandrogen compounds to treat sexual offenders occurred in West Germany and Switzerland in the 1960's.[52] Experimenting with rats, scientists discovered the antiandrogenic properties of several drugs and began applying the new drug to human beings in selected clinics. The compounds were found to suppress the production of testosterone in the testes. In contrast to estrogen compounds, which in the male produce effeminate body changes and may cause irreversible infertility, the drugs being used were progesterone derivatives which have fewer unpleasant side effects, which are reversible and which have no known permanent adverse side effects.[53] The drug was approved in the United States for several medical applications, but the Food and Drug Administration (FDA) has not released it for the general treatment of sexually deviant behavior. It has been possible, however, for behavioral researchers working with sex offenders to substitute a synthetic progesterone known as Depo-Provera, manufactured by the Upjohn Company.

Effective treatment with Depo-Provera depends upon careful selection of appropriate candidates. For the treatment to be most effective, it is crucial that the offender be a willing participant; psychologically, the personal commitment of the patient is important in achieving the goal of preventing the repetition of deviant behavior.

Sex offenders selected for treatment with Depo-Provera typically receive a 300 to 400mg. intra-muscular injection of the drug every 7-10 days, the dosage dependent on the individual's physique and body weight. The objective of the treatment is the reduction of sex drive and visual imagery which causally precipitate the sexually deviant behavior. The drug is administered and regularly monitored in an attempt to lower testosterone levels from

---

[52]J. Money, "The Therapeutic Use of Androgen-depleting Hormones," in H.L.P. Resnick and M.E. Wolfgang, eds., *Treatment of the Sex Offender*, see note 50, p. 165. [Hereinafter cited "Therapeutic Use"]

[53]M.K. Spodak, Z.M. Falk and J.R. Rappeport "The Hormonal Treatment of Paraphiliacs with Depo-Provera," *Criminal Justice and Behavior* 5 (1978)pp. 304-314.

normal male levels to normal female levels.[54] By substantially reducing the level of testosterone in the male offender, Depo-Provera reduces potency and ejaculation, reduces the frequency of erotic imagery and diminishes sexual interest. Behavioral and cognitive behavior therapies are almost always included as part of the treatment.[55]

In contrast to other, more traditional forms of treatment for paraphiliacs (e.g., psychotherapy, behavior therapy, long term institutionalization or antipsychotic chemotherapy), Depo-Provera is said to be more specific and lasting in eliminating sexually dangerous behaviors.[56] There is also some evidence which suggests a relationship between androgens and aggression, indicating that lowered testosterone levels may also affect a decrease in aggressive drive states.[57] Others have found that Depo-Provera does not treat aggression *per se*, but reduces sex-related aggression.[58] Several theories have been postulated, but to date there is no conclusive evidence to explain the multiple biochemical and clinical effects of Depo-Provera.

A 1986 survey of 650 programs specializing in the treatment of sex offenders found that 14 percent of the adult programs and 6 percent of the juvenile programs were using Depo-Provera on an experimental basis.[59] The programs used the drug primarily to determine if Depo-Provera, in conjunction with extensive counseling, could reduce the

---

[54]Kelly and Cavanaugh, "Sexually Dangerous," see note 51, p. 104. Research also suggests that some offenders have excessively high levels of testosterone. F.S. Berlin and C.F. Meinecke, "Treatment of Sex Offenders with Antiandrogenic Medication: Conceptualization, Review of Treatment Modalities, and Preliminary Findings," *American Journal of Psychiatry* 138 (1981), pp. 601-646, at p. 605; P. Gagne, "Treatment of Sex Offenders with Medroxyprogesterone Acetate," *American Journal of Psychiatry* 138 (May 1981) p.645.

[55]With counseling only, the patient often becomes discouraged as a result of relapses into deviant behavior. With counseling and Depo-Provera there are almost immediate behavioral changes, thus increasing the effectiveness of psychological therapy.

[56]Kelly and Cavanaugh, "Sexually Dangerous," see note 51, p. 102.

[57]Ibid., p. 103

[58]Bradford, "The Hormonal Treatment of Sex Offenders," *Bulletin of the American Academy of Psychiatry and the Law* 11 (1983) p. 167, cited in Larry McFarland, "Depo Provera Therapy as an Alternative to Imprisonment," *Houston Law Review* 23 (1986), p. 810. Bradford believes there is little evidence of a correlation between serum testosterone and aggression, although there is a highly complex relationship between aggression and various biological factors.

[59]*Nationwide Survey of Sex-Offender Treatment Programs*, see note 49, reported in *Criminal Justice Newsletter* 17 (June 16, 1986), p. 6.

probability of recidivism with high risk, non-violent sexual offenders. One of the first programs to treat sex offenders with Depo-Provera was the Biosexual Psychohormonal Clinic at Johns Hopkins University Hospital in Baltimore, Maryland. Drs. John Berlin and John Money began research on the use of progesterone for the treatment of male sex offenders in the late 1960's. Weekly injections of Depo-Provera were combined with therapy sessions that utilized an acknowledgment and reinforcement approach similar to that of Alcoholics Anonymous. In a follow up to a 1979 study, 17 out of 20 men who had histories of paraphiliac behavior and who were being treated with Depo-Provera, were not involved in subsequent sexual offences. When medication stopped, however, substantial recidivism was observed.[60] In 1982-1983, the program served approximately 150 sex offenders, mostly as a condition of probation: 70 of the 90 men from seven states participated in the program under court order.[61] Program research suggests that Depo-Provera, when administered with counseling, can reduce the risk of recidivism.[62] The program stresses, however, that screening is critical to success and the drug has only been effective with paraphiliacs (i.e., those requiring bizarre imagery, voyeurs, sex masochists, pedophiles, etc.). The drug reportedly does not work well with antisocial career criminals.

Although the drug has met with limited experimental success, it does have several side effects. Depo-Provera is a progesterone derivative and therefore sex offenders may suffer the side effects that frequently accompany the use of oral contraceptives, i.e., fatigue, depression, weight gain, change in the growth of body hair, nausea, elevated blood glucose and headaches.[63] Evidence indicates, however, that these side effects are temporary and reversible when treatment is terminated. Money reports no contraindications

---

[60]Berlin and Meinecke, "Treatment of Sex Offenders," see note 54, pp. 604-605.

[61]*Criminal Justice Newsletter* 14 (September 12, 1983), p. 3

[62] These findings have been supported by the results of a similar program in Galveston, Texas; the Rosenburg Clinic reports that 70-80 percent of the men treated with Depro-Provera in conjunction with psychological treatment did not repeat their offensive behavior. See *Houston Post*, June 29, 1985, at 4A, col.1.

[63]P. Gagne, "Treatment of Sex Offenders with Medroxyprogesterone Acetate", see note 54, p.645; Kelly and Cavanaugh, "Sexually Dangerous," see note 51, p.104.

or irreversible side effects and reports that within six to twelve months following the last administration of the drug, the individual's testosterone level returns to its pretreatment level.[64] In addition to these side effects, the literature also reports some controversy regarding the drug's possible carcinogenic effects.[65]

INFORMATION PROCESSING AND COMMUNICATION

In the three and one-half decades that have elapsed since the development of the Univac I, computers have undergone a stunning metamorphosis. With the development first of transistors, and later of microprocessors, the size and cost of computers have significantly diminished, while their speed and storage capabilities have grown tremendously. The recent introduction of the 32 bit microprocessor has spawned the emergence of microcomputers which can easily provide the power of yesterday's mainframe on today's desktop, at a fraction of the original cost. This explosion in technology has launched law enforcement operations into the future, providing agencies with significant new capabilities.

Ticketwriter system:

The City of Newport News, Virginia became the first municipality in the world to issue computerized parking tickets when they adopted the Ticketwriter system, marketed by KET, Inc., on August 5, 1985. The system uses a hand carried portable computer, weighing 4.7 pounds, that issues parking tickets and automatically checks a scofflaw list

---

[64]J. Money, "Therapeutic Use," see note 52, p. 166; Kelly and Cavanaugh, "Sexually Dangerous," see note 51, p.104.

[65]Researchers opposing the use of Depo-Provera claim that high doses of medroxyprogesterone acetate have caused breast cancer in female dogs (See A. Rosenfield, et. al., "The Food and Drug Administration and Medroxyprogesterone Acetate", *Journal of the American Medical Association* 249 (1983) pp. 2924-2925.) Several other researchers, however, believe that these findings are inconclusive as to the carcinogenic effects the drug may have on human beings. Berlin and Meinecke,"Treatment of Sex Offenders,"see note 54, p.603.; A. Liang, et. al., "Risk of Breast, Uterine Corpus and Overian Cancer in Women Receiving Medroxyprogesterone Injections" *Journal of the American Medical Association* 249 (1983) p. 2909.

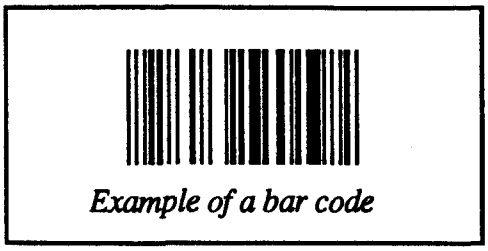
(violators with three or more oustanding citations) containing up to 10,000 entries. The unit has its own power source and printer, so the ticket is printed directly from the unit carried by the officer. The officer is prompted for all information necessary for ticket issuance (i.e., type of violation, license number, car make, etc). The unit also has its own independent memory, allowing automatic time and date posting for the tickets, and it enables the tracking of tickets issued by the officer throughout the day.

At the end of each shift the unit is returned to the station, where it is plugged into the main receiving unit which downloads the data, recharges the unit, and updates the scofflaw list in preparation for the next day's work. By downloading the data at the end of each shift, managers receive statistical and administrative reports at the end of each day, and the city's data processing center is able to post receivables/collections on a daily basis.

The system has the potential for substantially increasing the city's revenues, by reducing the number of tickets lost by illegibility, increasing the number of tickets issued by the officers, and increasing the apprehension of scofflaws.

Universal Product Codes (UPC or bar codes):

A promising recent technology in information processing is the Universal Product Code (UPC or bar code). The UPC enables rapid data entry while significantly reducing key entry error. The system utilizes a hand-held computer terminal with an attached reader or scanning wand. The bar code is comprised of a series of vertical black and white lines of varying widths. Each pattern is associated with pre-set alphanumeric codes. The reader wand emits a light which, when scanned across a bar code, is absorbed by the black lines and reflected by the white lines. The scanner transforms the patterns into a series of electrical impulses which are measured, decoded, and translated into binary digits for transmission to the computer. By measuring the relationship between light and dark bars, the computer can translate a single bar code into one or more variables.



Example of a bar code

Since each unit also has a full alphanumeric key pad, the system allows rapid entry of a variety of data, including both preset bar codes and raw alphanumeric data. The equipment frequently has an acoustical coupler for online transmission of data. Typically at the end of each shift or the end of a day, the data are downloaded from the remote entry device to a microcomputer at the local agency level. Management and administrative reports may then be generated immediately. The data can also be regularly transferred to a central county or state level for further analysis.

One of the advantages of UPC system is its ability to concatenate information read from one or a series of bar codes, thus tying several different variables to a single case. Individual UPC codes can also be designed to capture multiple values and variables. Thus, a single bar code can be designed to capture not only state statute citation, for example, but also the applicable NCIC coded offense. This is a significant advantage as it reduces the duplicity of routine data entry.

Although the UPC technology has been available for over two decades, recent advances in electronics and microcomputer design have allowed the units to become portable, maintaining their own source of power, and capable of storing large amounts of data. This is a very promising technology which is currently being used in police inventory, court case tracking and statistics compilation. It also appears to be a promising technology for use in inmate tracking, disposition reporting, and incident-based UCR.

Computer-Assisted Dispatching and Mobile Digital Terminals

One of the many advances microcomputers have achieved in recent years is the development of computer-assisted dispatching and the introduction of mobile digital terminals (MDT) into police cars. This new technology has many benefits for police agencies. Once an incident is reported by a citizen, the operator enters the appropriate data into the computer, an incident number is automatically assigned, and the incident is automatically routed to a dispatcher station based on functional or geographic area of responsibility. Entry of the violation code can result in the automatic assignment of an incident priority. As soon as he is free to accept a new call, the dispatcher may request an unassigned incident. Incidents may be assigned to dispatchers by priority of the incident. The major role for the dispatcher, once the incident has been assigned, is to monitor and update the unit's (police officer assigned) status and location.

The MDTs installed in the police cars allow nearly instantaneous communication between the dispatcher and the street units without the necessity of audio transmission. In addition to allowing rapid transmission between the dispatcher and the street unit, the MDT enables the officers to query a variety of databases, ranging from automobile license plate files, drivers' license files, NCIC wanted persons files, outstanding local warrants, and many others. The MDTs also typically contain an emergency button which the officer may activate to signal distress.

All relevant times regarding the incident are automatically recorded by the system, including the time the incident was received, transferred to the dispatch station, actual dispatch, unit arrival on the scene, transporting time, and the time the incident was closed. All unassigned incidents may be continuously displayed on a status monitor showing both the time and the priority of the incident.

The computer will suggest unit assignments and provide alert messages for officers responding to "hot addresses" (i.e., pre-coded addresses where officers have experienced problems).

The CAD systems can also be linked to vehicle locator systems, which display the geographic location of police cars on a map of the city. In combination, the two systems allow the dispatcher to actually see the location of the cars on shift and the location of their current assignments.

THE GENERAL CAPABILITIES OF NEW TECHNOLOGIES

The introduction new technologies in criminal justice enhance our general capabilities in many important respects. They:

—Increase the operational effectiveness and efficiency of existing criminal justice operations. They do this by speeding the processing and accuracy of existing capabilities, such as classifying and searching fingerprints with the new AFIS systems;

—Grant us new capabilities and tools not previously available; such as the introduction of DNA Fingerprinting, which gives us a new tool in the positive identification of suspects, and again the AFIS systems, which grants us the ability to search a latent fingerprint recovered from a crime scene against hundreds of thousands or millions of prints on file;

—Improve use of information for better allocation of resources, for targeting violent and repetitive offenders, and for the enhancement of our ability to invoke sanctions which address the dual objectives of crime control and equitable decisionmaking; and

—Expand our ability for social control by

--widening the breadth of social control (through such devices as electronic monitoring)
--expanding the depth of social control (through such technologies as depo provera.).

Given the expanding range of information systems, and the increasingly easy and broad access to the data, significant questions regarding the quality of the data also arise.

New technologies in criminal justice also raise important questions regarding basic ethical values and human rights. For example, they pose important challenges to the voluntary nature of consent obtained from imprisoned convicts, equal protection in the application of sanctions, our concepts of cruel and unusual punishment, and our basic notions of privacy and freedom.

Although the new technologies being applied in criminal justice grant us significant new capabilities, they are merely the means to an end. Society must continue to set the goals and objectives of the justice system, and these goals must contemplate the intended as well as the unintended consequences of technological innovation.

DEUXIEME PARTIE

PART II

LES APPLICATIONS DES ORDINATEURS
THE APPLICATION OF COMPUTERS

APPLICATION OF COMPUTERS IN POLICE

James M. Tien
Department of Electrical, Computer and Systems Engineering
Rensselaer Polytechnic Institute
Troy, New York 12180-3590, U.S.A.

Abstract

The paper is based on findings of a recently completed study assessing the status and impact of computer applications in U.S. law enforcement. Inasmuch as the applications have been most significant in the police, command, control, and communications (PCCC) area, the paper focuses on the PCCC technnologies of nine-one-one, computer-aided dispatch, automatic vehicle monitoring, mobile digital communications, and management information systems. In particular, the paper reviews the nature of these PCCC applications, especially in terms of the police functions they are intended to impact and the objectives they are intended to achieve; assesses the current status and actual impact of these applications; and outlines areas where further considerations are required.

Introduction

Two decades ago, the President's Commission on Law Enforcement and the Administration of Justice highlighted the computer as a means for improving the delivery of police services, especially in connection with the police command, control and communications (PCCC) area. The Commission (1967, p. 252) wrote:

> The entire police command-and-control function should be subjected to a basic reexamination taking full account of the promising new technologies offered by computers and communications links... An experimental program to develop a computer-assisted command-and-control system should be established with Federal support.

Since 1967, there has been a steady growth in the development and implementation of a wide variety of computer-based PCCC applications or technologies, including nine-one-one (911), computer-aided dispatch (CAD), automatic vehicle monitoring (AVM), mobile digital communications (MDC), and management information systems (MIS). Still, the successes of and approaches to PCCC applications seem to vary significantly from one police department to another, and a number of questions remain as to the benefits of such applications. Relying on a systematic assessment of these applications (Tien and Colton, 1980; Colton et. al., 1983), this paper both summarizes the status and impact of PCCC applications in U.S. law enforcement

and outlines areas where further considerations are required. While the focus of the paper is on the PCCC area, it should be noted that the computer has also had an impact in other law enforcement related areas, including office automation (e.g., word processing, spreadsheet, etc.), administration (e.g., financial, personnel, traffic citations, crime statistics, etc.) and investigation (e.g., crime analysis, modus operandi analysis, etc.). However, it can be stated that computer applications have been most significant in the PCCC area.

Before discussing the status of each PCCC application, it is helpful to consider the law enforcement functions that the PCCC technologies are intended to impact. Functionally, an effective PCCC system must be able to, on an immediate or tactical basis, monitor the status of the available police resources so that appropriate actions can be taken to respond to the needs that are identified. Additionally, on a longer term or strategic basis, the PCCC system must be able to manage the resources so as to ensure their productive deployment and use. In sum, the four PCCC functions are needs identification, status monitoring, response/adjustment, and resource management; these functions are further detailed in Fig. 1 in terms of specific PCCC actions and related time measures. It should be noted that the time measures are not drawn to scale and the composite time measures are not indicated. The critical composite time measures that should be borne in mind in considering the PCCC functions include dispatch delay time (i.e., sum of the operator and dispatcher processing times), response time (i.e., sum of the dispatch delay and travel times), and service time (i.e., sum of the travel and on-scene times). Additionally, although some police administrators do not consider the needs identification function as being in the purview of the command and control area, it should be pointed out that the identification of a need for police assistance is the basis for nearly all command and control decisions. Thus, it would be myopic, if not negligent, to omit needs identification as one of the PCCC functions.

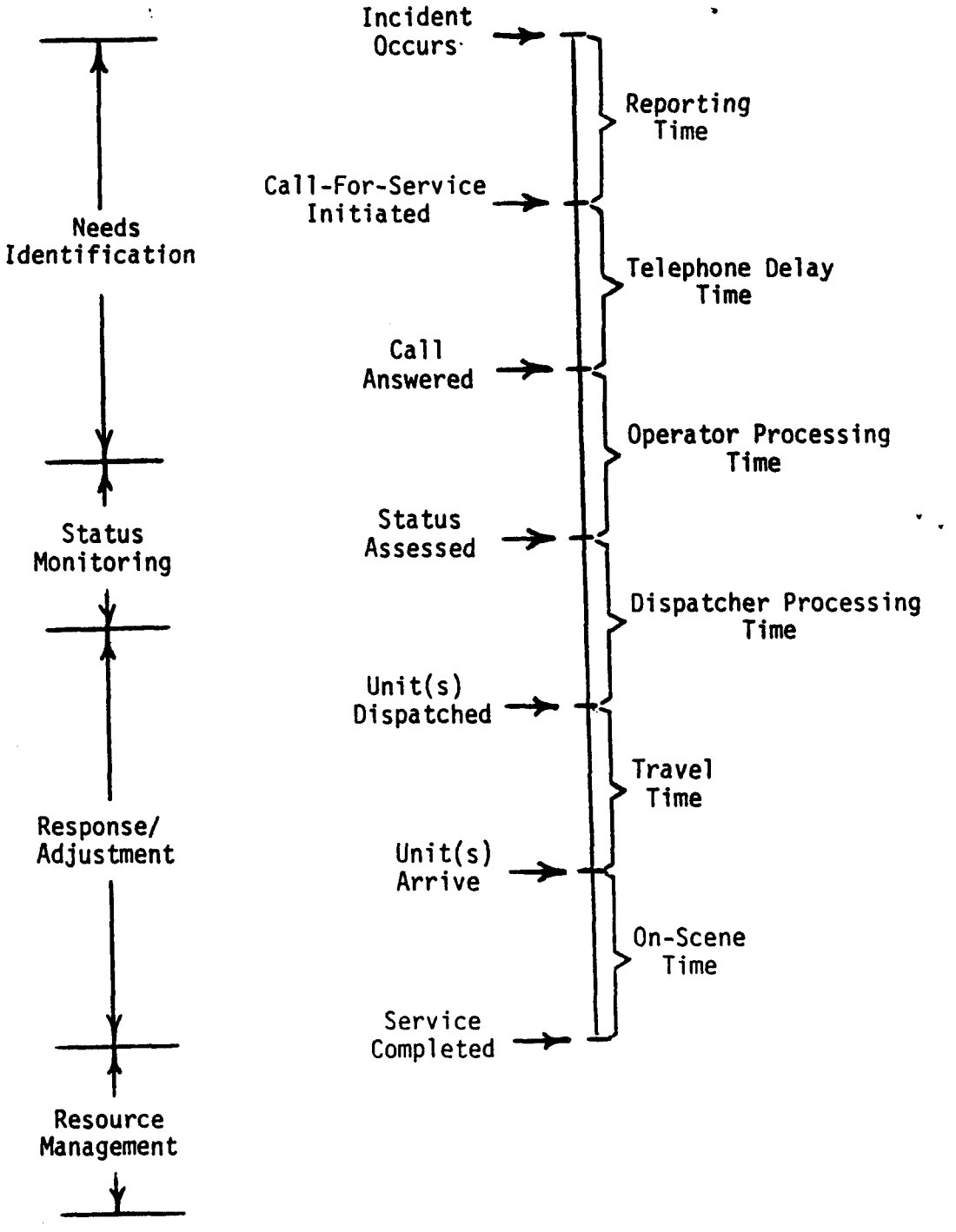


Fig. 1. PCCC Functions and Related Time Measures

The identified functions are obviously related and not always mutually exclusive. For example, an in-progress incident being detected by a police officer on patrol would simultaneously result in an identification of a need for police assistance, a change in the officer's non-busy status, and an appropriate response by the officer, together with other back-up assistance, if required. One way to distinguish between the four functions is to identify the communications means by which each individual function is effected. Needs identification is primarily communicated by telephone; other means include intrusion alarms, call boxes, and the police radio. Status monitoring and response/adjustment are typically effected by the same means (e.g., police radio, mobile digital, and computer-assisted communications) and include interaction between police officers in the field and in the communications center. The automatic vehicle monitoring system is primarily used for status monitoring, although it also relates to the other functions. Finally, resource management can be effected by a management information system that is fed by the data generated in the course of performing the first three PCCC functions and supported by appropriate resource allocation models.

Current Status

As noted earlier, the discussion in this section on the status of PCCC applications is primarily based on the findings of Tien and Colton (1980) and Colton et. al. (1983). In the ensuing discussion of the five PCCC-related computer applications, it is helpful to refer to Figures 2 and 3 which, respectively, summarize the stated objectives and the status of the applications as of 1981.

Nine-One-One (911)

In response to growing public and law enforcement demand, the American Telephone and Telegraph (AT&T) announced on January 12, 1968, that the three digit number, 911, was being reserved as the all-purpose emergency telephone number in the U.S. However, contrary to the telephone industry's established practice of forwarding those emergency calls placed by dialing "0" for operator assistance, AT&T viewed the

PCCC Applications	Stated Objectives
Nine-One-One (911)	• To have a simple to remember number for emergency purposes. • To have a central reporting potential for all emergencies. • To minimize the time required to dial and to reach an emergency operator. • To reduce the number of false fire alarms, bomb threats, and other malicious calls--by using the automatic number identification (ANI) option. • To allow for call-back and address identification in case a distressed caller gives inadequate information--by using the ANI and automatic location identification (ALI) options. • To overcome the fact that the municipal or jurisdictional boundaries do not usually coincide with the telephone company's central office exchange boundaries--by using the ALI and jurisdictional selective reporting (JSR) options. • To overcome the fact that the identified zones or precincts of the emergency response units do not usually coincide with the telephone company's central office exchange boundaries--by using the ANI, supplementary dispatch support data (SDSD), and internal selective routing (ISR) options. • To enhance an emergency operator's area familiarity, awareness of resource availability, and identification of redundant calls--by using the ALI, SDSD, and ISR options. • To minimize the level of transcription errors--by using the ANI, ALI, and automatic registered name identification (ARNI) options.
Computer Assisted Dispatch (CAD)	• To monitor and display better call-for-service related data. • To improve officer safety--by monitoring the status of officers and responding more rapidly in case of emergency. • To improve the response time (i.e., time between the receipt of a call until a unit arrives at the scene). • To improve the police service to the public. • To provide automatic or easy access to remote data files. • To improve the quality of the data maintained as a part of the dispatch process.
Automatic Vehicle Monitoring (AVM)	• To reduce response time--by reducing both dispatch and travel times. • To increase apprehension rates--by reducing response time. • To improve officer safety--by monitoring the status and location of police vehicles. • To improve dispatch efficiency and coordination--by providing the dispatcher with precise data and allowing for more effective coordination. • To improve tactical command and control--by having on-line direction of special tactical events (e.g., high speed chases, bank robberies, emergency deployment, and support for covert operations, etc.). • To improve patrol efficiency and effectiveness--by having available information regarding the location of the patrol force, and by the realization of patrol officers that they are being monitored. • To improve supervision of the patrol force--by having available timely information regarding the location and allocation of the patrol units.
Mobile Digital Communications (MDC)	• To reduce radio air time and expand the message handling ability of a radio channel. • To improve message security--by using digital signals which are harder to decipher than voice signals. • To allow for selective routing of messages--by using mobile digital terminals which could be addressed individually. • To allow for unattended message reception--by using mobile digital terminals which could record messages. • To increase officer safety--by using a pre-programmed and/or timed alarm key. • To increase officer effectiveness--by using mobile digital communications which facilitate and increase remote data base inquiries, resulting in potentially more "hits" (i.e., apprehensions and recoveries). • To increase dispatcher effectiveness--by using digital signals which could relieve the dispatcher from routine data inquiries and updates.
Management Information System (MIS)	• To integrate and analyse call-for-service related data--by using data generated by the other PCCC applications (i.e., 911, CAD, AVM, and MDC). • To make strategic resource management decisions--by using available data and resource allocation models.

Fig. 2. Stated Objectives of PCCC Applications

	Nine-One-One (911)	Computer-Aided Dispatch (CAD)	Automatic Vehicle Monitoring (AVM)	Mobile Digital Communications (MDC)	Management Information Systems (MIS)
Systems In Operation[1]:					
Over 1 Million	4	5	0	4	--
500,000-1 Million	7	19	2	9	--
250,000-500,000	Unknown	18	0	9	--
100,000-250,000	Unknown	18	1	7	--
50,000-100,000	Unknown	6	0	1	--
Less Than 50,000	Unknown	1	0	0	--
Total	About 800	67	3	30	--
Systems Being Installed	Unknown	15	0	5	--
Systems Previously Installed But Now Abandoned	Unknown	1	2	12	--

[1]Stated as a function of the population size of the city or county.

Fig. 3. Status of PCCC Applications: As of 1981

answering of 911 calls for public safety assistance to be outside of the scope of telephone business.

The shifting of the responsibility for processing the public's request for emergency assistance to the local government has resulted in two critical problems. First, local government officials are now burdened with the task of implementing and operating an integrated system for processing the disparate requests for emergency assistance, including requests for police, fire, ambulance, and other emergency services (e.g., suicide prevention, poison prevention, gas leakage, etc.). The establishment of such public safety answering points requires close cooperation between the various local agencies, and typically, this is not an insignificant political problem. The second problem is more technical in nature; it is caused by the fact that the telephone company's central office exchange boundaries do not usually coincide with the politically-defined municipal or jurisdictional boundaries. These two problems have to a large extent constrained the widespread adoption of 911. Although it has been almost two decades since the AT&T announcement and there were some 800 separate 911 systems in operation throughout the U.S. in 1981, only one out of every four persons could access a 911 system in 1981. The next decade should see a greater rate of growth as the political and technical problems are resolved.

As indicated in Fig. 2, the 911 objectives are for the most part almost exclusively supportive of the needs identification function of PCCC; they can be divided into two groups, according to whether the 911 system is basic (i.e., the first three objectives) or enhanced (i.e., the latter six objectives). The basic objectives emphasize easier and quicker access to emergency services, while the advanced objectives are based on sophisticated technical features. Most implemented 911 systems are, of course, basic systems. One of the most advanced 911 systems was recently implemented in Chicago, while another advanced system was scheduled to be implemented in Alameda County, California. At this time, an even more advanced 911 system -- based on a sophisticated network technology -- is being planned (Dimore et. al., 1987).

Computer-Assisted Dispatch (CAD)

CAD systems are those police dispatch systems which involve the computer in the process of handling calls for service from the public; in making decisions as to which patrol units should be designated to respond to the call; and in making appropriate resource adjustments. A number of police departments are currently using CAD systems, although the actual rate of implementation has been somewhat slower than initially predicted. The failure of some departments to establish operational CAD systems is an indication of the difficulties involved in implementing such systems. It is also indicative of the fact that the trend toward the use of CAD systems is still in an early phase.

In 1981, 67 operational CAD systems had been identified: 53 municipal systems and 14 county-wide systems. In addition, another 15 police departments were in the process of implementing CAD. CAD systems were most prevalent in large cities: as identified in Fig. 3, 31 out of the 65 cities with populations of more than 250,000 had them. However, with the explosive growth of powerful microcomputers and flexible software during the past six years, there has been an exponential increase in the number of installed CADs. Today, even a municipality of less than 25,000 in population can

afford a sophisticated CAD system. Unfortunately, there has not been a systematic and national study done since 1981 to capture the current status of CAD systems.

The stated objectives of CAD, as summarized in Fig. 2, reflect the range of functions encompassed in a CAD system. Most of the objectives focus primarily on the status monitoring and response/adjustment functions of PCCC. However, CAD also has the potential of contributing to the resource management function. In terms of the response time objective, there is some feeling by police administrators that CAD has helped; but, unfortunately, there are no data to justify this impression. In fact, the overall impact of the PCCC technologies on reducing response time has been disappointing (Colton et al., 1983). Concerning the outcome objective of improved police service to the public, it is very difficult to relate a technological change like CAD to such outcome measures as, for example, crime rates, especially since crime incidence is a product of a wide range of influences, including time of day, weather, economic condition, and neighborhood land use.

Automatic Vehicle Monitoring (AVM)

An AVM system provides a police dispatcher with real-time location estimates of every police vehicle, and, through its monitoring function, provides additional vehicle status information (e.g., "in pursuit", "enroute to scene", "driver door opened", etc.). Different technological approaches have been developed for locating vehicles as part of an AVM system: they include navigation (i.e., Loran C), trilateration, signpost and dead-reckoning methods.

AVM for urban applications is a relatively new technology. The development of commerical AVM systems was not begun until the late 1960s, and only a handful of cities have installed police AVM systems since then. Signpost systems were installed in Montclair (California), Stamford (Connecticut), and Huntington Beach (California). Both the Montclair and Stamford systems are reportedly no longer in operation, primarily because of the high cost of operation and maintenance, together with no significant

benefits. As of 1981, St. Louis (Missouri) and Dallas (Texas) were the only large police departments which had implemented an AVM system; St. Louis had a computer-assisted dead-reckoning system, while Dallas had implemented a trilateration system. While AVM technology has improved significantly since 1981, very few additional AVM systems have been installed in police departments. Instead, AVM-type technology is being introduced into the private auto market, where dead-reckoning techniques are allowing individuals to track the location of their auto on a detailed screen displayed street map.

The stated objectives of AVM, as summarized in Fig. 2, are primarily supportive of the status monitoring function of PCCC, and are secondarily related to the response/adjustment and resource management functions. Although AVM has not reduced response time to emergency calls for service, it has improved the tactical command, control and supervision of police units. Unfortunately, this latter benefit is perceived in a negative manner by the police officers; they are apprehensive about having "cowbells for cops".

Mobile Digital Communications (MDC)

MDC allows direct digital transmission between police vehicles (which are equipped with mobile digital terminals) and headquarters. Although military applications of MDC have been on-going for many years, its introduction into police operations dates only to the early seventies. In fact, most police applications have been quite limited in scope; they have typically been experimental in nature and it is fair to say that there has not been a widespread adoption of MDC technology. There has, however, been several studies assessing the potential of MDC in law enforcement, as well as somewhat formal evaluation studies of three test systems -- in the Hennepin County (Minnasota) Sheriff's Department, the Minneapolis (Minnesota) Police Department, and the Oakland (California) Police Department.

Congestion of police radio frequencies has been the primary reason for introducing MDC into police operations. In fact, the National Advisory Commission on Criminal Justice Standards and Goals (1973, p. 566) predicted that MDC would have the capability of reducing frequency congestion by 40 to 50 percent. A second major reason for the interest in digital communications is that many law enforcement data bases are now computerized, and a patrol unit equipped with a digital communication capability can automatically access these data bases if a suitable switching device (i.e., a minicomputer) is provided at the base station. It is felt that easier data base access would in turn contribute to enhanced officer safety as well as increased "hit" rates. It is interesting to note, however, that the above two MDC objectives are somewhat conflicting. That is, on the one hand, transmitting digitized instead of voice signals may alleviate the frequency congestion problem, but, on the other hand, providing automatic access to remote data bases would tend to increase the number of data base inquiries and thereby aggravate the congestion problem. Ironically, because of interference between voice and digital signals (when both are simultaneously transmitted on the same radio channel), as well as the increased digital traffic (due to increased access to remote data bases), the installation of an MDC system has typically required the addition of another radio channel (used exclusively for digital transmission). This requirement, together with a significant yearly maintenance cost (which can be as much as one third of the cost of the entire MDC system), contributed to a situation in 1981 where over 25 percent of the installed MDC systems had been abandoned -- see Fig. 3. The situation since 1981 has improved significantly, commensurate with the improvement in the MDC technology. Unfortunately, as stated earlier in the case of CAD systems, there has also not been a systematic and national study done since 1981 to capture the current status of MDC systems.

A complete list of MDC objectives is contained in Fig. 2; it shows that MDC supports both the status monitoring and response/adjustment functions of PCCC.

However, in actual practice, all implemented MDC systems have status monitoring potential, while only a few of them are capable of effecting the more general response/adjustment function, including, for example, the direct dispatch of patrol units using only digitally transmitted instructions.

Management Information Systems (MIS)

The 911, CAD, AVM, and MDC applications are all primarily supportive of the tactical PCCC functions of needs identification, status monitoring, and response adjustment. Although these same applications can provide the necessary data to support the strategic PCCC function of resource management, the experience to date has been dismal -- the computer-based data from these applications have been only intermittently analyzed, if at all. What is missing is a computer-based management information system (MIS) which, as indicated in Fig. 2, could automatically, and, on an ongoing basis, integrate and analyze the tactically generated data, and derive results that could be used to make strategic resource management decision. As of 1981, there were no such PCCC-related MIS in existence. There are, of course, several general police management and/or crime analysis systems, but they are typically limited in scope and not linked to the PCCC components. For example, although the Virginia Beach Police Department had both a CAD system and an Automated Police Management System, the two computer-based systems were not linked and did not encompass the range of PCCC functions.

As stated above, a general MIS should perform functions other than the PCCC function of resource management. Moreover, in order to effectively assist in resource management decisions, the computer-based MIS must include resource allocation algorithms which could descriptively and/or prescriptively identify appropriate allocation alternatives. Although there are no PCCC-related MIS, there do exist several resource allocation models which have been tested and used for resource management decisions. These models include the Patrol Car Allocation Model (Chaiken and Dormont, 1975) and the Hypercube Queuing Model (Larson, 1975).

Further Considerations

Fig. 4 summarizes the reported impacts of specific applications on the four PCCC functions; the summary is in terms of three subjectively defined impact categories (i.e., significant, moderate, and minimum). It is seen that the needs identification function is, as expected, being significantly impacted by 911, but it should also be significantly impacted by CAD (which can better record and verify the needs), MDC (which could be used to transmit needs that are identified while on patrol), and MIS (which, through analysis of historical data, could better identify those characteristics of need that are important for response purposes and which must, therefore, be carefully recorded). While the status monitoring function is the most impacted function, it should still be impacted by MIS (which, through analysis of historical data, could identify those variables that should be better monitored). Likewise, the response/adjustment function could benefit from an ongoing MIS analysis. The resource management function is the least impacted function; as discussed earlier, it requires a PCCC-oriented MIS which could automatically analyze the 911, CAD, AVM and MDC generated data with the aid of tested resource allocation and scheduling algorithms.

In sum, the PCCC functions of needs identification, status monitoring, response/adjustment, and resource management must be further supported and sustained before an effective PCCC system can be realized. More explicity, the power of the computer has not been exploited to enhance the PCCC functions; as discussed below, an integrated, proactive and flexible PCCC system could and should be developed.

Integrated System

The PCCC applications are individually reviewed in this paper not only because they are relatively distinct in purpose and focus, but also because, in practice, they have been implemented on an individual basis and in an independent manner. To the author's knowledge, no police agency has yet implemented an integrated PCCC system which links all the various PCCC applications or elements. Fig. 5 identifies an integrated PCCC

Specific Applications	PCCC Functions			
	Needs Identification	Status Monitoring	Response/ Adjustment	Resource Management
Nine-One-One	Significant			
Computer Assisted Dispatch	Minimum	Significant	Significant	Minimum
Automatic Vehicle Monitoring		Significant	Minimum	Minimum
Mobile Digital Communications		Significant	Moderate	
Management Information Systems				Minimum

Fig. 4. Summary of PCCC Impacts

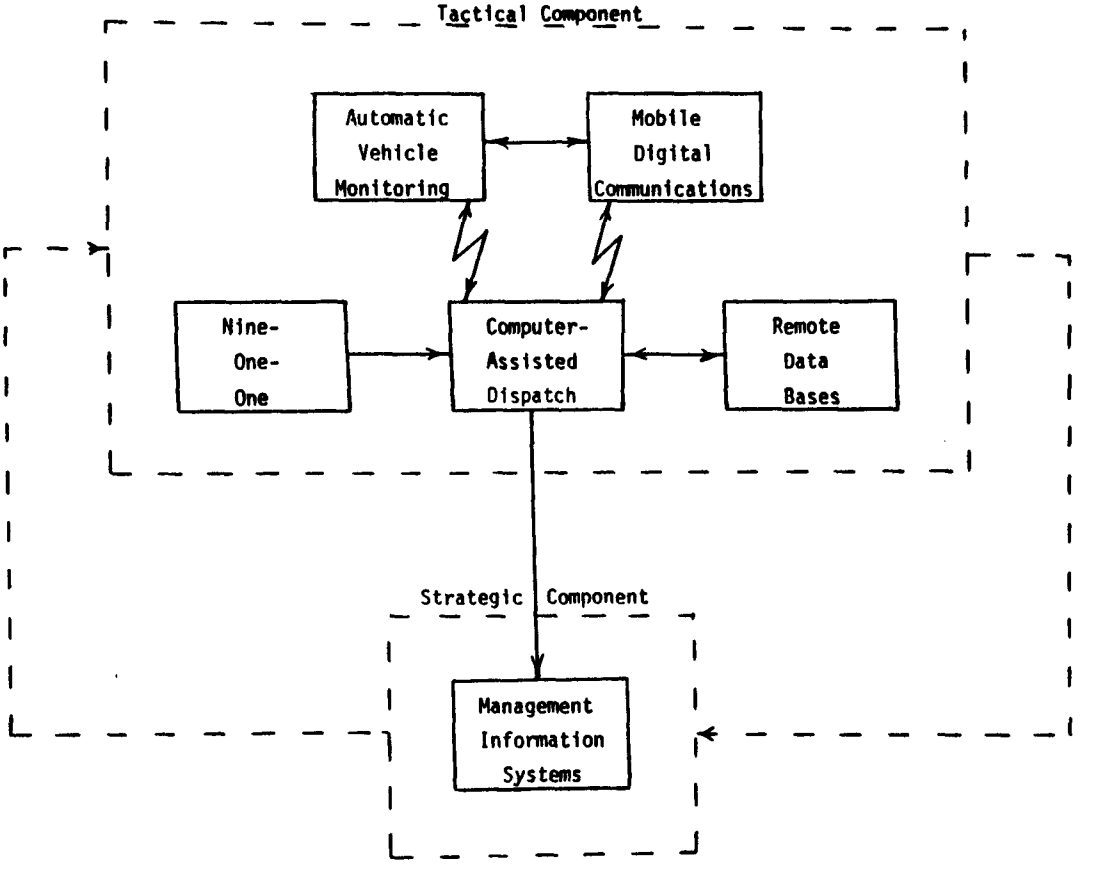


Fig. 5. An Integrated PCCC System

system, assuming that the 911, CAD, AVM, MDC and MIS applications are effective and pertinent to the PCCC functions. Briefly, the system includes 911 information that is entered into the CAD computer, which also i) interacts digitally with the AVM and MDC systems; ii) serves, if necessary, as a switching machine for MDC inquiries to remote data bases; and iii) provides pertinent data to the MIS element. The AVM and MDC systems are actually a part of the same mobile system. Similarly, it may be cost-effective for the MIS to share the same CAD computer.

Aside from the physical links between the different PCCC elements, it is important to recognize that the PCCC system can be divided into two components. The first component -- comprised of 911, CAD, AVM, MDC, and the remote data bases -- primarily supports the tactical PCCC functions of needs identification, status monitoring, and response/adjustment. The second component -- comprised solely of MIS -- primarily supports the tactical PCCC function of resource management. As shown in Fig. 5, the two components are interactive; the tactically generated data are analyzed by the MIS, which, in turn, produces results that would strategically impact the tactical component.

It is obvious that because of budgeting constraints a police department cannot implement the total PCCC system at one point in time. It is, therefore, necessary to prioritize the various PCCC elements from an implementation perspective. A quick glance at Fig. 5 suggests that CAD is the heart of the integrated PCCC system; that is, among other factors, the CAD computer can be the host computer for all the other PCCC elements or applications. Thus, CAD should be the first PCCC application to be implemented, followed perhaps by 911, AVM/MDC, and MIS. Although any of the applications can stand alone, proper sequencing of their implementations would lead to greater effectiveness and overall compatibility. For example, implementing AVM before CAD would require that the cursor be manually positioned by the dispatcher, whereas with CAD the positioning could be automatically performed by the CAD computer. Further, dispatching personnel trained in the ways of a computer operation within a CAD

context are less likely to be resistant to AVM, which would be a natural add-on to the CAD system.

A final comment is required concerning the integrated PCCC system shown in Fig. 5. Although the depicted system is conceptually relevant for all police departments, it is obvious that not all departments would require such an encompasing system. Some departments may only require a microcomputer-based system; others may not need an AVM or MDC system. Indeed, some very small departments may only require an automated telephone answering system which would allow officers to answer incoming telephone calls while in their patrol cars.

Proactive System

To a large extent, the computer-based PCCC applications have to date simply replaced previous manual opeations. The potential of a computer has not been fully realized. A computer-assisted dispatch system, for example, can be used not only to assist in the traditionally reactive response/adjustment function, but also to provide the necessary information for a more proactive decision-oriented dispatch operation. More specifically, a proactive or, in Larson's (1985) term, intelligent CAD would be effective in:

- checking the validity of calls for service;
- efficiently allocating patrol resources in a dynamic manner to account for fluctuating manpower levels;
- standardizing dispatch assignments among dispatchers and between dispatcher actions and departmental policies;
- improving police service by incorporating strategies which, for example, increase neighborhood identity or provide better response to emergency situations;
- incorporating complex mathematical models for purposes such as estimating patrol unit location and managing queues of calls for services; and
- collecting and analyzing statistics which are useful to police administrators.

Another promising area for proactive decision-making is the management of police demand. Recognizing that some 86 percent of all calls for police service are non-critical in nature (i.e., not requiring immediate response) and that citizen satisfaction is a function of expectation, Cahn and Tien (1981) proposed that the demand for police services be managed and that alternative methods (i.e., other than the traditional method of dispatching a costly patrol unit) be used to respond to non-critical calls for service, provided the callers are forewarned and appropriately advised. Proactive management of police demand can reduce or shift random demand peaks and may even lower the demand level, so as to allow for a more efficient and effective allocation of limited police resources, thus increasing the productivity of these resources. Whatever management of demand and alternative response procedures can be identified can be straightforwardly translated into computer-based algorithms which could be on-line to assist complaint operators and dispatchers in the performance of their PCCC responsibilities. One such algorithm was recently developed by Tien and Chou (1985) for estimating the amount of time that a caller for police service can be expected to wait before a police car can arrive at the scene; this conditional response time would be communicated to the caller by the complaint operator instead of the traditional (and unrealistic) statement of "we'll have a car right out."

Flexible System

The modern PCCC system is totally dependent on the computer. Computer technology, meanwhile is undergoing major changes, and technological advances are occurring on a daily basis. Any PCCC system must, therefore, remain flexible to take advantage of and be compatible with these advances. Changing computer technology will impact the PCCC functions in three areas.

First, the decreased cost of computers, together with increased computing capabilities, should make computer-based PCCC systems available to even the smaller police departments. Efficient memory media, device miniaturization, parallel processing,

superconductivity of materials at room temperatures, and sophisticated (including artificial intelligence) software are just five reasons for this amazing development in computer technology. Second, computer networking and distributed processing should allow PCCC functions to be decentralized and yet coordinated. In a distributed system, data communication and data base management functions can be performed by a number of small computers which are both physically connected together and software coordinated in their functions. The data base could also be organizationally and physically distributed, which would be advantageous in terms of flexibility, management and privacy. Third, sophisticated terminals should facilitate interactions with the computer-based PCCC system. These terminals include intelligent interactive graphics terminals, optical character readers, and voice data entry terminals.

While technological advances are always enticing and vendors -- who have been the primary agents of technology transfer (Colton and Tien, 1979) -- will always speak highly of PCCC applications which make use of these advances, caution should be exercised; the new advances should be carefully tested and evaluated before their widespread transfer and adoption in PCCC systems.

References

Cahn, M. F., and J. M. Tien, *An Evaluation of the Wilmington Management of Demand Program*. Washington, D.C.: National Institute of Justice, 1981

Chaiken, J. M. and P. Dormont, *Patrol Car Allocation Model: User's Manual*. New York, NY: The Rand Corporation, 1975.

Colton, K. W. and J. M. Tien, "Technology Transfer of Computer-Based Applications in Law Enforcement," *Journal of Technology Transfer*, Vol. 4, Fall 1979, pp. 63-67.

Colton, K. W., M. L. Brandeau, and J. M. Tien, *A National Assessment of Police Command, Control, and Communication Systems*. Washington, DC: National Institute of Justice, 1983.

Dimone, V. P., D. Elsinger, and V. Perez, "911: A Good Thing Just Gets Better," *Bell Communications Research Exchange*, July/August 1987, pp. 3-7.

Larson, R. C., *Hypercube Queuing Model: User's Manual*. New York, NY: The Rand Corporation, 1975.

Larson, R. C., "The Future of Police Emergency Response Systems," *National Institute of Justice Reports*, March 1985.

National Advisory Commission on Criminal Justice Standards and Goals, *Police.* Washington, D.C.: U. S. Government Printing Office, 1973.

President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime in a Free Society.* Washington, D.C.: U. S. Government Printing Office, 1967.

Tien, J. M. and K. W. Colton, "Police Command, Control, and Communications in the United States: Evaluating Computer-Based Technology," *Proceedings of the 1980 International Conference on Security Through Science and Engineering,* Berlin, West Germany, September 1980, pp. 71-77.

Tien, J. M. and C. Y. Chou, "CART: A Decision Support Model for Estimating Conditional Response Times," *Proceedings of the 1985 IEEE International Conference on Cybernetics and Society,* Tucson, Arizona, November 1985, pp. 259-264.

APPLICATION OF COMPUTERS IN CORRECTIONS

James M. Tien
Department of Electrical, Computer and Systems Engineering
Rensselaer Polytechnic Institute
Troy, New York 12180-3590, U.S.A.

Abstract

All but a handful of the 50 states in the U.S. have implemented or are in the process of implementing some version of a computer-based or automated correctional data system (ACDS) for the storage and retrieval of offender-related data. In fact, many such systems have been upgraded or changed several times since their inception, which, in some cases, date back to a dozen years or more. The current status of ACDSs is reviewed in this paper. It can be stated that current ACDSs are indeed data -- rather than information -- systems; that is, their capabilities are quite limited. Future considerations, including a proposed distributed automated correctional information system (DACIS), are also included.

Introduction

The creation of the Law Enforcement Assistance Administration (LEAA) in the Omnibus Crime Control and Safe Street Act of 1968 has significantly accelerated the development and proliferation of automated correctional data systems (ACDSs) for the storage and retrieval of offender-related data. It is estimated--based on an extrapolation of data contained in the LEAA Grant Management Information System--that close to 20 million dollars of LEAA's total budget have been expended on ACDSs; this estimate includes 11.9 million dollars for the Offender-Based State Corrections Information System (OBSCIS) program. Together with substantial state level funding, the total estimate of ACDS-related spending could be well in excess of 200 million dollars. Further, the adoption of ACDSs by certain counties (e.g., St. Louis County and San Diego County) and local jails (e.g., Washington, DC) would also serve to bolster this conservative estimate.

An obvious question is whether ACDSs have been effective or, more precisely, cost-effective? A recent study funded by the National Institute of Justice (Tien et. al. 1982) attempted to answer this question or, at least, to begin to answer the question. Although the paucity of available information about ACDSs -- indeed, there has, to date, been no impact evaluation or cost-effective analysis of an ACDS -- prevented Tien et. al.

(1982) from providing an explicit answer at this time, they were able to undertake a critical review or assessment of existing ACDSs. The assessment was national in scope and was based on available ACDS-related reports, structured telephone interviews, and brief visits to 26 ACDS sites. While this paper is primarily based on Tien et. al. (1982) and Tien (1986), it also draws from a recent effort by Tien and McClure (1986) in which they consider technical approaches for making computers more effective in public organizations.

Finally, it should be emphasized that the focus of this paper is limited to those automated systems which deal with offender-related data. It also includes those systems affecting probationers, parolees and detainees which have been implemented as a part of or in conjunction with systems dealing with incarcerated, sentenced offenders. Conversely, computer useage in such support functions as office automation (e.g., word processing, spreadsheet, etc.) and administration (e.g., financial, inventory, personnel, etc.) is not considered herein, although it obviously constitutes a critical and sizeable application of computers in corrections.

Current Status

As of 1980 (Tien et. al., 1982), the 50-state corrections agencies had a total of 311 years of ACDS experience, with an average of 6.2 years and a median of 5.0 years. These figures are significant in that the field of automation is one in which experience counts. Frequently, the first system installed by a corrections agency was subject to special problems resulting from the fact that the agency staff had not yet learned what the computer could do for them. Subsequent systems were often more successful due to the added sophistication of both users and data processing staff. In total, 40 states, Washington, D.C., the Federal Bureau of Prisons and numerous regions and localities had ACDSs which were "operational" in 1980. (By operational, it is meant that at least one offender-based application was operating and officially in use by the appropriate agency staff.)

Although current ACDSs run on a wide variety of different central processing units or mainframes, the IBM 370 and its look-alikes (such as Amdahl or Itel equipment) dominate the field, with 28 installations. Six states have, in addition to their large mainframes, minicomputers located in their institutions; in most cases, these are used for peripheral applications such as inmate fund accounting or psychological test scoring. The majority of the ACDSs are written in COBOL; some have parts written in assembler language as well.

An important characteristic of any automated data system is the extent to which on-line processing is available. On-line processing refers to the ability to interact with the computer system through a terminal device such as a teletype or a cathode ray tube (CRT). The functions of data entry, data editing, data retrieval, and data or file updating may be performed either on-line (i.e., via the terminal) or through batch processing. Thirty-five of the state-level ACDSs operating in 1980 had some degree of on-line capability; that is, at least one of the above four stated functions was being performed via the terminal. Further, 18 of the 29 systems which were undergoing development in 1980 were scheduled to have some degree of on-line capability. The function of data or file updating deserves further explanation. When a system has on-line file updating (i.e., the files are modified at the time that the data are entered), it is known as a real-time system. Real-time systems provide the advantage that a piece of data can be retrieved and used as soon as it is entered rather than being unavailable until the batch file update takes place. Thus, if data are entered in a timely fashion, real-time systems can provide up-to-the-minute information. Surprisingly, while there are several real-time informational needs in corrections (e.g., inmate count taking and transportation scheduling), there were no real-time ACDS applications implemented in 1980, although a few of them had the capability to do so. Perhaps, it is because real-time systems are quite costly, in that they are much more complex to program and require a higher degree of data security.

The potential value of an ACDS can be partially gauged by the number and types of applications it can perform. Twenty of the more prominent inmate- or offender-based applications are considered in Fig. 1; they include the following:

- *Admission Reporting* refers to the recording and reporting of an offender's admission activity. Nearly all of the ACDSs either have or are planning this application.

- *Offender Record Retrieving* refers to the ability to retrieve an offender's records using keys other than the agency's assigned identification number (e.g., name or FBI number). Thirty systems have this ability and 12 more are planning it.

- *Classification/Program Assignment Reporting* consists of maintaining offender profile data in a form in which it can be promptly retrieved and used as a basis for assessment, classification and/or program assignment. This is one of the few applications that may directly benefit the offender, in the form of improved classifications and assignments. At least 1 of the 12 states having this application has reported such an improvement. Sixteen additional states are planning to add the application.

- *Problem/Special Needs Monitoring* involves producing reports which identify medical or psychological problems or special situations (e.g., enemies, educational skills and religious dietary requirements) that may affect the placement and/or assignment of offenders. Four systems have some form of this application (i.e., reporting on some subset of the possible problems or needs) and 13 are planning to add it.

- *Test Scoring* refers to automatically scoring answer sheets for psychological, vocational and intelligence tests. It is interesting to note that 5 of the 11 systems that have this application run it on a separate microcomputer (using a proprietary software package) that is not linked to the main ACDS. Five systems are planning to add this application.

- *Reporting of Program Participation* refers to collecting information on program participation and reporting program participation by program and/or by offender. Twenty-two states have this application and 14 more are planning to add it.

- *Disciplinary Reporting* involves collecting and reporting data on disciplinary infractions. Although associated with an offender's record, the information collected for this application has also been used to pinpoint an institution's trouble spots. Eighteen systems have this application and 13 are planning to add it.

- *Offender Tracking* refers to updating records regarding any change in the status and location of an offender. This application is present in 35 systems and planned for 10 more; for many of them, it represents the core or primary function of their ACDS.

- *Movement Reporting* refers to reporting offender movement between institutions and between status categories. Nearly all the systems either have this application or are planning to add it.

Does The ACDS Include The Following Application Areas?
(Y = Yes, N = No, P = Planned, S = Separate System)

1 = Admission Reporting, 2 = Offender Record Retrieving, 3 = Classification/Program Assignment Reporting, 4 = Problem/Special Needs Monitoring, 5 = Test Scoring, 6 = Program Participation Reporting, 7 = Disciplinary Reporting, 8 = Offender Tracking, 9 = Movement Reporting, 10 = Transportation Scheduling, 11 = Parole/Discharge Eligibility Date Calculation, 12 = Legal Status Reporting, 13 = Parole Hearing Scheduling, 14 = National Statistical Reporting, 15 = Inmate Accounting, 16 = Health Services Tracking, 17 = Visitor Control Reporting, 18 = Victim Restitution Reporting, 19 = Probation Status Reporting, 20 = Parole Status Reporting, 21 = Total "Yes" Replies.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Alabama	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N[1]	N[1]	12
Alaska	P	P	N	P	N	N	N	P	P	N	N	P	P	P	N	N	N	N	P	P	0
Arizona	Y	Y	N	N	YS	N	Y	N	Y	N	P	Y	Y	Y	N	N	N	N	N	Y	9
Arkansas	P	Y	P	P	P	P	P	N	Y	N	Y	Y	P	Y	P	P	N	N	N	Y	6
California	Y	Y	YS	N	N	P	N	Y	Y	N	N	N	N	Y	PS	N	N	N	N	Y	7
Colorado	Y	Y	Y	P	Y	N	Y	Y	Y	N	P	Y	P	Y	YS	N[2]	N	Y	N	Y	12
Connecticut	Y	Y	N	P	N	N	N	Y	Y	N	P	Y	P	P	N	N	N	N	P	P	5
Delaware	P	P	P	P	P	P	P	P	P	N	P	P	P	P	N	P	N	N	P	P	0
Florida	Y	Y	P	N	N	Y	Y	Y	Y	N	Y	Y	N	Y	YS	P	N	Y	Y	Y	13
Georgia	Y	Y	P	N	YS	Y	Y	N	Y	N	Y	Y	Y	Y	P	P	N	N	Y	Y	12
Hawaii	Y	Y	N	N	N	P	P	Y	Y	P	Y	Y	Y	Y	N	N	N	N	N	Y	9
Idaho	Y	P	N	N	N	P	N	P	Y	N	N	Y	P	N	N	N	N	N	N	P	3
Illinois	Y	Y	P	Y	N	Y	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	N	N	9
Indiana																					
Iowa	Y	N	N	N	N	P	P	Y	Y	N	P	Y	N	Y	N	N	N	N	N	Y	6
Kansas	Y	Y	N	N	N	Y	N	Y	Y	N	N	Y	Y	Y	P	N	P	N	N	Y	9
Kentucky	P	P	P	P	N	P	P	P	P	N	N	P	P	Y	N	N	N	N	N	N	1
Louisiana	Y	Y	P	P	N	Y	N	Y	Y	N	N	Y	YS	Y	YS	P	N	N	Y	Y	11
Maine	Y	N	Y	N	N	Y	N	Y	Y	N	Y	N	N	Y	N	N	N	N	Y	Y	9
Maryland	Y	N	P	P	P	P	P	Y	Y	N	P	P	P	P	N	N	P	P	P	P	3
Massachusetts	Y	P	N	N	N	N	N	P	P	N	N	N	N	N	P	P	N	N	N	P	1
Michigan	Y	P	N	P	Y	Y	P	P	P	N	P	Y	Y	Y	Y	YS	P	N	N	N	8
Minnesota	Y	Y	P	P	P	P	Y	Y	Y	N	P	Y	Y	Y	P	P	Y	N	Y	Y	11
Mississippi	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	P	P	N	Y	Y	Y	15
Missouri	Y	Y	Y	P	N	Y	Y	Y	Y	N	Y	Y	P	P	P	P	P	N	N	N	9
Montana	Y	Y	Y	N	N	Y	P	Y	Y	N	Y	Y	Y	N	Y	Y	N	N	Y	Y	13
Nebraska	Y	Y	N	P	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	YS	N	P	Y	N	Y	14
Nevada	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	1
New Hampshire	Y	Y	N	N	N	Y	Y	N[3]	N[3]	N	Y	Y	N	Y	N	N	N	N	N	P	7
New Jersey	Y	P	N	N	N	N	P	Y	Y	N	P	P	N	Y	N	N	N	N	N	YS	5
New Mexico	Y	Y	Y	N	N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	11
New York	Y	Y	N	N	N	P	N	Y	Y	N	N	Y	N	Y	YS	YS	N	N	N	N	8
North Carolina	Y	P	P	N	N	Y	Y	Y	Y	P	Y	Y	Y	Y	N	Y	N	P	Y	Y	12
North Dakota																					
Ohio	Y	Y	N	N	YS	N	N	Y	Y	N	N[2]	Y	N[2]	Y	N	N	N	N	N	N	7
Oklahoma	P	Y	P	N	YS	P	Y	Y	Y	P	N	Y	Y	N	P	P	N	P	P	P	7
Oregon	Y	N	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	YS	N	N	Y	Y	Y	13
Pennsylvania	Y	N	N	N	N	N	N	Y	Y	N	N	Y	N	Y	N	N	N	N	N	N	5
Rhode Island	P	P	P	N	P	P	P	P	P	N	N	P	P	N	N	N	N	N	N	N	0
South Carolina	Y	Y	P	N	N	Y	Y	Y	Y	P	Y	Y	Y	Y	Y	P	N	N	N	N	11
South Dakota	P	P	N	N	N	N	N	P	P	N	N	P	N	P	P	N	N	N	N	P	0
Tennessee	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	N	YS	YS	P	15
Texas	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	N	Y	Y	P	Y	N	N	N	11
Utah	Y	P	P	P	N	P	P	P	Y	N	N	Y	P	P	N	N	N	N	Y	Y	5
Vermont	Y	P	N	N	N	Y	P	P	Y	N	Y	P	P	Y	N	N	N	N	N	N	5
Virginia	Y	Y	P	N	N	P	P	Y	Y	P	Y	Y	P	P	P	N	N	N	Y	Y	8
Washington	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	P	N	N	Y	Y	15
West Virginia																					
Wisconsin	Y	N	N	N	YS	Y	YS	N	Y	N	N	Y	N	Y	P	N	N	P	YS	YS	9
Wyoming																					
Washington, DC	Y	Y	N	N	N	YS	N	Y	Y	N	N	Y	Y	P	P	N	Y	N	N	Y	9
St Louis Co.	Y	Y	N	N	N	N	N	Y	Y	N	N	Y	N	N	N	N	N	Y	Y	Y	8
San Diego Co.	Y	Y	P	N	N	N	N	Y	Y	N	Y	Y	N	Y	N	N	N	Y	N	N	8
Total "Yes"	41	30	12	4	11	22	18	33	40	3	20	37	19	31	11	5	3	8	15	24	387

[1]Alabama Board of Pardons and Parole has a separate computer system which provides this application, using the same data base as the OBSCIS system.
[2]Application exists but is not being used.
[3]Only one institution or facility has this application.
[4]Washington has three separate computer systems which perform the various applications.

Fig. 1. Offender-based ACDS applications: as of 1980.

- *Transportation Scheduling* involves scheduling and/or reporting offender transfers both within the correctional system and outside of it (e.g., to court, to a doctor's office). Only three states have even a limited form of this application and each of these only produces a transfer report; no explicit scheduling is done. Five states are planning to develop this application.

- *Parole/Discharge Eligibility Date Calculation* involves partial or complete computer calculation of dates on which an offender is eligible for parole and/or discharge. Although many agencies claim this function is too complex to be automated, 20 agencies have done so and 9 more are planning to do so. In most cases, not all calculations can be done by the system; the more complex and involved calculations must be done by hand.

- *Legal Status Reporting* includes reporting offenders who are eligible for parole hearings or other review processes and providing relevant status and history information for those hearings. Thirty-seven systems have this application and 8 more are planning to add it.

- *Parole Hearing Scheduling* involves scheduling parole hearings and/or reporting of outcomes of those hearings. Nineteen systems have this application and 13 are planning to add it.

- *National Statistical Reporting* involves general data for the National Prisoner Statistics (NPS) and/or Uniform Parole Reports (UPR) programs; the data may be generated either in the form of printed reports or in machine readable form. Twenty-eight systems have this application and 10 more are planning to add it.

- *Inmate Accounting* involves processing offender bank accounts and commissary purchases. Twelve state agencies have this application; however, in 6 of these agencies it is a separate system rather than a part of the ACDS, a situation which is not unreasonable since an offender's financial record is generally not pertinent to the other ACDS applications.

- *Health Services Tracking* includes recording an offender's medical treatments. Five systems have developed such an application and 13 are planning to add it.

- *Visitor Control Reporting* includes tracking those individuals who are allowed to visit an offender and/or how many visits an offender has received. Three agencies now have this application and 5 are planning to add it.

- *Victim Restitution Reporting* includes recording and tracking an offender's participation in a victim restitution program. In many states, there are no victim restitution programs; where programs do exist, they are frequently administered by agencies other than the correctional agency. Of the 12 state corrections agencies which do administer victim restitution programs, 6 of them have the victim restitution application on their ACDS while 4 more are planning to add it.

- *Probation Status Reporting* involves tracking and reporting the status of a probationer, including any violations. Fourteen state agencies having responsibility for probation supervision have this application, while 5 more states are planning to add it.

- *Parole Status Reporting* involves tracking and reporting the status of a parolee, including any violations. Twenty-two of the 33 corrections agencies having both

a responsibility for parole supervision and an operational ACDS have this application.

In regard to ACDS experience, the below statements summarize the state of such knowledge; they are grouped into four sets of issues -- input, process, outcome and systemic issues. The input issues focus on the system's background and development; the process issues focus on the system's operation or performance; the outcome issues focus on the system's immediate impacts, especially in relation to its users; and the systemic issues focus on the system's broader impacts, as gauged from a total systems viewpoint. The input issues include:

- The absence of a formal needs assessment (and related functional specification) effort has been a major reason for ACDSs -- especially their earlier versions -- to have failed or not to have lived up to expectation.
- The lack of user involvement throughout the ACDS development process (i.e., planning, designing, testing, implementing, operating and maintaining) has resulted in a lack of user support of ACDS at both the data input and data utilization ends of the ACDS.
- While LEAA -- in particular OBSCIS -- funds have been critical in the development of ACDSs, they have not prevented the "reinventing of the wheel."
- Several problems can occur when a corrections agency does not have direct control over its ACDS mainframe.
- Several problems can occur when data elements and procedures are not first clarified, codified and/or standardized.
- Problems can occur in data base design if data files are sequential; if the data base management system (DBMS) is not well understood; if the historical data file cannot be directly accessed by statistical analysis packages; and if no purging criteria exist for historical data.
- Creation of an initial data base for an ACDS is a major undertaking and one whose difficulty has frequently been underestimated.
- User involvement and elaborate approaches to ACDS system testing have been minimal.
- System documentation has been poor to nonexistent, causing problems in system operation and maintenance.
- Most agencies have not carried out intensive user training, which in turn has contributed to decreased user support.

The process issues include:

- ACDS performance has been negatively affected by the relatively low rank of data processing administrators, the high turnover of data processing staff, and frequent reorganizations within the corrections agency.

- ACDS operation has been negatively affected by impractical designs, programmers reassigned to other tasks, and contractors who are unfamiliar with corrections.

- Lack of software maintenance has resulted in some severe problems.

- System security has been quite lax and the potential for misuses and abuses of offender data exist.

- Reliable system cost data have been uniformly unavailable.

- Although for legal and practical reasons the manual files must duplicate at least a portion of the ACDS files, redundant manual files (which could be displaced by the ACDS) have been maintained.

- Real-time (versus delayed) file updating and local (versus central) data entry have been topics of controversy.

- Although improving, data quality -- in terms of factual accuracy, entry accuracy, completeness, and timeliness -- has been a problem.

The outcome issues include:

- Most offender-based applications have been operating at the "data" level, producing listings or summaries of data.

- While the operational or tactical needs of corrections are being met (at least partially), the more strategic needs of planning, research and management have, for the most part, not been met.

- While they have been reporting to the NPS and UPR reporting programs, corrections agencies have problems with the reporting formats and see no benefit in return for their efforts.

- While the ACDS applications have resulted in significant time savings for corrections staff, they have barely begun to make use of the power of the computer.

- The attitudes of users toward ACDS have, for the most part, not been positive, primarily because of a lack of perceived benefits of the ACDS.

- The attitudes of some administrators toward ACDS have been less than positive and have caused some severe problems.

- ACDS goals have been ambitious, ambiguous and not measurable; their attainment have been mixed.

The systemic issues include:

- Very few ACDSs have interfaced with other criminal justice information systems.

- Transfers of ACDS technology have been few (i.e., mostly of the Basic OBSCIS Software Package) and with mixed results.
- There has been no technology transfer from other environments (e.g., inpatient hospital systems) similar to that of corrections.
- Except in helping to prove fair treatment in a handful of litigation cases, ACDSs have not been used to protect an offender's right to have adequate and fair treatment.
- Except in a few cases, ACDS data have not been used to shed light on corrections issues, and ACDSs have not assisted in the monitoring of an agency's compliance with correctional standards.

In sum, what can be said about the status of today's ACDSs? It can be stated that current ACDSs are indeed *data* -- rather than *information* -- systems; that is, their capabilities are quite limited. It should, however, be recognized that computer applications in related areas of criminal justice are no more advanced than that in corrections; for example, law enforcement applications have also not utilized the full potential of the computer and they continue to be data -- instead of information -- driven (Colton and Tien, 1979; Colton et. al., 1983). Similarly, the above listed statements regarding ACDS experience to date are also reflective of automation experience in other public sector organizations (Tien and McClure, 1986).

Future Considerations

In considering the future progress in ACDS development and growth, four important issues must be addressed. First, The issue of user support is paramount, inasmuch as organizations cannot derive the benefits planned from their automated systems if those systems do not have user support. In fact, implementing an automated data system without user support can have far reaching detrimental effects. When employees have a negative attitude regarding the system, error rates increase and acts of sabotage may occur. Specifically, i) data are not supplied to the system (eventually the files become out-of-date or inaccurate); ii) the system is not used or is used improperly; and iii) staff continue to use the old methods while being expected to keep up the new system (thus they feel overworked and their resentment of the new system is increased).

These conditions may cause morale to drop and staff turnover to rise, ultimately decreasing the productivity of the organization.

The problem of lack of user support stems from the way in which an automated system is implemented, the effects of an automated system on the organization, and the users' perceptions of the system and its effects. It has long been recognized that any change in the organization creates uncertainty which generates resistance. In the introduction of an automated system, there are other causes of resistance as well. Among them is the fact that automation or computerization always necessitates the transfer of some power from the user department to the data processing department. Also, managers resist because functional lines, which were formerly clear, become blurred by the introduction of the automated system. Further, the increase in volume of data brought about by computerization overloads managers with data and data processing-related tasks, causing a decrease in their job performance, at least by traditional standards. Users at all levels of the organization are afraid of the way in which the system may change their jobs, especially when their skills (which have been developed over the years) are no longer needed and new skills must be developed. Finally, certain characteristics of the automated system itself may tend to irritate users and thus reduce their support; among them are rigidity of the system, obscure input and output codes, and errors in the system.

The many conditions cited above which cause a lack of user support need not occur. Various steps can be taken to mitigate or eradicate these problems; they can be grouped into i) those that apply through all the phases of planning, developing and implementing the automated system, ii) those that apply principally at the planning phase, iii) those that apply principally at the development phase, and iv) those that apply principally at the implementation phase. While the specific steps are detailed in Tien et. al. (1982), it should be noted that if they had been followed in the development of the existing ACDSs, many of the observed problems would not have occurred. Additionally,

DeBrabander and Thiers (1984) advocate the prescence of a third party to overcome the power asymmetry and semantic gap between users and data processing specialists.

The second is one that concerns federal support. It has already been stated that federal support for ACDS-related activities during the past decade has been very beneficial; the number of ACDSs would not be as many and the state of ACDS development would not be as advanced if it were not for federal support. Certainly, the limited support -- an estimated 20 million dollars of LEAA monies -- provided by the federal government could not have by itself resulted in such widespread impact: indeed not, what the federal support has been able to do has been to leverage state and local spending in this area. Thus, in this case, the federal role has been quite appropriate and effective; it has not only stimulated state and local interest in ACDSs, but also provided direction and guidance.

Given the demise of the LEAA and the general cut-back in federal funding of public programs, what should the federal role be in supporting ACDS development? It is recommended that the federal government support four types of ACDS-related activities. First, the federal government should continue to support basic ACDS research and development efforts, including the assessment of correctional data needs and the development of offender-based application modules (that is, basic application programs which must be modified to meet the specific needs of a particular agency). Second, the federal government should expand its support of technical assistance assignments to states which require them; the assignments could range from general ACDS audits or reviews to more basic, but limited, coding assistance. Third, the federal government should expand its support of a national clearinghouse for ACDS-related information; the clearinghouse should actively seek out information and should also sponsor a yearly national meeting for ACDS administrators to meet each other and to be exposed to recent ACDS developments. Fourth, the federal government should institute an ACDS-related

evaluation program, which would provide the needed feedback with regard to what works, what doesn't work, and why.

Privacy and security constitute the third issue which merits attention in connection with future ACDS development efforts. Ever since the establishment of statewide correctional institutions, correctional data systems have always existed, both to track inmates within the system as well as for administrative and other functions. With the computerization or automation of the correctional data system, access to inmate information is quicker, if not easier, thus security and privacy are concerns in any data system, manual or computerized, correctional or other.

In regard to ACDSs, it should be noted that while no significant privacy and security problems have occurred to date, the potential is there, since system security is lax. Further, privacy and security problems could become even more exarcebated in situations where an ACDS is automatically or electronically interfaced with other automated data systems, including other criminal justice systems. Fortunately, as one systems designer at a correctional institution said, "There just does not seem to be much market value for stolen offender data." If adequate privacy and security measures are not implemented and this "market value" rises, then it is quite possible that the frequency of privacy and security abuses would go up.

The fourth and final issue concerns the direction that future ACDS development should take. As depicted in Fig. 2, it is recommended that current ACDSs, which are predominantly data systems, be upgraded into information systems and, eventually, into knowledge systems. In this evolutionary process, data systems support only transactions processing and provide only data. Information systems support transactions processing, tactical decision making, and strategic decision making, and provide both data and information (i.e., processed data). Knowledge systems support transactions processing, tactical decision making, strategic decision making, and policy decision making, and provide data, information, and knowledge (i.e., processed information). In particular, the

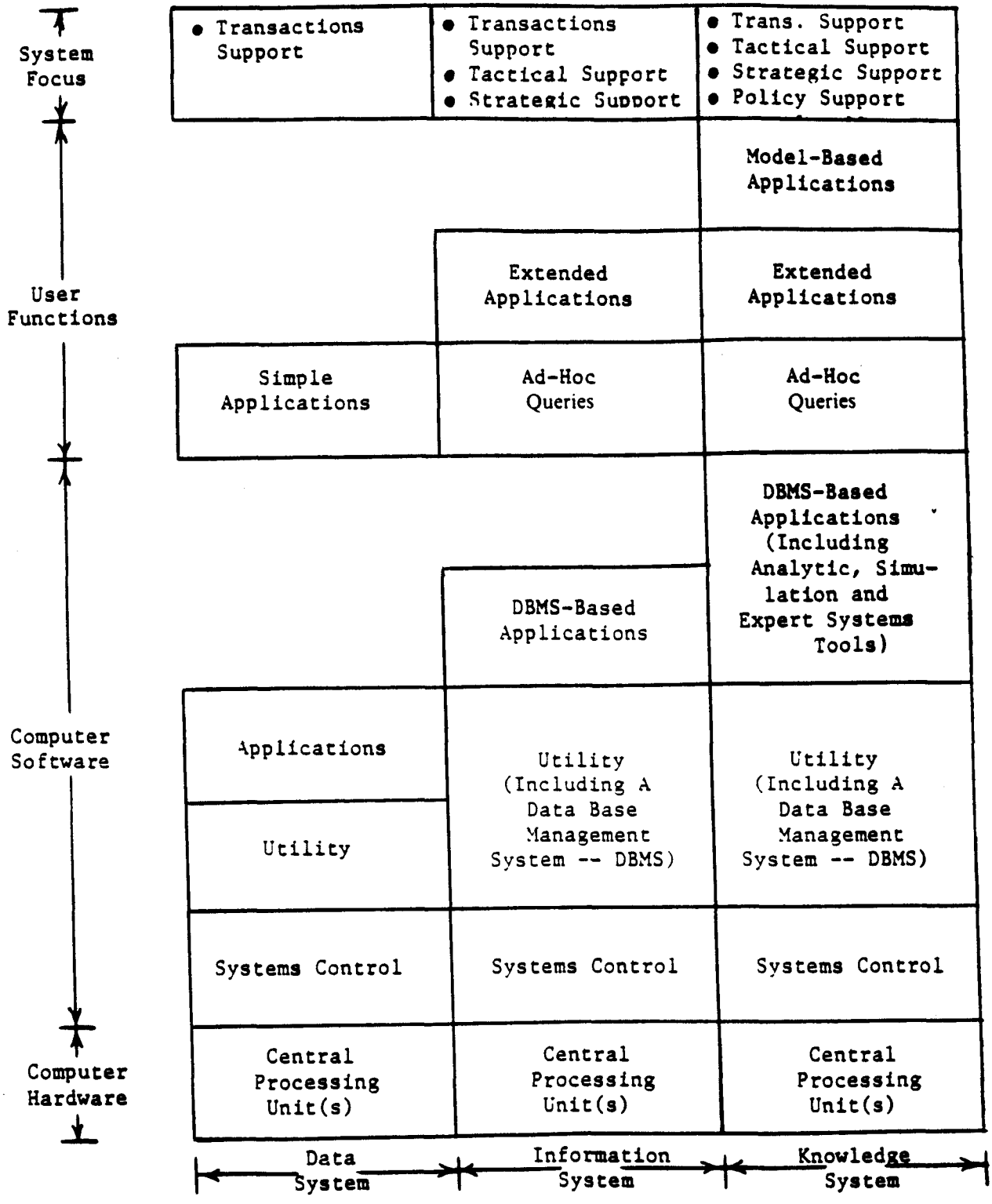


Fig. 2. **Data, Information, and Knowledge Systems**

data base management systems (DBMS) can help to process data into information, and the extended DBMS-based applications programs can help to process information into knowledge, especially through the use of analytic, simulation, and expert systems tools.

Fig. 2 also highlight another fact -- that, in the future, the emphasis should be on software, not hardware. Software is the new driving force in the computer industry. Software costs is skyrocketing, while hardware cost is on a steady decline. It is for this reason that software should be developed on a hardware-independent operating system.

While future ACDSs should be total knowledge systems, what could be an effective ACDS in the interim? Given the current status of ACDSs and a knowledge of correctional information needs, an appropriate interim system must recognize that i) users have a need for decision-oriented information (not just listings or summaries of data elements), and ii) users have a need to "control" their data (and not to give it up to a distant data storage device that is under someone else's -- most likely data processing's -- jurisdiction). The latter need is based on the perception that data constitute power, a perception that is held in many organizations, both public and private.

Fortunately, the state of computer technology is such that the above two needs can be very appropriately met. First, the DBMS can be a very effective analyzer or processor of data into information. Second, a distributed network of computers (including mainframes, minicomputers and microcomputers) can allow for a data base in which data can be geographically distributed, with each data set residing in a computer (or "node") at or near the location where the data are entered; yet, all the data in such a network can still be viewed as one data base and are accessible from all nodes, subject to prespecified security constraints of the network. Further, the processing of data can also be carried out locally, on a distributed basis. In sum, the system that would be effective in the corrections environment, especially in a large environment, is a distributed automated correctional information system (DACIS).

A final consideration is whether and how to interface DACIS with other criminal justice data systems. Given that any automated correctional system should be electronically or automatically interfaced with other criminal justice data systems (especially since they require some of the same data elements), the problems of privacy and security, although real, can be overcome by limiting access and monitoring all exchanges between systems. In regard to a DACIS interface with another criminal justice data system, DACIS could treat the other system as just another node (if it contains just one computer) or another network (if it itself is a distributed system); thus, one day an automated criminal justice information system could be characterized as a multi-network system.

References

Colton, K. W. and J. M. Tien, "Technology Transfer of Computer-Based Applications in Law Enforcement," *Journal of Technology Transfer,* Vol. 4, Fall 1979, pp. 63-76.

Colton, K. W., M. L. Brandeau, and J. M. Tien, *A National Assessment of Police Command, Control, and Communication Systems*. Washington, DC: National Institute of Justice, 1983.

DeBrabander, B., and G. Thiers, "Successful Imformation System Development in Relation to Situational Factors Which Affect Effective Communication Between MIS-Users and EDP-Specialists," *Management Science,* Vol. 30, January 1984, pp. 137-155.

Tien, J. M., S. Rosenberg, F. DiCesare, and P. B. Mirchandani, *National Evaluation Program: Automated Correctional Data Systems*. Washington, DC: National Institute of Justice, 1982.

Tien, J. M., "On Automated Correctional Data Systems," *Computers, Environment and Urban Systems,* Vol. 10, No. 3/4, 1986, pp. 157-163.

Tien, J. M. and J. A. McClure, "Enhancing the Effectiveness of Computers in Public Organizations Through Appropriate Use of Technology," *Public Administration Review Special Issue: Public Management Information Systems,* Vol. 4-6, November 1986, pp. 553-562.

TROISIEME PARTIE

PART 3

IDENTIFICATION DES INDIVIDUS

IDENTIFICATION OF PERSONS

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS: AN OVERVIEW

by
Thomas F. Wilson, Ph.D.
SEARCH Group, Inc.

Presented at the
XXXVIIIe Cours international de criminologie
NOUVELLES TECHNOLOGIES ET JUSTICE PENALE

Montréal, le 18 août 1987

Introduction

The term "revolutionary" is attatched to the word technology with alacrity—so much so that we that we now hear it as the white noise of advertising language. If, however, we mean by revolutionize that which profoundly and fundamentally changes, then we have to call what Automated Fingerprint Identification Systems (AFIS) technology has done to criminal identification revolutionary. AFIS has, in fact, revolutionized law enforcement capability to identify offenders and solve crimes. Before AFIS, when a fingerprint was found at a crime scene, and no suspects were known, there was little or no chance that the print would be matched to one in law enforcement files. In fact, in most cases, there would not be a search. The problem was that there are too many prints in the file and not enough people to do the searching.

AFIS has changed the fingerprint processing with state-of-the-art computer searching and matching. Identification rates have increased dramatically in jurisdictions that have implemented AFIS. The sensational California "Night Stalker" serial murder case was

broken by a latent print lifted from a stolen car. At the California Department of Justice, the print was entered into the state's new AFIS, and the hit on alleged serial killer Richard Ramirez was made in a matter of minutes. In similar fashion, the first latent print run against San Francisco Police Department's AFIS data base had been the subject of thousands of hours of manual searching over an eight-year period. That print belonged to the killer of Miriam Slamovich, a World War II concentration camp survivor, who was shot point blank in the face by an intruder in her home in 1978. Her assailant left a full, perfect print at the scene, but with no suspect and no other clues, there was little chance of making a match on existing file prints by conventional manual searching methods. Police detectives agressively pursued the case, however, and when the AFIS system was implemented in 1985, it matched the print in six minutes. Slamovich's alleged killer was in custody the same day.

This new generation of AFIS technology has given law enforcement agencies around the country a capability to identify suspects in cases that previously would have gone unsolved. AFIS technology finally has brought the use of fingerprint evidence into the twentieth century and promises to spur clearance rates more than any other single law enforcement tool. AFIS may well have the greatest impact of any technological development on law enforcement effectiveness since the introduction of computers to widespread use in the criminal justice system in the 1960's.

What makes AFIS so revolutionary? The heart of AFIS technology is the ability of new computer equipment to scan and digitize fingerprints, to automatically create a spatial geometry or

map of the unique ridge patterns 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 compare a new fingerprint with massive collections of file prints in a matter of minutes and can make identifications that previously were possible only through a time-consuming and error-prone process of manual comparison. My presentation today is intended to provide a brief introductory look at this new technology. I will try to explain in non-technical terms how AFIS technology works, how it differs from manual fingerprint search and comparision methods, how it has changed the ten-print and latent print identification functions in law enforcement, and what impact the technology is having on law enforcement capability to identify criminal perpetrators with the use of AFIS.

MANUAL FINGERPRINT PROCESSING

An examination of manual fingerprint processing will provide not only an understanding of how fingerprints were processed prior to AFIS, but also show the problems that had to be overcome. The classification system describe below is the predominant manual classification systems now in use in most law enforcement agencies.

Manual Fingerprint Classification

The unique and unchanging patterns of ridge detail on the friction ridge skin found on fingers of all primates have provided law enforcement agencies throughout the world with a means of positive

identification. Fingerprint comparison has become the universal method of verifying identity and ensuring the integrity of criminal record systems. To support the investigation and identification functions, criminal record repositories and identification bureaus have established files of fingerprints that are often massive. Generally, these files are of two types. The most extensive files are "rolled" inked impressions maintained on ten-print cards filed according to some classification system. Typically, these fingerprint cards are prepared at the time of an individual's arrest and are used to verify his identity and to determine whether he has a prior criminal record. Ten-print cards also are often submitted in connection with certain employment or licensing applications to determine whether the applicant has a criminal record that would legally bar him from being hired or obtaining the license.

A second general type of fingerprint records are so-called "latent" fingerprints (that is, they are sometimes not visible to the naked eye) developed as a result of criminal investigations. These prints generally are obtained at crime scenes or from documents or material related to the crimes. Latent fingerprints developed in this manner usually occur as isolated single finger impressions or as fragmentary parts of two or three adjacent fingers. They are often of poor quality. Nevertheles, latent prints have linked suspects to crime scenes and have been used as evidence to convict. In England in1905, a fingerprint taken from a bloody cash box was used as evidence against a known suspect, Albert Statton, in a murder case. That latent prints' 34 points of minutiae led to Stratton's conviction and hanging.

From the very beginning of fingerprint retention systems it was apparent that it would be necessary to create a system that would not require incoming search prints to be compared with every fingerprint card already on file. Manual comparison and elimination of prints is a time-consuming and expensive process. As file sizes increase, such searches become more difficult until, at some point, a successful match becomes improbable, if not humanly impossible. From its inception until recent years, therefore, fingerprint identification methodology has been predicated upon the necessity of dividing file prints into classification categories based upon distinctive ridge patterns to eliminate the necessity of searching the entire file.

In the final years of the nineteenth-century, Sir Edward Henry, an Englishman who served as Inspector General of Police in India and as Commissioner of London's Metropolitan Police, developed the first successful fingerprint classification system. His system was installed in New Scotland Yard in 1902. The Henry System, which, with modifications and improvements, remains the predominant classification system in use today, classified fingerprints by assigning each finger to one of two primary fingerprint pattern types—whorl or non-whorl. The fingerprints were represented as a unit rather than as individual fingers by assigning to each ten-print set an alphanumeric designation reflecting the pattern characteristics of all ten fingers. Thus, two pattern types times ten fingers yielded 2^{10} or 1,024 classification categories into which to subdivide fingerprints.

Given the size of the files when Henry installed his system in New Scotland Yard in 1902, the Henry System was a manageable and

workable system—notwithstanding the fact that the most common classification category was found to contain about 25 percent of all fingerprint records. However, considering that the FBI now maintains approximately 23 million criminal fingerprints and the state of California maintains approximately 7.5 million fingerprint cards in its state repository, it is obvious that the basic Henry System would not work for today's file sizes. As a result, the history of fingerprint technology development until very recently has been one of devising extended classification subcategories to enable the Henry System to accommodate increased numbers of prints. In recent years, the portion of fingerprints in the most common classification category has decreased from 25 percent to 6 percent. Nevertheless, 6 percent of the FBI's files is still a very large number to search. In addition, as increasing file sizes have necessitated more complex rules for subclassification, human judgment has come more into play, with the result that particular technicians might classify fingerprints differently. Misclassification, of course, results in the risk of missed identifications.

The inherent limitation for latent print searching in the Henry System is that it classifies the ten fingers as a unit rather than as separate fingerprints. A single latent print cannot be filed or searched as a unit. In manual classification systems, therefore, if the results of comparing latent prints with the prints of known suspects are negative, the latent impressions usually are filed for future reference in an "unsolved latent" file.

Manual Fingerprint Processing

Manual fingerprint processing begins when fingerprint cards are submitted to identification bureaus or criminal record repositories—primarily as a result of an arrest or a criminal investigation or in connection with applications for employment or licensing. These ten-print cards are searched against existing criminal fingerprint files to determine whether the individual has a prior criminal record. Whether the search is for criminal justice or noncriminal justice purposes, the process begins with a so-called "name search." The individual's name, date of birth, sex and other identifying information are taken from the incoming fingerprint card and searched against a master name index. In most of the states, this part of the search process is fully or at least partially automated. If a match or a close match is found in the name index, the file fingerprint cards associated with the match candidates (usually only one or two cards per search) are retrieved and are manually compared with the incoming search card by a fingerprint technician to verify positive identification. In the processing of criminal fingerprint cards, the great majority of successful matches, or "hits," are made in this relatively quick and inexpensive way—name search verified by manual fingerprint comparison. Statistical information developed recently by the state of California[1] indicated that approximately 47 percent of arrested persons are found to have prior criminal records through the process of identification by the name search and verification by fingerprint comparison.

[1] *Tracking Juvenile Recidivists: Three Options for Creating Statewide, Longitudinal Records of Juvenile Offenders*, California Department of Justice, Bureau of Criminal Statistics and Special Services, August 1985, pp. 36-37.

If an identification is not made on the basis of the name search, the fingerprints are classified by a trained technician and a "technical search" (actual fingerprint comparison) is performed to ensure that the individual has not escaped identification by using an alias or as a result of clerical error in conducting the name search. Manual technical searches are extremely time-consuming and expensive. Although the classification of the fingerprints limits the search to a portion of the entire file, it is still necessary to compare the search card with all of the file cards within that classification, plus additional cards on either side of the classification to compensate for possible classification errors in the search print or file prints, or both. In large files, this can entail a review of hundreds of file cards. But, for criminal prints, these searches may be quite productive. According to the California statistics noted above, 47 percent of arrestees are idenfified by name search. By conducting a technical search of the entire file, an additional eight percent of those arrested will be discovered to have criminal records, bringing the total to 55 percent.[2]

Fingerprints submitted for noncriminal justice purposes, such as employment and licensing (applicants), yield very few "hits," yet require the same kind of technical search. Statistics developed by the FBI[3] indicate that only about five percent of employment and licensing applicants are identified as having previous criminal

[2]ibid, pp. 36-37.

[3]*A Study to Identify Criminal Justice Information Law, Policy and Management Practices Needed to Accommodate Access to and Use of III for Noncriminal Justice Purposes,* prepared for the FBI by SEARCH Group, Inc., September 1984, p. 58.

records. An additional 1.5 percent of the applicants are identified through technical searches, bringing the total to 6.5 percent. This means that 95 percent of all applicant fingerprint cards must be classified and manually searched (i.e., those not identified by name search), and that the hit rate on them will only be one or two percent. It is hardly surprising, therefore, that most state record repositories process noncriminal justice cards by name search only, regarding technical searches as unjustifiable because of their high cost and low productivity.

The essential problem, as stated earlier, is that latent fingerprints cannot be classified and searched under the Henry System, whcih needs all ten fingers. Thus, latent prints usually are searched only against the file prints of known suspects and, if there is no match, the prints are placed in an unsolved latent file. If there is an extremely high priority on the case, the latent print may undergo a file search with little or nothing to limit the search. Such efforts are known as "cold searches" and the rare resultant hits are referred to as "cold makes."

AFIS TECHNOLOGY

It took the maturation and sophistication of three critical elements to make AFIS the revolutionary technology it is today. The first element was the selection of digital computer. Translating fingerprint ridge and minutiae data into binary data provided the mechnaism necessary to provide the speed to search thousands or millions of fingerpints and the memory sufficient to store the data. The second critical element was the development of scanners

sophisticated enough to capture and translate the inked fingerprint image into digital data. The third element necessary for the AFIS revolution was the sophistication of the algorithms for searching and matching. The result of utilizing sophisticated scanners and algorithms with high speed digital computers in the 1980's was the creation of an ability to scan fingerprint impressions and automatically extract identifying characteristics in sufficient detail to enable the computer's searching and matching algorithms to distinguish a single fingerprint from thousands or even millions of file prints that have been similarly scanned and stored in digital form in the computer's memory. This concept of computerized digital image processing has eliminated the necessity for time-consuming and error-prone manual classification and comparison of fingerprints. It has greatly increased the speed and accuracy of ten-print processing and has made it possible to conduct cold searches on latent prints against very large fingerprint files. Thus, it has significantly improved the efficiency of the criminal identification process and has added an important new crime-solving capability to the law enforcement arsenal.

Fingerprint Scanners

What is perhaps most extraordinary about these new systems is the sophistication and intricacy of the scanning and mapping algorithms, which convert the unique spatial relationship of a fingerprint's ridge endings and ridge bifurcations, called "minutiae points," and additional ridge direction and ridge contour information into a digitized representation of the fingerprint. In a ten-print to

ten-print search on good quality rolled impressions, the computer plots the spatial relationship of 90 or more minutiae points for each finger, a number high enough to distinguish the uniqueness of that print from all others and to make it virtually certain that the computer will be successful in matching the candidate prints with the prints in the file. Latent prints have less minutiae data for the scanners to map, but the systems are able to work with only a portion of the minutiae map and can score matches with an average of only 15 to 20 minutiae points. One law enforcement agency reported a hit on a fragmentary print which yielded only eight minutiae points.

In preparing fingerprints to be searched, the AFIS system provides a capability for enhancing the prints, correcting for breaks in the skeletal pattern, cuts or breaks in the ridges caused by scars or burns, or other kinds of interference caused by dirt, blood or chemicals. The system can even provide an evaluation of the quality of the print, disqualifying inferior prints. This print enhancement capability is especially important in searching latent prints, since it enables an experienced technician to fill in missing or blurred portions of print fragments to produce more useful images for the computer to work with.

Digitized Searching

Equally sophisticated are the search algorithms used in the new AFIS systems to convert the minutiae data and ridge direction and contour data extracted by the scanner into a unique binary code that the computer can use in searching its files. The search algorithm

determines the degree of correlation among the location, angle and relationship of the minutiae of the search print and the minutiae patterns of file prints. The computer is not actually comparing fingerprint images in its search; it is conducting a mathematical search that will provide a candidate list of those binary codes in the file most similar to the binary code used in the search.

The mathematical search is carried out by an AFIS system component called a matcher, which can search a candidate print against the file prints at a rate of 500 to 600 prints per second. Matchers operate in parallel, each taking a portion of the data base. As file size increases, matchers may be added so that there need be no diminution of searching speed. Average searching time is, however, relative to a number of factors including the number of matchers employed, time spent in preparing and enhancing the prints, entering demographic data to limit the number of prints to be searched, and the time the candidate prints wait in the system's queue (temporary memory storage) prior to the search process. Search time for a ten-print search (rolled print to rolled print comparison) in a file of under 500,000 is a matter of minutes. For a latent search, the search time averages about one-half hour.

In its quest for a mathematical match, the computer employs a scoring system that assigns points to each of the criteria used in the match. The technician sets a threshold score above which he has assurance that a match has produced a hit. At the conclusion of the search, the system reads out the candidate list, the number of which is defined by the technician as a search parameter. Based on parameters set in the scoring system, the score of the candidate in

the number one position, if high enough, indicates that the match is probably a hit. If the score is low, it means that the system has chosen the selected number of candidates most similar to the search print, but there is little probability of a hit. The optimal functioning of an AFIS would produce a hit on the candidate in the number one position every time and the score would be high enough to leave no doubt. For the 10-print search, fingerprint experts are reporting that in approximately 98 percent of the prints that are matched, the candidate's score met the threshhold and was in the large number one position.[4] This level of accuracy, which is made possible by the number of minutiae available from rolled prints, eliminates the necessity of comparing the search prints with the file prints of the other candidates on the list. If all of the candidates fall below the threshold score, then there is a high probability that the candidate's prints are not in the system. Nevertheless, some AFIS systems have policies calling for review of some of the candidate prints in such cases as an added precaution against missed identifications. For example, California Department of Justice's California Identification System (Cal-ID) policy requires comparison of the search prints with the file prints of the candidate in the number one position if there is a sizable differential between the scores of the number one and two positions. For latent searches, where there are fewer minutiae to work with, comparisions may be made on as many as three to five candidates. Again, as a policy matter, Cal-ID checks only the number

[4]*Proceedings of a SEARCH National Conference on Automated Identification Systems.* Sacramento: SEARCH Group, Inc. (forthcoming). The conference was conducted in Kansas City, Missouri, February 26-28, 1986, and included managers of operational Automated Fingerprint Identification Systems, who were in general agreement on performance capabilities of new AFIS technology.

one candidate for verification in property crimes, but checks up to three candidates for person crimes. Cal-ID's policies governing the verification process are the result of careful study and testing of its AFIS performance relative to candidate position and hit frequency. Such policy determinations, in general, factor technical performance, cost, time, and the priority given to particular kinds of crimes.

Finally, it is important to note that an AFIS makes no final decisions on identity. While the score may virtually guarentee 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.

DIGITAL IMAGE RETRIEVAL

It is a very time-consuming process to compare candidate prints with the file prints, even with AFIS. Remember, an AFIS candidate list is composed of an operator-selected number of prints most like the search print. Even if the scores for all candidates are not above the threshold, the operator wants to check to be sure. That normally entails going to the hardcopy fingerprint files, pulling the candidate cards and returning to the AFIS monitor to make comparisons. The latest technological development in AFIS—image storage and retrieval—addresses that problem. The digital image essentially is a by-product of the initial conversion process by which

the search print is read into the system in digital form. New image storage and retrieval technology allows the digitized fingerprint images used to plot the minutiae to be stored on an optical disk and retrieved at a later time for comparing candidate lists with the search prints. It allows the digitized search prints and the retrieved image of the candidate file prints to appear side by side on the operator's screen for comparison. This gives the technician the distinct advantage of not having to leave the terminal to retrieve the prints. Without image storage and retrieval, the process entails going to the hard-copy file of rolled prints to collect the prints of candidates to be compared with the search prints. As a less costly alternative to image retrieval, some law enforcement agencies use microfilm and microfiche readers to speed the verification process.

Sharing AFIS Data

Can an AFIS computer in other jurisdictions share its data with an AFIS in another jurisdisdiction? The answer is that if they are from the same vendor, that vendor has the technical capability to allow the two systems to share data. If the AFIS computers are not from the same vendor, then the answer is no, the computers cannot "talk" to each other directly because the algorithms and communications protocols are different. The technology is incompatible simply because the computers of the various vendors were designed differently. Thus, one AFIS computer cannot search the files of another AFIS computer of a different manufacturer. Some technologists are quick to point out that a "black box" (a piece of equipment that translates the protocols and algorithms of one

vendor to those of another) is soon to be developed and operational. That assumes that vendors are willing to share the secrets of their algorithms. Such as technology could be developed, but it is perhaps more the case that practically terms the vendors have no economic incentive to do so at this time. At this writing at least, there is no such interface available.

Compatibility among AFIS computers of different vendors is not the direction this technology seems to be heading. Instead, AFIS technology is moving toward the development of a national standard for the interchange of fingerprint data and images. Since an AFIS computer works by having an input device read and digitize a rolled fingerprint image, what the computer needs from another jurisdiction is digitized fingerprint image data and personal identification information, or demographics, to limit the search. Simply stated, an AFIS computer just needs good fingerprint images that it can read on its own terms. On August 25, 1986, the American National Standards Institute accepted the standard entitled "Data Format for the Interchange of Fingerprint Information" (NBS/ICST-1-1986), which was developed by the Institute for Computer Sciences and Technology of the National Bureau of Standards (NBS). Most observers believe that this NBS standard for electronically transferring fingerprint images will pave the way for the sharing of fingerprint data among law enforcement agencies in a form that can be utilized by all AFIS systems.

Facsimile technology is also making advances in providing another method for sharing AFIS image data. Facsimile-reproduced fingerprints represent a low-cost method of transmitting fingerprint

images from remote sites to the AFIS computer. The critical questions are whether the facsimile prints are of sufficient quality to use as substitutes for the inked impressions in the AFIS, and whether there will be a degradation in the scores produced in the search. Thus far, the testing of facsimile image transfer and use in AFIS sytems has shown that good quality facsimile copies of good quality inked prints can meet search accuracy requirements.

The future appears excellent for sharing fingerprint image data among law enforcement agencies. Capabilities at present are limited, but the experiments in image transmission standards and facsimile transmission of prints promise that the technology is not far from becoming an operational reality.

IMPACT ON LAW ENFORCEMENT CAPABILITY

AFIS technology will create a significant impact on the functions of law enforcement. First and foremost, it seems certain that the technology will significantly increase the *efficiency* of the ten-print search and the *effectiveness* of the latent search, with attendant cost and manpower savings and greatly increased crime-solving potential. (Attatched exhibits show the impact of AFIS in statistics from the California Department of Justice, San Francisco Police Department, Royal Canadian Mounted Police, and the National Police Agency of Japan.)

Ten-Print Processing

The ten-print to ten-print search—the comparison of newly-rolled prints with rolled file prints—is the bread and butter of both

criminal and noncriminal identification. As noted earlier, virtually all identification bureaus and criminal record repositories begin the processing of fingerprint cards by conducting a search of their master name indexes. This will continue to be the prevailing practice in agencies with AFIS systems. Nationally, some 50 to 55 percent of name searches result in identifications. With manual systems, some agencies stop here; if no hit is produced, they do not conduct a technical fingerprint search because such searches consume too much manpower. The majority of agencies, however, conduct a manual technical fingerprint search when there is no hit on the name search. Manually classifying and comparing fingerprints requires a significant investment of time and people. With an AFIS, those remaining 45 to 50 percent of incoming fingerprint cards that do not produce a hit on the name search can undergo a fast, efficient and accurate technical fingerprint search.

Available information suggests that manual fingerprint searches on a national basis achieve an accuracy rate ranging from 60 to 74 percent.[5] (Accuracy in fingerprint terminology is a measure of the ability of the system to locate a print that is in the data base. Failure to locate a print in the file can be attributable to a variety of factors, including errors in data entry, classification, filing, and comparison, as well as errors in the search algorithm and scoring

[5]See Terry Lindh and Stephen Ferris. *Fingerprint Identification Systems* (Paper prepared for presentation at the Automated Fingerprint Identification Seminar, University of Tennessee Space Institute, April 15-17, 1985), p. 28. In a national survey Lindh and Ferris found a 60-65 percent manual accuracy rate. Inspector Ken Moses, Crime Scene Investigation Unit, San Francisco Police Department, conducted a national survey in 1979 and found a 74 percent manual accuracy rate. Experts agree that the range in percentage is largely attributable to the degree of thoroughness of the actual comparisons of the suspect print with the file prints.

system. Accuracy rate is different than hit rate, which measures the percentage of candidate prints that are matched with file prints.) At the upper boundary, a 74 percent manual accuracy rate is an impressive figure in one sense, given the vast numbers of fingerprint records in criminal history files; but it still means that one in four potential fingerprint identifications is missed. The AFIS technology has changed these numbers dramatically. In agencies that have implemented AFIS systems, the accuracy rate of ten-print fingerprint searches has improved to an estimated 98 percent, and 99 percent in systems with a million records or less.[6] In the first few months of operation, the AFIS system in Baltimore, Maryland identified 525 arrestees using aliases. The San Francisco Police Department estimates that as many as 17 percent of arrestees lie about their names and other identifying information, but still are identified by the Department's AFIS system.

It is not surprising that the increased speed and accuracy of AFIS equipment produces greatly increased efficiency in state-level ten-print functions that must accommodate large volumes of searches against massive files. California officials have reported that the California Department of Justice's CAL-ID statewide AFIS system in its early stages of operation has achieved a productivity increase of 300 to 400 percent in the processing of ten-print cards. The system is now processing 1,000 to 1,400 fingerprint cards a day using 12 people. In a manual mode, that level of production would

[6]*Proceedings of a SEARCH National Conference on Automated Fingerprint Identification Systems, op. cit.* For example, Peggy A. James, Latent Print Examiner, Houston Police Department, reported that in its six years of operation, Houston's AFIS has missed 750 10-print records known to be in a data base, a figure representing one-half of one percent of the 151, 237 records in the data base.

require an estimated 46 to 50 people. CAL-ID officials project an eventual savings of 50 percent reduction in the costs of ten-print processing, which is on the order of $2 million annually.[7]

Latent Print Processing

The latent to ten-print search, which runs a crime scene print against files of criminal and noncriminal ten-print cards, is the crime-solving function of identification bureaus. As stated earlier, manual searches of latent prints are exceedingly time-consuming and costly and yield little results even when there are suspects and other information to limit the number of comparisons that must be made. Although an estimated 35 percent of crime scenes yield usable latent prints, very few identifications have resulted from manual searching methods. A study of four major metropolitan police departments conducted by the Rand Corporation found that the hit rate for manual latent searches ranged from four to nine percent.[8] Moreover, most agencies will only conduct manual latent searching when there are suspects or other information to limit the search. "Cold makes," which are based on the latent print alone, are rarely undertaken.

The speed and accuracy of the AFIS technology, however, makes it possible to search a single latent print against the individual

[7]California Identification System CAL-ID Project, Project No. 2100-23, Feasibility Study Report Update, October 15, 1984, California Department of Justice; page 4.

[8]P. Greenwood, J.M. Chaiken, J. Petersilia. *The Criminal Investiigative Process.* New York: D.C. Heath and Company, 1977;pp.162-165. Of the four cities examined in the study, three had approximately the same percentage rate of idenfifications from latent prints: Miami, Florida had 9.0 percent; Richmond, California had 9.9 percent; and Los Angeles, California had 9.1 percent. Washington, D.C. had 4.3 percent.

fingers of thousands or even millions of file prints in a matter of minutes. Not surprisingly, the impact of the technology on latent print processing has been phenomenal. In its first two phases of development, CAL-ID entered 420,000 fingerprint cards into the file that is used for latent searching. The file includes persons born in 1950 or later who have been convicted of a felony, a group that is estimated to represent only 34 percent of the AFIS data base but 47 percent of daily AFIS activity.[9] When the file is fully implemented, the latent file will contain 1.5 million records of individuals with felony convictions born 1940 and after. CAL-ID is now experiencing a hit rate of 15 percent on latent searches and officials project an increase in the hit rate to 18 percent. In its first year of operation, the San Francisco Police Department's AFIS system conducted 5,514 latent print searches and made 1,001 identifications, a hit rate of 18 percent. San Francisco cleared 816 of those cases, including 52 homicides, compared to 58 cases cleared the previous year on the basis of latent print identifications.

In Houston, 4,645 latent searches have resulted in a hit rate of 13 percent, clearing over 600 cases that officials say could not have been solved any other way. One hit cleared 30 cases in five counties. In Prince George's County, Maryland, an AFIS computer shared by six city and county police departments made 150 hits in its first nine months of operation, including one hit that cleared some 40 burglaries.

---

[9]ibid, pp. 5-6.

Law enforcement officials believe that the AFIS systems not only are helping to solve crimes that otherwise would not have been solved, but are putting chronic offenders in jail and halting repeat offenses. By the end of fiscal year 1985, San Francisco had jailed over 900 burglars identified by its AFIS, which has been credited as a contributing factor in the city's 25 percent drop in burglaries.

The Future of AFIS

As stated earlier in this paper, without known suspects, manual systems have very little chance of matching a crime scene print with a print in the fingerprint files. In fact, most often no search is attempted. Now AFIS has given law enforcement the capability to match those crime scene prints in "cold searchs." This new capability should invigorate crime scene work; investigators now feel that if they can detect a latent print, they have a real chance of solving a case. What we should see in the future is an advance in fingerprint detection and lifting technologies. At least in the United States, federal funding for forensic science research, including crime scene fingerprint detection technologies, has been inadequate. With the success of AFIS, we may see an infusion in support for technologies associated with forensic science.

One of the problems associated with fingerprint technology is the poor quality of inked prints. Poor quality inked prints erode the quality of the AFIS data base and result in the system not matching a print in the database. Technologies for taking "inkless" prints are nearing levels of quality that may make them an integral part of an AFIS.

As mentioned earlier, AFIS systems have the capability to enhance the quality of a print once it has been scanned and digitized. That capability can either be manual tracings or automatic tracing by the AFIS. There are merits to both methods. What we may see in addition to automatic enhancing is the use of an Expert Systems to enhance digitized fingerprints. As a component of Artificial Intelligence, Expert Systems capture or "clone" the institutional knowledge of experts. Expert Systems make decisions about the best possible method available for a given situation, as oppossed to compouter systems that simply automatically activate a programmed response to a given situation. What this would mean for AFIS is that if the knowledge of the finest fingerprint technicians could be captured in an Expert System, then the Expert System could be used to determine the best possible tracing to restore what might have been the original pattern of the print.

Finally, an AFIS is at heart a biometric technology—that is, a technology that physically corroborates the identity of a given individual. As such, we should begin to see AFIS systems used in the future in a variety of applications outside of the criminal justice environment. For example, documents such as the birth certificates, drivers licences, and passports do not at present have a biometric corroboration physically linking the individual with the document. Without such verification, fraud based on false identification documents results in annual losses in the United States of over 25 billion dollars. AFIS may well be called into service to bring integrity and reliability to identification documents.

Exhibit 1

CALIFORNIA IDENTIFICATION SYSTEM CAL-ID)
CALIFORNIA DEPARTMENT OF JUSTICE

System Intalled October 9, 1985
Through December 1986

Latent Fingerprint Identification Statistics

Fingerprints Searches	11,695
Total Cases Submitted	9,211
No. of Agencies Submitting	250
Suspect Identifications	1,207
Total Cases Hit	1,055
Case Hit Rate	13.2%
Total System Hits	2,007
Searches Per Day	280
Percent of Hits in No. 1 CandidatePosition	99%

By Crime Catagory

	No. Cases	*Percent*
Felony Burglary	686	65.0
Robbery	135	12.8
Homicide	90	8.5
Auto Theft	73	6.9
Rape/Sex Crimes	25	2.4
Grand Theft	18	1.7
Narcotics	7	.7
Assult	6	.6
Attempted Homicide	3	.3
Other felony/Misdemeanor	12	1.1
TOTAL	1,055	100.00

Source: California Department of Justice

Exhibit 2

SAN FRANCISCO POLICE DEPARTMENT
AFIS Statistical Report

From Start of Operations on February 28, 1984 through June 30, 1987

START DATE	THIS YEAR	FROM
Number of Searches	2373	11831
Number of identifications	540	2344
Hit Rate (percent)	22	19
Number of Cases	441	1925
—Burglary	270	1337
—Robbery	40	177
—Sexual Assult	13	38
—Homicide	17	84
—Auto Theft/Boosting	70	184
—Fraud	6	17
—Assults	9	35
—Hit & Run	9	22
—Other	7	31

Source: Inspector Kenneth Moses, San Francisco Police Department

Exhibit 3

ROYAL CANADIAN MOUNTED POLICE
HISTORY OF AFIS TECHNOLOGY

Ten-Print	**Manual**	**Phase 1 1971**	**Phase 2 2nd Gen AFIS 1979**	**Phase 3 3rd Gen AFIS Dec '85**	**Phase 4 Orion Dec '87**
Staff	123	73	76	79	79-15=64
Data Base Size	900,000	1,000,000	1,312,330	1,931,939	2,500,000 (2 fingers)
Daily Search Volume	780	957	826	923	2,500
Turnaround Time	7 days	24 hrs	24 hrs	24 hrs	2 hrs
Measured Accuracy	75%	75% (1/2 man)	94%	96%	96%
Latent					
Staff	21	11	19	19	19
Data Base Size	69,000	30,000	122,164	331,445	2.5 mil
Daily Search Volume (In Cases)	100	100	500	1,000	45,000
Turnaround Time	1-3 mo.	1-3 mo.	5 days	3-4 days	4 hrs. Major 24 hrs. Minor
Total Idents Per Year	85	21	139	708	+6,000

Source: Royal Canadian Mounted Police, July 1987.

Exhibit 4

NATIONAL POLICE AGENCY OF JAPAN
AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

Year of Implementation: October 15, 1983

Latent Print Identification Statistics

	1982 Pre-AFIS	1986 AFIS
Latent Inguiries Received	3,500	13,700
Number of identifications	200	1500
Processing Time	3.5 days	24 hrs.
Hit Rate (percent)	5.7%	11%

Searching time

1.5 second per finger
15 seconds per set
7 seconds per latent finger
1.3 seconds per one to one finger matching

Source: Yuji Tatuzawa, National Police Agency, Japan

FORENSIC USES OF POLYGRAPHIC INTERROGATION

David T. Lykken

University of Minnesota

A Lecture Presented at the 38th International Course in Criminology

The International Centre for Comparative Criminology

University of Montreal

18 August, 1987

Polygraph tests or "lie detectors" are widely used in the United States and in Canada for screening job applicants for security or police work and for examining suspects in criminal investigations. In spite of a swelling tide of criticism of the lie detector, from the press and from the scientific community, polygraphers and the agencies that employ them remain firmly convinced of the accuracy and value of these techniques. I want to examine first the reasons for this seemingly unshakeable faith in lie detection on the part of its practitioners.

Next, I will outline what I believe to be the opinion of most professional psychologists about the lie detector. Any polygraph test is a psychological test in the sense that it seeks to determine something about the subject's psychological state: is he consciously lying or does he believe he is telling the truth? The polygraph test uses measures of more-or-less involuntary physiological reactions as the evidentiary basis for making these psychological inferences. I will outline the assumptions on which these techniques are based, assumptions which most psychologists regard as implausible on their face.

We will then survey the scientific evidence concerning the accuracy of polygraph-based diagnoses of truthfulness or deception, evidence that psychologists take considerably more seriously than they do the claims or opinions of the practicing polygraphers.

Finally, I want to outline for you a radically different method of polygraphic interrogation, a method designed not to diagnose truth or deception but, rather, to determine whether the subject possesses guilty knowledge.

WHAT THE POLYGRAPH MEASURES

To begin with, however, we should make sure that we all understand what a polygraph is and what is does (and does not) measure. The standard field polygraph is a relatively simple instrument, the size of an attache case, containing four pens that draw wiggly lines on a moving paper chart. Two pens are connected pneumatically to soft rubber tubes placed around the subject's chest or stomach. These two pens record thoracic and abdominal breathing movements. A third pen is connected to a blood pressure cuff wrapped around the subject's upper arm. During the test proper, the cuff pressure is increased sufficiently to partially block the flow of blood to the lower arm. Then each heart beat causes this "cardio" pen to jump upwards on the chart and the entire tracing may move up or down with transitory changes in blood pressure. Because the cuff pressure can get painful after several minutes, the test must be interrupted every three or four minutes so that the pressure can be released. Approximately ten questions can be asked during these three or four minutes; the polygraphic tracings of

the physiological responses to these ten or so questions is called a "chart." The usual polygraph test will consist of from two to five charts. Normally the same question list is used on each chart, perhaps in a different order each time.

The fourth pen is connected electrically to a pair of metal plates or electrodes attached to two fingers of the subject's hand. This pen records electrodermal responses, brief changes in the electrical conductivity of the skin that are related to sweat gland activity. These responses appear as waves in the electrodermal record. Thus, the field polygraph measures disruptions of normal breathing movements, blood pressure changes, and the sweating of the palms. All three of these variables can reflect stress, that is, emotional disturbance associated with the questions or with any other sources of stimulation occurring at the time.

The first point to emphasize is that the polygraph cannot detect lying. The human animal is not constructed, like Pinnochio, to produce some distinctive involuntary response, or pattern of responses, when and only when lying. Any known physiological reaction I might display while lying I am likely to also display while truthfully denying a false accusation. All that anyone can determine from a polygraph chart is that this subject was more disturbed by Question A than he was by Question B; we cannot tell <u>why</u> he was disturbed. We cannot determine whether the question made him feel guilty or frightened or angry or merely surprised. We cannot even be sure that it was the question, rather than some covert activity like biting the tongue, that caused the

reaction (Lykken, 1981a.)

Since the polygraphic response to a particular question, by itself, cannot distinguish truth from deception, the examiner must rely on the comparison of responses to different types of questions. We will look at how that is done, and the assumptions involved in these comparisons, in a moment. First, however, I want to consider the practicing polygrapher's opinions about his techniques and why he holds them.

WHAT POLYGRAPHERS THINK ABOUT POLYGRAPHY AND WHY

There is no question that polygraphy can be useful in criminal investigation for one reason alone -- the lie detector is a powerful inducer of confessions. Skilled interrogators know that, if a guilty suspect can be led to give himself away -- by blushing or stammering or blurting out something revealing -- so that he realizes that the questioner now knows that he is guilty, then at that point many perpetrators will break down and confess. Even innocent suspects have been known to confess once they are certain that the authorities are convinced of their guilt. The liar may know that he is responding -- "blushing" -- internally to the questions but as long as he thinks he has concealed these internal reactions from his questioner, he continues to feel safe.

The polygraph seems to provide a way around the suspect's defenses by directly monitoring his internal reactions. "The polygraph shows that you aren't being truthful, George. Why don't you tell me what really happened?" Experience shows that from 10 to perhaps 30 percent of

guilty suspects may be led to confess during the post-polygraph interrogation. Since this form of "bloodless 3rd degree" can sometimes elicit false confessions, it is important always to treat these admissions with at least a grain of salt unless they provide new information that allows the confession to be independently verified.

But I am acquainted with a number of highly experienced polygraphers, people who have administered thousands of tests in the course of their careers, and these people do not value the polygraph merely as a useful interrogation tool. They firmly believe that, at least in their hands, the polygraph test is extremely accurate as a test. In recent years, most polygraphers have become cautious about the claims they make in public; a typical estimate I have been hearing recently is that the lie test is at least 90 percent accurate. I think, however, that most professionals privately believe that their own findings are 95% or 99% accurate -- nearly infallible -- and that the test errors one reads about from time to time are due to the incompetence of other polygraphers.

If a man has been giving polygraph tests to hundreds of people a year for 20 years, and if he is honestly convinced that he has made no more than a handful of mistakes, if any, over that time, should we not accept his judgment? The answer is "No, we should not", and here's why. (I am happy to acknowledge that I am indebted to my former student, Dr. W. G. Iacono, for this insight.)

* * * Table 1 about here * * *

Suppose an examiner working for the Los Angeles Police Department has assisted in 200 cases a year over the past 10 years. It often happens that there may be more than one suspect in the same case and, for the sake of this illustration, we shall assume that every case involves exactly two suspects. When the polygrapher tests the first suspect in each case, we can suppose that he classifies half of them as deceptive. He will interrogate only those suspects who fail his lie test, 1,000 of the 2,000 first suspects tested, and let us say that 200 of them confess during the interrogation. The examiner then proceeds to test the other suspects but, since he has faith in the polygraph, he only tests the second suspects in those 1,000 cases where the first suspect to be tested passed the lie test, since these are the only cases that he feels still have not been resolved. I shall assume that 500 of this second group of suspects fail and that 100 of them confess during the post-test interrogation. In the remaining 500 cases, the polygrapher tells the detectives that both of their suspects are innocent and they had better cast a wider net.

At the end of the 10 years, this examiner has tested 3,000 people and has obtained 300 confessions. Every confession came as the result of a failed test so, assuming that none of these were false confessions, 300 of his results have been verified as correct. The 100 confessions obtained from suspects in cases where the first suspect passed the test also verify those first tests -- since the second suspect was guilty, the first suspect must have been innocent just as the test indicated. Therefore, he has a total of 400 verified lie tests -- and no errors.

Is there any way of checking on the accuracy of the remaining 2,600

tests, of establishing "ground truth" for those cases? Some of those suspects will go to trial but polygraphers are understandably reluctant to accept trial outcomes as a criterion of lie test accuracy. Moreover, trial outcomes are usually so long delayed that the polygrapher never learns about them. In their study of polygraph accuracy as used by the Royal Canadian Mounted Police (RCMP), Iacono and Patrick (1987) were able to verify a handful of charts from information in the precinct files (e.g., the alleged victim found the money was mislaid rather than stolen), but this information was not available in the files of the polygraph section. As a general rule, just about the only feedback a polygrapher gets about the accuracy of his techniques is the feedback provided by confessions during the post-test interrogation. And this feedback is guaranteed to indicate nearly 100 percent accuracy!

Since he gets confessions only when he interrogates, and he interrogates only when the suspect fails the test, confessions are almost invariably associated with failed tests. If another suspect in that same crime has been tested previously, he will have passed his test since, if he did not pass, the suspect who confessed would not have been tested and would not have confessed. Hence, all of the tests that are verified by post-test confessions are virtually certain to have produced correct results. And it is important to see that this would be true even if the polygraph tests were in fact no more accurate than flipping coins!

The chance accuracy for lie detection is 50% since the suspect is either lying or not so that one can expect to be correct half the time

just by random numbers. If he were using a completely invalid or chance accuracy lie test, our police examiner would fail half of the guilty suspects and some of them will confess. Their confessions will verify their tests and also any tests administered to prior suspects in the same crimes. The feedback will be all positive, the confirmed tests will be 100% correct, even though the true accuracy of this polygrapher's determinations is no better than chance. Therefore, the examiner himself, and also his supervisors or employers, can hardly be blamed for believing that the polygraph is an extraordinarily accurate and valuable forensic tool. Yet, as this example illustrates, we should put very little credence in their opinions on this matter. The curious nature of the polygraph business virtually guarantees only positive feedback irrespective of the true accuracy of the method.

WHAT PSYCHOLOGISTS THINK ABOUT POLYGRAPHY AND WHY

We saw earlier that there is no "specific lie response", no unique physiological reaction that is diagnostic of deception, and we saw that examiners therefore have to base their judgments on the comparison of the subject's responses to one type of question with his responses to some other question or questions. The earliest type of test, still used by some of the older examiners, was called the Relevant-Irrelevant test because it involved comparing the reaction to Relevant or "Did you do it?" questions with the responses elicited by Irrelevant questions, questions like "Is today Tuesday?" or "Do they call you 'Bill'?" The theory of the R-I test was that any suspect who is plainly more disturbed by the Relevant questions than by the Irrelevants is probably answering the Relevant questions deceptively. One does not have to have

a doctorate in Psychology to realize that this is an implausible assumption. One only has to imagine one's self, innocent but accused of some crime and taking a polygraph test at the request of the police, to realize that it is perfectly normal for an innocent accused also to be disturbed by the accusatory Relevant questions.

The only available study of the true accuracy of the R-I test was published by its inventor, J. A. Larson, in 1938. Larson found, as might be expected, that the R-I test produces a very high rate of false-positive errors; as many as 50% of the innocent suspects in his study were classified as deceptive. The fact that the R-I test with its implausible assumptions and high degree of inaccuracy was the standard technique of the polygraph industry for 50 years or more is additional evidence that the practicing polygraph examiner is insulated from his mistakes and, no matter how many errors he makes, tends to get exclusively positive feedback.

The standard test format currently used was invented by late John Reid in the 1940s and modified in various ways by others, notably Cleve Backster. This format is called the Control Question Test or CQT and it involves adding a third kind of question, called "Control" questions, along with the Relevant and Irrelevant questions of the R-I procedure. Control questions ask about previous misdeeds of the subject: "Before two years ago, did you ever tell a lie to get out of trouble?" In the pre-test interview, the examiner tries to get the subject to think that he had better deny these previous misdeeds, that he should answer the Control questions "No." He also tries to convince the subject, however,

that if the polygraph indicates that he is lying about the Control questions this may make him fail the test. The theory of the CQT assumes that an innocent person will be less concerned about the Relevant questions, which he can answer truthfully, than he is about the Control questions which, it is assumed, he is either answering deceptively or else at least he is in doubt about. Therefore, the subject is classified as Truthful only if he gives larger reactions, on the average, to the Control questions than to the Relevant questions.

These assumptions mean that the polygrapher has to be very clever and very devious. He must be clever enough to be able to construct three or more Control questions about misdeeds in this subject's past life which the subject cannot truthfully deny. Yet he must be devious enough to make the subject think he must deny them -- lie about them -- in order to pass the test. And he must be clever enough to make any innocent subject think that he is in more jeopardy with respect to the Control questions than he is with respect to the Relevant questions, although the truth is just the opposite of this.

That is, the CQT involves at least two specific deceptions (Lykken, 1987.) First, the examiner must make the subject think that he might fail the test if he admits the misdeeds referred to in the Control questions; this is required in order to get him to deny them. Second, he must make the suspect believe that he might fail the test if he does lie about these misdeeds and the polygraph reveals that he is disturbed by the Control questions. The truth is that the only way the suspect can pass the test is by being truly disturbed by the Control questions.

I am a psychologist with more than 30 years' experience and yet I look at this list of requirements with dismay. I am not nearly clever enough to sit down with a stranger and, in 20 minutes, invent three questions about his past misdeeds which he should answer "Yes" but which he will answer "No" on the polygraph test. Nor am I skillful enough to make each suspect think, if he is innocent, that he has more to fear from these questions about his past, which obviously cannot get him into trouble now, than from the Relevant questions about the crime of which he is presently suspected. Any psychologist will also be suspicious of a test that requires that the examiner be able to deceive the subject, as the CQT does, not only because this is asking a lot of the examiner's skill but also because any person who has learned about the test and these deceptions will thereafter never be able to be validly tested himself.

The Research Findings

Field Studies. Systematic study of polygraph accuracy in the real life field situation requires some sort of criterion of ground truth. Then we can take the charts of suspects whom we know were lying, together with charts of verified-truthful suspects, and have them re-scored by other polygraphers. When this re-scoring is done blindly, we know that the results will not be contaminated by the polygrapher's knowledge of the fact situation, by his subjective reactions to or impressions of the subject, or by other non-polygraphic factors.

Two kinds of ground-truth criteria have been used. One approach is to let a panel of judges examine the final evidentiary file on each

suspect and decide his guilt or innocence. If the panel can discard all cases where they feel the evidence is ambiguous or inadequate, then their decisions on the remaining cases can be taken to be reasonably accurate.

The one published field study that used blind scoring together with the panel judgment criterion was that by Barland and Raskin (1976.) In that study, the blind scorer (Raskin) classified 88% of the charts as deceptive so we would expect him to have identified at least 88% of the criterion guilty suspects just on a chance basis. In fact, he correctly identified 98% of them but, at the same time, he misclassified more than half (55%) of the criterion innocent.

Another approach is to use confessions as the criterion. As we have seen, most such confessions will result from interrogations that follow failed polygraph tests. Therefore, the verified-guilty charts will all come from suspects whom the original polygraph examiner believed to be deceptive. Moreover, all the verified-innocent charts will be from suspects whom the original examiner believed to be truthful. This means that, if the original examiner based his judgments solely on the polygraph charts, then any subsequent scoring by other polygraphers who use the same method of chart interpretation will tend to be correct. That is, the charts selected for re-scoring will have been chosen because they fit the assumptions of the polygraph method and they will not necessarily be representative of polygraph charts generally. The accuracy of the blind scorers on such confession-verified charts will be a measure of the inter-scorer agreement or

reliability rather than a measure of polygraph accuracy or validity.

In three published studies, however, we can tell that the original examiners did not rely solely on the charts. In Horvath (1977), for example, the original examiners were correct in 100% of the cases, as we expect for the reasons already discussed. The 10 polygraphers who later scored the charts independently, agreed with each other 89% of the time, a measure of their inter-scorer reliability, but they agreed with the original examiners only 63% of the time. This indicates that the original examiners must have been allowing extra-polygraphic factors to influence their judgments. This difference between the inter-scorer reliability and the agreement with the original examiner is the clue which indicates that a confession-based study may yield a useful estimate of polygraph accuracy. However, such studies are likely to over-estimate the sensitivity of the lie test, that is, its level of accuracy in detecting the verified-deceptive suspects.

The reason why studies using confession-verified charts tend to over-estimate polygraph sensitivity has to do with the way in which these confessions are normally obtained. As we have seen, confessions are produced by the post-test interrogation. Examiners will interrogate most vigorously and most successfully those subjects whose polygraph charts show the strongest reactions to the Relevant questions; that is, the suspects who "fail" the test most emphatically will receive the most searching interrogations. These are the cases the polygrapher feels most confident about, the ones where he can display the actual charts to the suspect:

"Look how you reacted when I asked if you had taken the money. The polygraph doesn't make mistakes, George. You know you're guilty; that's why you reacted this way. Now I know you're guilty because the polygraph has proved it. Why don't you quit pretending and tell the truth? Then maybe we can work out the best deal for you."

Thus, the confession-verified deceptive charts tend to be those charts which best fit the polygrapher's model of what a deceptive chart looks like, charts that most other polygraphers would also score as deceptive.

Confession-verified truthful charts, on the other hand, are more likely to include marginal or ambiguous charts. That is, while a polygrapher is more likely to conduct successful interrogations after obtaining "obviously deceptive" charts, the prior tests that are verified as truthful by those confessions will include some that other examiners might have scored only weakly truthful or as inconclusive or even as possibly deceptive. Therefore, as can be seen in Table 2, field studies based on confession criteria appear to have reasonable validity in detecting deception while their ability to identify the truthful subject - their <u>specificity</u> -- is not much better than chance.

* * * Table 2 about here * * *

Theoretical considerations argue that the CQT <u>ought</u> to be biased against the truthful subject, that is, that sensitivity should be higher than specificity. On the other hand, the bias inherent in the confession criterion design, just discussed, should tend to over - estimate the true sensitivity of the test. Therefore, we can conclude

from the four studies summarized in Table 2 that, while an innocent suspect has nearly a 50:50 chance of failing the CQT, the probability that a guilty suspect will be identified as deceptive is probably something less than .88. If the guilty suspects in these studies had known how to beat the CQT, how and when to artificially augment their reactions to certain questions so as to be scored as "truthful", then we can be sure that the CQT's sensitivity -- its ability to detect deception -- would have proved out much lower than .88. I will return to this question of beating the polygraph shortly.

Analog or Laboratory Studies. Another approach to validity estimation is to have volunteer subjects participate (or not) in a mock crime. One then attempts to identify the "guilty" by administering polygraph tests. The advantage of this analog design is that it avoids the criterion problem; one knows for certain which subjects were deceptive and which were truthful during the questioning. On the other hand, it is difficult to simulate in the laboratory the emotional concerns experienced by actual criminal suspects in the field situation and, since these emotional reactions drive the polygraph responses, it has been widely believed that laboratory studies are an inadequate test of polygraph validity. Volunteers are assigned to the "guilty" or "innocent" conditions arbitrarily, "guilty" subjects are instructed to commit the mock crime, instructed to lie during the polygraph test, no consequences significant to the subject result from the outcome of the test, and so on.

A particular weakness of the conventional mock crime design is that, while the Relevant questions have little emotional significance to

the subject, whether "guilty" or "innocent", the Control questions still refer to actual misdeeds that the subject might have committed in the past. It seems reasonable to suppose that volunteer subjects feel genuine concern and embarrassment about references to previous dishonesty, just as they would feel as criminal suspects undergoing polygraph testing in real life. This means that, in the mock crime studies, the "innocent" volunteers will tend to be more disturbed by the Control questions than by the Relevant questions. Therefore, it is not surprising that most conventional mock crime studies have reported remarkably low rates of false-positive errors.

In recent years, however, two simple modifications of the mock crime design have yielded very promising results. One modification, used by Iacono & Patrick (1987), involved creating a situation in which both guilty and innocent subjects believed they had reason to fear the consequences of failing the polygraph test. That study was conducted in a maximum security prison and the subjects were all inmate volunteers who were to be paid $20 each for their participation. It was agreed in advance that these payments would be forfeit if more than 10 of the total group of 48 inmates were to fail their polygraph tests. The names of those who failed the test were to be posted for all to see and it was expected that subjects would be concerned about the possibility that they might be blamed by their fellow inmates, if they should fail the test, for contributing to the loss of the anticipated $20. Two highly experienced examiners each tested half of the inmates and each examiner also blindly scored the charts of the other. Inter-scorer reliability was very high but only 63% of the charts were correctly classified. The

average sensitivity was 87% (i.e., 13% false-negative errors) while the specificity was 56% (44% false-positive errors.) These results are essentially identical to the averages for the field studies listed in Table 2.

Foreman and McCauley (1986) allowed their volunteer subjects to decide for themselves whether to participate in the mock crime, and thus have to lie during the polygraph test, or to accept a smaller reward by participating as one of the "innocent" subjects, who were able to be truthful during the test. The polygrapher did not know whether the person he had tested had elected to be "guilty" and was lying or had rejected the temptation of the larger payment promised to mock crime participants if they succeeded in passing the lie test. This simple modification seems to greatly increase the "ecological validity" of the mock crime design. Instead of being assigned to a given experimental condition, instructed to lie or not lie, the subject feels that he has made his own choice for which he must then be responsible. One might think that this might make the "guilty" subjects more easily detectable but the effect of this modification seems to be to increase false-positive errors as compared to the usual mock-crime design where such errors are rare. Foreman and McCauley obtained a sensitivity of 86% and a specificity of 52%; again these results are very similar to the aggregated field study findings.

It is to be hoped that additional studies will appear using these new designs in combination, studies in which subjects can elect to be either "guilty" or "innocent" and where significant adverse consequences are expected to result from failing the polygraph test. In the

meanwhile, it is encouraging to note that well designed studies of polygraph validity, whether field studies where the criterion of ground truth is the principal problem or analog studies where ecological validity is the problem, all tend to converge on the same range of outcome. As we see in Table 2, the lie test findings tend to be wrong about one-third of the time over all and innocent suspects have nearly a 50:50 chance of being erroneously classified as deceptive.

Beating the Lie Detector. You will "pass" a control question polygraph test if your physiological reactions to the Control questions are, on the average, larger than your reactions to the Relevant questions. It is easy to artificially augment one's response to any question merely by self-stimulation. By biting one's tongue or constricting the anal sphincter while each Control question is being asked, the amount of apparent disturbance registered on the polygraph can be substantially increased. Another effective method is to secrete a small nail or tack in one's shoe and then press on it at the desired times. Polygraphers think they can detect counter-measures because every now and then they do detect what appears to be an unsophisticated attempt to disrupt the recordings by coughing or moving in the chair or by tensing the biceps under the blood pressure cuff. Obviously, these examiners have remained unaware of more sophisticated attempts that were successful. It has now been demonstrated in at least two different studies (Hontes, Hodes, & Raskin, 1985; Lykken, 1981a) that, with brief training, guilty subjects can successfully produce charts scored as "truthful" without the examiners being able to identify who was employing counter-measures and who was not.

There seems to be little likelihood that many or any of the subjects in the validity studies already reviewed knew how to "beat the lie detector." During the last few years, however, explanations of this simple and effective technique have appeared in many places -- it has been demonstrated on national television, for example -- and it would be surprising if many of the more planful and professional of criminals have not learned the secret. If we were to do a field study of CQT validity in criminal interrogation now, I would predict that the professional criminals, the spies trained by the KGB, the wealthy white-collar criminals who employ expensive criminal lawyers, would turn up as false-negative test errors. In the near future, perhaps, the only persons who continue to fail the lie detector will be the uneducated petty criminals, the first offenders, -- and of course the innocent.

THE FORENSIC UTILITY OF THE LIE DETECTOR

Even if the polygraphic lie detector is based on implausible assumptions, even if it wrong about one-third of the time, even if it is easy for a sophisticated villain to beat it, does it not still earn its keep forensically by virtue of the fact that a considerable number of unsophisticated perpetrators can be led to confess in the course of a polygraph test? This is a question of weighing costs and benefits and it would be presumptuous of me to be dogmatic about it. If I were working in criminal investigation myself, I can readily imagine situations in which I might resort to the polygraph for just this purpose of quickly and efficiently resolving a case by eliciting a confession. I could trust myself to do this because I would know enough

not to take the test outcome seriously as a piece of evidence. If there were two or three possible suspects, I would be sure to test all of them and, moreover, to interrogate all of them afterward, whether they had appeared to "fail" the test or not. If I got a confession, I would not put much credence in it unless and until I could independently corroborate it. Almost any genuine confession will carry with it some circumstantial detail which can be either checked for accuracy or which at least can be evaluated for credibility.

In other words, I think I could make use of the polygraph as a kind of "bloodless third degree" while at the same time minimizing the risks and costs because I am very clearly aware of how nearly worthless the polygraphic lie test is as a test and I have a strong appreciation of how disoriented and hopeless an innocent suspect can be when he is told that the polygraph indicates he is a liar and that he might as well give up his denials now since now no one will ever believe them. Therefore, I would not take the test results seriously as evidence and I would not take confessions seriously unless they contained the new information that genuine confessions do contain. But there are not many other people whom I would trust to be able to remain adequately skeptical of this technique because I know how strong the myth of the lie detector is, at least in North America, and I have seen too many instances in which honest and well meaning investigators or polygraphers have let the polygraph lead them to false and damaging conclusions.

An example of such a travesty is in the news as I write this. A United States Marine, Sgt. Clayton Lonetree, while serving guard duty at the American Embassy in Moscow, became involved with a Russian woman who

introduced him to a Soviet intelligence officer. Thinking he had made a contact that might be useful to American intelligence, Lonetree informed his superiors about what was happening. Naval Investigative Service (NIS) investigators, whose faith in the polygraph is apparently absolute, began a marathon interrogation consisting of repeated polygraph sessions alternating with intensive questioning based on his polygraph reactions. Other Marine Guards were similarly interrogated. Frightened and confused, aware that the investigators suspected them of serious crimes like espionage, these young men sought to explain the polygraph results by admitting to fraternizing with Soviet women, minor dealings on the black market, the kinds of misconduct that were apparently endemic among the Embassy support staff at the time as a consequence of a general lack of discipline from the top.

These "damaging admissions" merely whetted the appetites of the investigators who began suggesting more serious possibilities. Sure enough, when those possibilities were presented as Relevant questions on the next polygraph session, the rattled Marines reacted to them, thus "confirming" the suspicions and leading to still more dramatic hypotheses. One of Lonetree's fellow guards, Cpl. Bracey, was especially susceptible and soon his interrogators had created a hair-raising tale of nocturnal rambles throughout the inner sanctums of the Embassy with Russian Mata Haris.

For the investigators, these extended polygraph-assisted interrogations are an exciting adventure, a kind of treasure hunt, but to the confused and frightened subject they have a nightmare quality.

To account for "failing the polygraph", one naturally thinks of whatever one has a bad conscience about and this is encouraged by the examiners. "Think of it as a kind of mental cleansing", they suggest. Any damaging admissions that are made in this way are treated as just the tip of an iceberg, a foot in the door. The investigators are so certain, so convinced of what they claim the polygraph has shown to be true about your crimes, and they seem less concerned about what you did than about your continued denials. It appears that the only thing that will satisfy them, the only way that you can bring this nightmare to an end, is to finally tell them what they want to hear. To escape from such an interrogation, Cpl. Bracey signed -- without reading -- a long confession whose only reality was in the excited imaginations of his interrogators.

What was wrong at the Moscow Embassy was a general laxness of security and poor supervision by the officer in charge of the Marine Guards who spent most of his time in another country. This led directly to Sgt. Lonetree's contact with the KGB, an improper but essentially harmless contact which he naively cultivated thinking to earn credit with his superiors. The NIS investigators with their polygraphs transmogrified this into the greatest scandal in Marine Corps history, an imaginary breach of security that commanded cover stories in Time and Newsweek, statements by the Corps Commandant, the Secretary of Defense, the President himself, Congressional delegations to Moscow where they were shown the very rooms and corridors through which the Marines supposedly conducted KGB agents in nocturnal forays. It was reported in the press that the Russians were laughing about all this flap; who can blame them?

Gresham's Law says that bad money drives out the good. I think a similar Law takes effect when the lie detector is relied on in security applications or in criminal investigation. The bad money of the polygraph tends to take the place of careful, disciplined security procedures and of thorough, professional investigation. Detective work is slow, painstaking, often boring, necessarily expensive in time and resources. The polygraph is cheap and quick. As long as the investigators themselves believe in it, it is inevitable that the polygraphic lie test will be substituted for traditional methods. But we have seen why it is that the polygraphers believe in the lie test -- it is because they sometimes learn of their successes but are almost wholly shielded from learning about their mistakes. They do make mistakes, however, a great many mistakes, and others learn about them and we all pay for them.

THE GUILTY KNOWLEDGE TEST

There is another approach to polygraphic interrogation that is based upon reasonable, plausible assumptions and has considerable promise for use in criminal investigation. This technique does not attempt to determine whether the subject is lying but, rather, whether this suspect possesses guilty knowledge, whether he recognizes details of a crime that he should not be able to identify unless he had been a participant. It will be easiest to illustrate the technique first in action and then make some observations about it.

One of the most widely celebrated failures of conventional lie

detection was the Floyd Fay case (Cimerman, 1981) in which Fay was routed out of bed in the early hours of a March morning and charged with the murder of his friend, Fred Ery, during an armed robbery earlier that evening. Ery, night clerk in a convenience store, had been held up by a man wearing a full ski-mask and carrying a sawed-off shotgun. A witness saw the robber shoot Ery once and then escape to a waiting car. Five hours later, sedated and at the point of death, Ery said the "Buzz did it", referring apparently to his friend Floyd "Buzz" Fay, a tall muscular man like Ery's assailant.

After protracted investigation which failed to turn up useful evidence against Fay (who had no prior record), the prosecution offered to drop the charge of aggravated murder -- then punishable by death in Ohio -- if Fay could pass a CQT administered by a polygrapher at the Ohio Bureau of Criminal Investigation. The offer required, however, that Fay stipulate in advance that the lie test results could be used against him at trial in the event that he failed the test. Having been in jail for 8 weeks by this time, and after being told by his then-counsel that polygraph tests were very accurate, Fay agreed to this stipulation. He failed that first test and then also a second test administered at a Michigan polygraph firm of high repute. After hearing the results of these polygraph tests, an Ohio jury found Fay guilty as charged. Ohio's death penalty having been recently declared unconstitutional, Fay was sentenced to life in prison.

Two years later the real killers were apprehended: the shooter, a lookout and a driver. The driver made a full confession, wholly exonerating Fay who was promptly released (Cimerman, 1981.)

When Fay was first arrested that March morning, a Guilty Knowledge Test could easily have demonstrated his innocence. Telling him only that he was being held on suspicion of homicide, the investigator would make the polygraph attachments and then proceed as follows:

1. "What was the first name of the victim, Fay? I'm going to mention some men's first names; just repeat each name after me. Was it: Bob? Andy? Fred? Walt? Bill? Pete?"

2. "Now, where did this killing take place? Was it: At the victim's home? In a car? On the street? In a store? In a bar? In an alley?"

3. "What sort of weapon was used in this killing? Was it: Your bare hands? A knife? An automatic pistol? A revolver? A tire iron? A shotgun?"

4. "The killing was in Fred Ery's store, Fay. Who else was in the store at the time? Was it: A confederate of yours? Fred's brother? A lone woman? Two teenage boys? A black man? A man and woman?"

5. "What were you wearing on your head in that store, Fay? Was it: A baseball cap? A Halloween mask? A ski mask? A stocking mask? A scarf? A motorcycle helmet?"

6. "What color was the ski mask you were wearing? Was it: Black? Red? ... etc."

7. "What were your first words when you entered the store? ... etc."

8. "What color was the jacket you were wearing?" ... etc."

9. "What did Fred say to you? ... etc."

Fay would be likely to react physiologically to each of the alternatives for each of these questions. If there were, say, five alternatives for each question, and if each of them sounded about equally plausible to an innocent person who knew nothing about the robbery, then there would be about 1 chance in 5 that Fay would react most strongly to the correct alternative of any one question. If Fay had actually been the masked killer earlier that evening, then it is very likely indeed that his strongest reaction on the first question would have been to the first name of the friend whom he had shot down. He would certainly recognize that the crime had occurred in "a store" and it is likely he would remember the lone woman customer who had been standing just a few feet away, the person who provided the police with most of the information. Had he been guilty, it is probable that Fay's strongest reaction would have been to the correct alternative on 6 or more of the 9 questions. Since he was innocent, however, there would be less than 1 chance in 10,000 that he would have given his strongest response to the correct alternative on as many as 6 questions, about 1 chance in 2 million that he would "hit" on all 9 questions.

There have not been any studies of GKT accuracy in the field situation for the simple reason that the GKT is almost never used in actual practice. There is a Gresham's Law that applies here, too. The polygraph lie test is so much easier to use. The polygrapher need not

know anything much about the crime, he does not have to investigate or plan or even leave his office. Moreover, as we have seen, polygraphers really have faith in the lie test and are therefore not motivated to experiment with a technique that is new and different and more demanding.

But there have been numerous analog or mock crime studies and I believe that we can put some credence in their results because, unlike the CQT lie test, the GKT does not depend on assumptions about how the guilty or innocent suspects will feel about the test situation. What it does assume is the following: (1) Guilty suspects will recognize the correct alternative in most (say, 80%) of the questions; (2) Innocent suspects will not recognize which of the alternatives is correct; and (3) A guilty suspect is likely to give his strongest physiological response to the alternative that he recognizes as the correct one. The so-called "Control" questions in the CQT lie test are not genuine controls in the scientific sense of that term. In the GKT, however, the incorrect alternatives are genuine controls in the sense that they permit us to estimate how strongly this suspect ought to respond to the correct alternative if he is without guilty knowledge and therefore does not recognize that alternative as different from the others.

* * * Table 3 about here * * *

Table 3 summarizes the findings from 8 published studies of the accuracy of the GKT in mock crime situations. Most of these studies employed only 6 questions with only 4 scored alternatives for each question. The assumptions of the GKT would lead us to expect that about

89% of the guilty suspects should be correctly identified with a short test like this; as shown in the table, the actual sensitivity was 88.2%. Where we would expect 96.2% of the innocent suspects to be cleared, the specificity actually found was 96.7%. With a few more items or more than 4 alternatives per item, these numbers could have been further improved.

I do not want to seem to over-sell the Guilty Knowledge technique. One obvious limitation is that there are some crime situations where it is simply impossible to generate the necessary items. Careless early questioning of suspects can communicate guilty knowledge to an innocent suspect and create difficulties. With this technique, the person responsible for constructing the test items has to be the investigator at the scene. In fact, the best arrangement would be for the investigator to construct the test while the polygrapher administers the test while he does not yet know the correct alternatives himself. This arrangement will help guard against his communicating clues about which alternative is correct as he reads them to the suspect. A still better technique would be to ask someone ignorant of the correct answers to tape-record the questions. In an important case it would be good practice to administer the test first to several known-innocent subjects in order to be sure that the alternatives had been chosen so as to seem equally plausible to someone without guilty knowledge.

A sophisticated suspect could, in principle, defeat the GKT by self stimulation much as can be done with the polygraph lie test but it would require much more presence of mind and self control. Since he cannot

hope to be able to suppress his reaction to the correct alternatives, his best bet would be to bite his tongue after one of the incorrect alternatives in each set. If he is optimally successful, then the examiner will find that this subject has given his second largest response consistently to the correct alternatives. At the very least, this should cause that examiner to want to repeat the test the next day. If, again, this suspect consistently gives his second-strongest response to the correct alternatives, his guilty knowledge would be convincingly revealed.

Another Example. As this is being written, a trial is underway in Israel of the man accused of being the notorious "Ivan the Terrible", sadistic guard in the concentration camp at Treblinka during World War II. The defendant maintains he is the victim of mistaken identity, that he never worked at any camp and was never in Treblinka. Some, but not all, of the surviving victims are sure they recognize him. This is an example of a case that could be settled quite conclusively by careful application of the Guilty Knowledge procedure.

By questionning of the survivors, one could determine the physical layout of the camp, the routes and locations that would be known to the real Ivan, the names and descriptions and salient facts about other guards whom he would have known, descriptions of standard routines or of unusual events that he would know about, and so on. Using this information, one could generate several Guilty Knowledge tests. Each test would be administered to two or three persons who had not been in that camp and who had no close friend or relative who had been at Treblinka; this would test the items to make sure that someone without

guilty knowledge would not recognize the correct alternatives or respond to them selectively. Each test would also be administered to several survivors of the camp; this would insure that someone with relevant knowledge could be expected to respond to the correct alternatives.

Finally, over a period of days, the several tests would be administered to Dimdanjuk, the defendant. If his pattern of response was like that of the known-innocent control subjects, he would be exonerated. Most reasonable people, hearing the basis for this decision, would accept it. If he systematically responded like those survivors who recognized the correct alternatives, then his claim of never having been to the camp would be invalidated. Moreover, these results could be explained in detail to the members of the jury. They would not have to accept the professional opinion of some polygraph examiner but could evaluate the GKT evidence for themselves and decide what it implied.

CONCLUSIONS

There is no doubt that a true lie detector would make life much easier for those with the responsibility for fighting crime or protecting national security. Indeed, if the current polygraphic lie detection methods were actually as accurate as their proponents, in their hearts, believe them to be -- 95% or 99% accurate -- then we could dispense with all the cost and aggravation of extended jury trials because a two-hour polygraph test would decide matters more accurately and thus more justly than any jury could.

But the present polygraphic lie detector is fundamentally unsound and inaccurate; it stigmatizes innocent people and can be beaten by sophisticated villains. There is no prospect for the development of a genuine lie detector in the foreseeable future. The Guilty Knowledge technique, while not nearly so easy or so generally applicable as lie detection, has an obvious but as yet unexploited potential. When the GKT comes to be more widely employed in the field, I have no doubt that ways will be found to misuse or abuse it. But the abuses of the polygraphic lie test are so wide spread and so serious that I believe we ought to risk making the change.

REFERENCES

Balloun, K.S. & Holmes, D.S. (1979). Effects of repeated examinations on the ability to detect guilt with a polygraphic examination: A laboratory experiment with a real crime. Journal of Applied Psychology, 64, 316-322

Barland, G. & Raskin, D. (1976). Validity and reliability of polygraph examinations of criminal suspects. (Report 76-1, Contract 75 NI-99-0001) Washington, DC: U.S. Department of Justice.

Bradley, M.T. & Warfield, J.F. (1974). Innocence, information, and the guilty knowledge test in the detection of deception. Psychophysiology, 21, 683-689.

Cimerman, A. (1981). "They'll let me go tomorrow": The Fay case. Criminal Defense, 8, 7-10.

Davidson, P.O. (1968). Validity of the guilty-knowledge technique: The effects of motivation. Journal of Applied Psychology, 52, 62-65.

Giesen, M. & Rollison, M.A. (1980). Guilty knowledge versus innocent associations: Effects of trait anxiety and stimulus context on skin conductance. Journal of Research in Personality, 14, 1-11.

Honts, C., Hodes, R. & Raskin, D. (1985). Effects of physical counter-measures on the physiological detection of deception. Journal of Applied Psychology, 70, 177-187.

Horvath, F. (1977). The effect of selected variables on interpretation of polygraph records. Journal of Applied Psychology, 62, 127-136.

Iacono, W.G., Boisvenu, G.A., & Fleming, J.A. (1984). Effects of diazepam and methylphenidate on the electrodermal detection of guilty knowledge. Journal of Applied Psychology, 69, 289-299.

Iacono, W.G. & Patrick, C.J. (1987). What psychologists should know about lie detection. In A.K.Hess & I.B.Weiner (Eds.), Handbook of forensic psychology. New York: John Wiley.

Iacono, W.G. & Patrick, C.J. (1988). Polygraph techniques. In R. Rogers (Ed.), Clinical assessment of malingering and deception. New York: Guilford Press.

Kleinmuntz, B. & Szucko, J.J. (1984). A field study of the fallibility of polygraphic lie detection. Nature, 308, 449-450.

Lykken, D.T. (1959). The GSR in the detection of guilt. Journal of Applied Psychology, 43, 385-388.

Lykken, D.T. (1981a). A Tremor in the Blood: Uses and Abuses of the Lie Detector. New York: McGraw-Hill.

Lykken, D.T. (1981b) The lie detector and the law. Criminal Defense, 7, 19-27.

Lykken, D.T. (1987). The case against polygraphy. In A. Gale (Ed.), The polygraph test: Lies, truth and science. Beverly Hills, CA: Sage.

Podlesny, J.A. & Raskin, D. (1978). Effectiveness of techniques and physiological measures in the detection of deception. Psychophysiology, 15, 344-359.

Stern, R.M., Breen, J.P., Watanabi, T., & Perry, B.S. (1981). Effect of feedback of physiological information on responses to innocent associations and guilty knowledge. Journal of Applied Psychology, 66, 677 681.

Table 1. Flow chart illustrating the experience of a police polygrapher who assists in 2,000 criminal investigations where there are two possible suspects in each case. Note that, although 100% of the 400 verified tests were correct, the examiner's over-all accuracy could have been anywhere from 50% (chance) to 100%.

I. THE FIRST SUSPECT IN EACH CASE IS POLYGRAPHED.

2000 SUSPECTS ARE TESTED, HALF OF THEM CLASSIFIED AS "DECEPTIVE."

1,000 "DECEPTIVE" SUSPECTS ARE INTERROGATED;

200 OF THEM CONFESS THEIR GUILT;

200 "FAILED" TESTS ARE VERIFIED AS ACCURATE.

1,000 "TRUTHFUL" SUSPECTS ARE CLEARED HENCE NOT INTERROGATED.

II. EXAMINER TESTS SECOND SUSPECT IN THESE 1,000 CASES ONLY.

1,000 SUSPECTS ARE TESTED, 500 CLASSIFIED AS "DECEPTIVE."

500 "DECEPTIVE" SUSPECTS ARE INTERROGATED;

100 OF THESE CONFESS THEIR GUILT;

100 "FAILED" TESTS ARE VERIFIED AS ACCURATE.

100 CLEARED SUSPECTS SHOWN TO HAVE BEEN TRUTHFUL;

THESE 100 "PASSED" TESTS ARE VERIFIED AS ACCURATE.

500 "TRUTHFUL" SUSPECTS ARE CLEARED AND NOT INTERROGATED.

III. SUMMARY OUTCOME

3,000 POLYGRAPH TESTS ARE ADMINISTERED, 400 VERIFIED AS ACCURATE.

THERE ARE NO VERIFIED ERRORS. APPARENT ACCURACY IS 100%.

THIS OUTCOME WOULD BE UNCHANGED IF THE TRUE ACCURACY WERE ONLY 50%.

Table 2. The four scientifically credible studies of polygraph accuracy in real-life or field circumstances. The data were aggregated by simply averaging the percentages shown.

STUDY:	BARLAND & RASKIN (1976)	HORVATH (1977)	KLEINMUNTZ & SZUCKO (1984)	IACONO & PATRICK (1987)	TOTALS
SENSITIVITY (GUILTY CALLED DECEPTIVE):	98%	79%	76%	98%	88%
SPECIFICITY (INNOCENT CALLED TRUTHFUL):	45%	50%	64%	55%	53%
OVERALL VALIDITY (MEAN OF ABOVE):	72%	65%	70%	77%	71%

Table 3. Aggregated results of 8 analog studies of the accuracy of the Guilty Knowledge Test (GKT).

STATUS OF SUBJECT:	GKT DIAGNOSIS		TOTALS	
	INNOCENT	GUILTY	N	ACCURACY*
GUILTY	19	142	161	88.2%
INNOCENT	147	5	152	96.7%

* For comparison with Table 2, the sensitivity (proportion of guilty suspects identified) of the GKT averaged 88.2% in these studies while the specificity (proportion of innocent suspects correctly identified) averaged 96.7%.

Identifying Drug Abusing Criminals

By

Eric D. Wish Ph.D.

Visiting Fellow, National Institute of Justice
(8/15/87)

Introduction

This paper describes issues relevant to the identification of drug abusers within the criminal justice system. In the first section, we discuss some of the reasons why the identification of drug abusing offenders may be an important role for the criminal justice system. This is followed by a review and comparison of available methods for screening large numbers of offenders for recent drug use. We conclude with a breif discussion of some policy implications of our review for identification and treatment of drug abusers within the criminal justice system.

Why identify the drug abusing offender?

To identify active criminals. During the past decade, substantial information collected from diverse offender populations has converged to show that hard drug abusing offenders are especially likely to commit both drug and nondrug crimes at high rates (Wish and Johnson 1986c). Heroin addicts in Baltimore reported committing six times as many crimes during periods when they used narcotics frequently as in periods of lesser use (Ball et al. 1981; also, McGlothlin 1979). Violent predators, the most criminally active class of incarcerated persons, were distinguishable by their histories of juvenile drug abuse and adult high cost heroin habits (Chaiken and Chaiken 1982). Drug abuse in an offender has been a prominent item in many of the more useful criminologic scales designed to predict recidivism (Blumstein et al.1986). Recent studies of arrestees in Washington D.C. and New York City have found that persons who test positive by urinalysis at arrest for one or more hard drugs (usually cocaine, heroin or PCP) had a greater number of rearrests than arrestees with a negative test result (Toborg et al. 1986; Wish et al. 1986b). And perhaps most important, treatment-induced reductions in narcotics use have been found to be associated with concomitant reductions in individual crime rates (McGlothlin et al. 1977). While early research focused primarily upon the link between heroin use and crime, a number of recent studies have documented a growing role of cocaine in street crime (Collins et al. 1985; Hunt et al. 1984; Johnson et al. 1985).

There are a number of reasons why drug abuse and crime are associated. In some instances, persons are so dependent upon a drug that they are driven to commit income generating crimes like theft, robbery, drug selling and prostitution. For other persons , the drug abuse appears to be merely one of many deviant behaviors they engage in, while for others, the crime may be the result of a violent, bizarre reaction to a drug. In planning effective responses for each person, it may be necessary to understand which of the above motives apply.

Because drug abusing offenders account for a disproportionate share of all crime, a policy that focuses upon identifying drug abusing offenders and applying appropriate interventions has promise for producing a substantial impact on community crime and the overburdened criminal justice system. Certainly one would prefer to apply limited criminal justice resources to the most active offenders. There is growing evidence that criminal justice referral of offenders to drug abuse treatment programs, often accompanied by urine monitoring, can result in persons remaining longer in treatment and in a reduction in both drug use and crime (Anglin et al. 1984; Collins et al. 1983; Stitzer 1986). There is also the possibility that one might reduce jail and prison overcrowding by referring drug abusing detainees to treatment and/or urine monitoring programs. In addition, because younger offenders are less likely to inject hard drugs and to use heroin, identification of the youthful offender who is abusing such drugs as marijuana, PCP or cocaine has promise for enabling society to intervene in and prevent the progression to more extensive drug use (Dembo et al. 1987; Wish et al. 1986b).

To identify persons in need of drug abuse treatment and health care. Abusers of hard drugs, and especially persons who inject drugs, are at high risk for health problems (Goldstein and Hunt 1984). Intravenous drug users are especially at high risk for contracting AIDS by sharing dirty needles that contain blood from infected fellow addicts (Marmor et al. 1984). Prostitutes are also likely to have serious drug abuse and associated health problems. The probability of a urine positive for drugs was higher for female arrestees in New York City than for male arrestees (Wish et al. 1986b) . More than 69% of the prostitutes among the female arrestees studied in New York City in 1984 were positive for cocaine. These females frequently reported instances of childhood sexual abuse and protracted histories of emotional and health problems. Because prostitutes usually receive fines or very short sentences (often as time-served) they are usually back on the streets of New York within hours of arrest, with no effort made to identify and treat their drug abuse or health problems. Given that more than one half of the arrestees in Washington, DC and in New York City have been found to test positive for one or more drugs, it would seem that the criminal justice system offers an unusual opportunity to society for identifying persons in need of immediate health care.

To monitor community drug use trends. As illicit drugs become available in a community, the more deviant persons can be expected to be among those who first use them. In time, use spreads to the larger society. One might therefore predict that changes in the level of illicit drug use in an offender population would be a leading indicator of community drug use. A comparison of urine test results for arrestees in Washington D.C. with the traditional indicators of community drug use showed this to be the case (Wish 1982; Forst and Wish 1983). The rise in heroin use in Washington, DC between 1977 and 1980 showed up in the statistics from the arrestee urine testing program, one to 1.5 years before it appeared in local statistics on overdose deaths, hospital emergency room admissions and drug abuse treatment program admissions. The results from the arrestee urine test ing program in Washington and our research in New York (Wish et al. 1986f) have also documented the rising use of cocaine in these cities 80's.

By operating a program of drug testing of arrestees on a regular basis, communities may derive a secondary bonus of being able to detect drug epidemics earlier, and being able to plan community responses. The potential benefit of urine testing of offenders for tracking drug crime trends has prompted the National Institute of Justice to establish a national Drug Use Forecasting (DUF) system based on urine samples obtained periodically from arrestees in large cities (Science 1986, NIJ Reports 1987). The impact of law enforcement and other interventions designed to reduce drug use and production can also be measured by an ongoing drug testing program. A study of the feasibility of establishing urine screening in jail facilities conducted in the 1970's serendipitously uncovered the availability of propoxyphene in the area. These results alerted law enforcement agencies to the problem so that action to locate the suppliers could be taken (NIDA 1979).

How can one identify the drug abusing offender?

For a civil commitment program to operate within the criminal justice system , there must be a feasible means available for screening large numbers of persons for recent drug use. The methods utilized must be low in cost, accurate, and capable of being implemented with minimum disruption to the already overburdened criminal justice systems in most large cities. We focus on four methods; offenders' self-reports, criminal justice records, urinalysis tests and radioimmunoassay of hair (RIAH). We have excluded blood tests from consideration because of the general difficulty presented by drawing blood from large numbers of detainees as well as fears of transmission of AIDS. We also have excluded breathalyzer tests because alcohol is a licit drug, is not in itself an indicator of high rate criminal activity (Wish 1986e). We also excluded physical and behavioral signs of drug use and intoxication, primarily because they are already widely employed to identify the sick drug abusing offender who is experiencing withdrawal symptoms or strong drug reactions, but are of less utility for identifying other users. We do discuss hair analysis even though it is at an experimental stage and still very expensive, because it has some interesting potential advantages over the other techniques. A more detailed description of these techniques can be found in Wish(1986f).

Offenders' self-reports

There is a long tradition in social science research of being able to obtain valid self-reports about deviant behaviors, including illicit drug use. Some of the best estimates of drug use have come from studies involving personal interviews or self-administered questionnaires (Robins 1974; Elliott and Huizinga 1984; O'Donnell et al. 1976, McGlothlin et al. 1977; Johnston et al. 1977). Much of what we know about the relationship of drug abuse to crime has also come from studies that have relied upon offender's self-reports. The validity of the information obtained in these studies has usually been tested and affirmed by comparing the respondent's self-reports with information in official records or the results of a urinalysis of a specimen obtained at the conclusion of the interview (Wish and Johnson 1986c; Harrell 1985). Even when we have interviewed active criminals in our secure, confidential research storefront in East Harlem, we have found considerable agreement between self-reported drug use and the urine tests (Wish et al. 1983ab). Among the most important reasons why the respondents in these studies appear willing to disclose sensitive information about themselves are that the data are collected voluntarily, for research purposes only, in a safe environment, and that the anonymity and confidentiality of the information is assured.

These are conditions that do not exist when attempting to identify drug using offenders detained in the threatening criminal justice system. The evidence is convincing that detainees will severely underreport their recent drug use, even in a voluntary, confidential research interview. Table 1 compares the estimates of drug use obtained in an arrestee population from self-reports in a research interview with their urine specimens analyzed by EMIT tests. It is clear that twice as many arrestees were found positive for any drug by urinalysis than admitted to recent use in a confidential voluntary research interview in Manhattan

TABLE 1

EVEN IN A CONFIDENTIAL RESEARCH INTERVIEW,
ARRESTEES UNDERREPORTED THE RECENT
USE OF DRUGS

	REPORTED USING DRUG 24-48 HRS. BEFORE ARREST (n=4847)	POSITIVE BY EMIT AT ARREST (n=4847)
	%	%
Cocaine	20%	42%
Opiates	14%	21%
Methadone	6%	8%
PCP	3%	12%
Any of the above:	28%	56%
2+ of above:	11%	23%

Central Booking. The arrestees who refused to participate in the confidential research interview had a high likelihood of rearrest similar to that found for arrestees who provided a urine that was positive for multiple drugs. When the pretrial release interview information was compared with their urinalysis test results, arrestees in Washington, DC. were also been found to underreport their recent use of drugs by about one-half (Toborg et al. 1986). Similar findings were obtained from a recent study of probationers assigned to the intensive supervision probation program in New York City (Wish et al. 1986d). In that study, only 24% of the probationers admitted to recent use of a drug in a research interview held in a

private area in the probation department office, while 68% tested positive by urinalysis (Table 2). Moreover, probation officers, who indicated that they relied most on the probationer for information about his current drug use also underestimated (23%) the prevalence of current drug use in their cases.

TABLE 2

ESTIMATES OF RECENT DRUG USE IN PROBATIONERS, FROM SELF-REPORTS, URINE TESTS, AND PROBATION OFFICER RATINGS
(N = 66 Interviewed probationers with urine test and officer's rating)

Drug	Probationer Reported Using In 24-48 Hours Before Interview	Percent of Probationers Rated By PO As Using Drug In Past Month	Urine Test At Interview
Marijuana	24%	21%	42%
Cocaine	3%	9%	52%
Heroin	3%	3%	2%
PCP	0	0	2%
Methadone	2%	3%	0
Any of above	24%	23%	68%

If one cannot obtain valid self-reports of recent drug use in a voluntary confidential research interview held within the criminal justice system, it is obvious that one could not do so when the information is to be used by someone to commit the person to treatment or urine monitoring.

In spite of these limitations, there are important uses for self-reports for identifying drug abusers detained by the criminal justice system. Although self-reports would detect only a small portion of drug users, the persons who do admit to drug use are a bona fide group for further action. A study of juvenile detainees (Dembo et al. 1986) found that youths who tested negative for marijuana but admitted to recent marijuana use had detention records that were more similar to persons who tested positive than to youths who were negative by test and self-report. The authors conclude that it would be beneficial to select out for further assessment youths who were positive by urine test or who reported recent drug use.

Furthermore, in our study of arrestees in New York City we found that self-reports of current dependence on drugs or a need for treatment were valuable in differentiating which of the persons who tested positive were more seriously involved with drugs and crime. Table 3 shows that among all arrestees who tested positive, those who admitted to dependence on drugs or alcohol at arrest or a need for treatment were much more likely to have reported the recent use of drugs, injection of cocaine, and prior treatment. The dependent persons also had more extensive criminal records than did the nondependent persons.

TABLE 3

DRUG USE AND CRIMINAL HISTORY IN ARRESTEES WHO TESTED POSITIVE FOR DRUGS, BY SELF-REPORTED DEPENDENCE OR NEED FOR TREATMENT

	Positive, Not Dependent (1651) %	Positive, Dependent* (926) %
DRUG USE (from self-reports)		
Reported using 24-48 Hrs prior to arrest:		
Cocaine	15%	61%
Heroin	6%	53%
Marijuana	34%	36%
Downers	2%	12%
Illicit Methadone	1%	8%
PCP	3%	6%
Injects cocaine:	9%	61%
Ever received drug treatment:	11%	60%
CRIMINAL HISTORY (from records)		
Ever arrested before:	78%	91%
2+ prior misdemeanor convictions:	32%	60%
2+ prior felony convictions:	10%	14%
Had a prior arrest for a drug-related offense:	33%	59%

*Male arrestees who tested positive for one or more drugs (opiates, cocaine, PCP or methadone) and who reported current dependence on drugs or alcohol, or a need for treatment.

Thus, while many drug abusers will conceal their drug problems, those who do report serious drug problems while in the criminal justice system maybe a valid group for further assessment and diversion to treatment. Jurisdictions wishing to implement some immediate, low cost action to identify drug abusers could assign persons to interview detainees and refer them to treatment programs. Although many drug abusers would go undetected, the number of persons identified would probably be all that most cities could handle, anyway, given the usually overburdened and limited treatment resources.

In summary, self-report information can be very valuable for obtaining indepth details about drug abuse, if the offender is willing to disclose the information. It is a poor method to rely on as the primary tool for screening for drug users detained in the criminal justice system. The most promising use for offender

self-reports in the criminal justice setting is probably in conjunction with other evidence of drug use that can be used to motivate the offender to discuss his behavior.

Criminal justice records

The criminal justice system maintains extensive files of information on offenders. Given our discussion above, and that much of the information in these records is obtained from the offender, it is not surprising to find that information about the offender's involvement in drugs is often minimal and unreliable (Goldstein 1986).

Even when an arrest report has a place to enter information about the arrestee's drug use, it typically is not completed. This is probably because the police officer often is unaware of the arrestee's involvement with drugs and because information not of immediate relevance to an officer tends not to be reliably entered into a data system. Even in Washington, D.C. where the U. S. Attorney has installed the PROMIS (prosecutor's management information system) system to track case information, the arresting officers identified as drug involved only 22% of the persons who were found positive for drugs at arrest by urinalysis (Wish et al. 1981). Pre-sentence investigation reports should contain more information about the offender's background. However, in the absence of urine tests, the investigator must rely upon the defendant's admission of drug use or that from a family member. And in large cities, the time and resources available for soliciting such information is limited.

If records do not contain detailed information about drug involvement, can a person's record of arrest or convictions for a drug offense serve as an accurate indicator or drug use? The evidence indicates that persons charged with the sale or possession of controlled substances are most likely to be drug users(Table 4) .

TABLE 4

WHAT CHARGES WERE MOST ASSOCIATED WITH HAVING A POSITIVE URINE TEST?

Arrest Charge	(N)	Percent Positive*
Possession of drugs	(615)	76%
Sale of drugs	(355)	71%
Poss. stolen property	(474)	61%
Forgery	(94)	60%
Burglary	(348)	59%
Murder/manslaughter	(64)	56%
Larceny	(667)	56%
Robbery	(676)	54%
Weapons	(157)	53%
Stolen credit cards	(56)	52%
Criminal mischief	(66)	48%
Gambling	(147)	45%
Sexual assault	(79)	41%
Public disorder	(108)	37%
Assault	(506)	37%
Fare beating	(98)	37%
Fraud	(54)	30%
Other offenses	(269)	45%
Total:	(4833)	56%

*Positive by EMIT for opiates, cocaine, PCP or methadone.

Almost three quarters of male arrestees in NYC (and of arrestees in Washington DC) charged with these offenses in 1984 tested positive for opiates, cocaine, methadone or PCP. However, more than one half the persons charged with robbery, burglary, larceny, or murder were also positive for drugs (Wish et al. 1986b). And 56% of the arrestees were positive for a drug when only 20% of the sample were charged with a drug offense. Only 10% of the 17,000 male and female arrestees drug positive by urinalysis in Washington, DC in 1973-4 were charged with a drug offense (Wish et al. 1981). Thus, while offenders with a history of drug offenses are most likely to be using drugs, it is clear that offenders charged with a variety of other offenses may be drug users. By relying solely upon a drug offense to identify the drug user, one would miss the majority of users.

Urinalysis tests

In recent years urinalysis tests have received considerable attention as a source of information about an offender's drug use (Wish 1982; Forst and Wish 1983). It should be noted, however, that researchers have been using the tests for the past 15 years as a means to validate information obtained in interviews about recent drug use. And drug abuse treatment programs have often monitored patients' drug use by urinalysis (McGlothlin et al. 1977). Urine tests were employed successfully by the Department of Defense to screen army personnel before they left Vietnam for the States in the 1970's, and in recent years to combat a growing drug use problem. Furthermore, in the initial years of the federally sponsored TASC (treatment alternatives to street crimes) program, urinalysis was used to identify drug using offenders for diversion into treatment programs. Urine tests have been used by the U.S. Department of Probation and by local probation departments to screen suspected drug users. Mass screening of offender populations for drugs has been used only in Washington, DC, however, where all arrestees detained in the Superior Court lock-up prior to court appearance have been tested, since 1971.

There are a number of possible urinalysis techniques and a common error made by persons when assessing the validity of drug testing is to fail to consider the type of test used. Until recently, most urine testing of offenders in the criminal justice system and in treatment programs was conducted using a thin layer chromatography (TLC) general screen. This technique is especially economical because it can screen for a variety of drugs, but is a very subjective process requiring experienced technicians to interpret the results.

Primarily because of their low cost, sensitivity, and ease of use, the most commonly used urine tests today are the EMIT (enzyme multiplied immune test) tests. These tests involve a chemical reaction of the specimen with an antibody designed to react to a specific drug. The chemical reaction causes a change in the specimen's transmission of light. This change in transmissibility is detected by a machine that provides a quantitative reading that is compared with the reading from a standard solution containing a known concentration of the drug. If the reading from the specimen is higher than that of the standard, the specimen is positive for that drug. Because the determination of a positive is based on specific numbers, the level of subjectivity required by the EMIT test is less than that required by TLC. TLC looks more economical because for approximately $2.00 one can screen for as many as 20 different types of drugs. EMIT tests are specific to one drug, and cost between $1.00 and $5.00 for each drug tested. (These are high volume, reduced rates charged to researchers by the New York State Division of Substance Abuse Testing Laboratory.)

Table 5 presents a comparison of the results from 4,847 specimens obtained from arrestees in New York City and tested by TLC and the comparable EMIT technique, by the New York State Testing Laboratory.

TABLE 5

DRUGS DETECTED IN URINE SPECIMENS FROM
MALE ARRESTEES, BY TYPE OF TEST
(n=4847 Specimens)

Drug Detected	TLC	EMIT
Cocaine	14%	42%
Opiates (morphine)	9%	21%
PCP	NA	12%
Methadone	4%	8%

It is clear that the TLC test underdetects the common street drugs by almost two-thirds. Many laboratories have used a two-test approach to identifying drugs. They would first screen for drugs using TLC and then confirm any positive result by an EMIT test. Such a procedure would clearly result in many drug users escaping detection. As a result of the findings above, EMIT tests are being substituted for TLC tests across the country.

The growing popularity of the EMIT tests has made them the object of several legal challenges. The primary criticism is that the EMIT tests have too high a rate of false positive errors. That is, the tests falsely indicate the presence of a drug. Much of the debate surrounds the possibility that some common licit drugs can cross-react with the test's reagents to produce a positive result (Morgan 1984). The ingestion of poppy seed bagels has been found to produce a positive test result for opiates. Furthermore, the EMIT test for opiates, will detect heroin (morphine) as well as prescribed drugs such as codeine. Sloppy recording procedures by laboratory staff and failure to maintain the chain-of-custody of the specimen can also produce serious test errors.

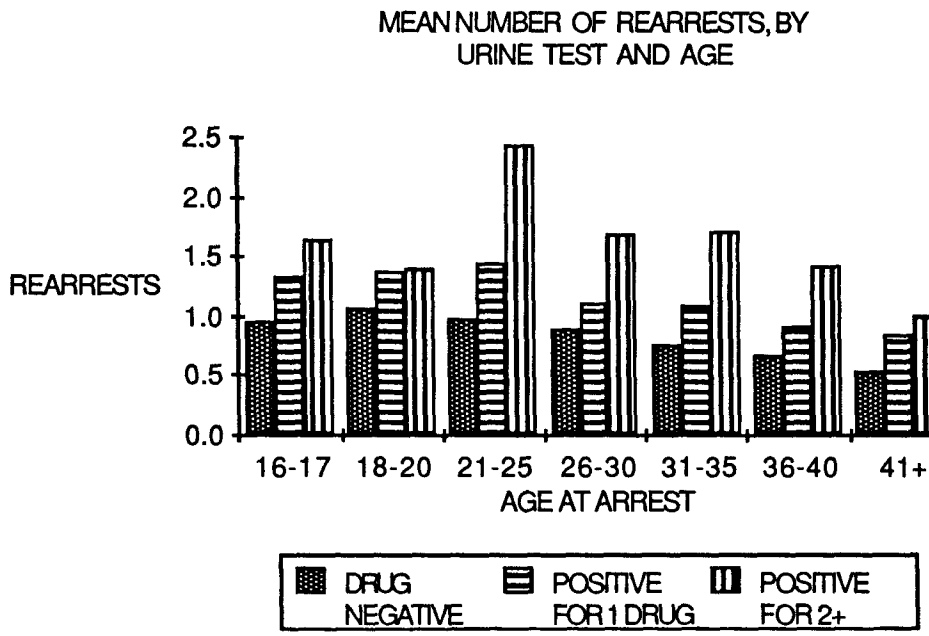
There are other urinalysis techniques available for detecting drugs, including radioimmunoassay and GC/MS, gas chromatography and mass spectrometry (Hawks and Chiang 1986). Some of these techniques have not been used frequently in the criminal justice system and sufficient case law does not exist regarding whether the courts consider them to be valid. GC/MS is too costly and time consuming to be used as the initial test in large scale screening programs although it has been required by some courts as a confirmation test.

A study by the Center for Disease Control (CDC) has been cited for its report of substantial errors in the results from the 13 labs that were surveyed (Hansen 1985). In a blind experiment, the CDC sent a group of blank urine specimens as well as specimens containing known quantities of drugs to the labs for analysis (the specific urinalysis tests used by the labs were not specified). The study found that while some labs failed to detect specific drugs contained in the specimens, few instances occurred where a lab reported a drug in one of the blank specimens. In fact, the average accuracy of the analyses of the blank specimens was 99% and there were so few false positive results that the analyses of this issue were limited.

Our experience using EMIT tests in offender populations also indicates that the problem of false negatives is much larger than that of false positive errors (except for the test for amphetamines, which may test positive for a number of chemically similar, licit drugs). In contrast to controlled laboratory experiments, when one tests for illicit drugs in offenders one cannot control for many of the factors that influence the concentration of the drug in the urine. The quantity of the drug taken, its purity, and its time since ingestion, are unknown. It is therefore somewhat amazing when a test does detect a drug! Our studies show that even when a person admits to taking a drug during the prior one or two days covered by the test, it is found in only 70% to 80% of the cases. Many drug users will, thus, escape detection by urinalysis.

It is probable that the future of urine testing in the criminal justice system will depend on a satisfactory solution to the problem of false positive errors. Preliminary NIDA guidelines for testing, state that all positive test results from immunoassay tests should be confirmed by GC/MS. GC/MS is the most accurate technique available for identifying drugs in the urine, but it costs about $70-$100 per specimen. It seems appropriate to require such a procedure when a single test result may cause a person to lose their job or liberty. However, when a test result is used solely to trigger further investigation of whether a person is involved with drugs, it may be that confirmation by other methods (urine monitoring or diagnostic interview) would be equally acceptable. The courts have yet to decide this issue.

Even though urine tests do contain some degree of error, the evidence is strong that the tests have a high degree of validity. The EMIT tests have been ruled valid by judges, although courts have differed on the need for confirmation of positive results (Wish 1986f). Furthermore, the construct validity of urine tests, the evidence that the the relationships found with the tests are consistent with the current knowledge about drug use, is impressive. Studies of arrestee and probationers in New York City and Washington, D.C. have found hypothesized relationships between detected drug use and age, prior arrest history, type of arrest charge and recidivism (Wish and Johnson 1986; Wish et al. 1986b; Toborg et al. 1986). And a positive test for marijuana was related to greater lifetime use of marijuana and a greater number of juvenile detentions in juveniles in Tampa (Dembo et al. 1986) In fact, we first discovered the lesser sensitivity of the TLC test in our research because the analyses of specimens from unapprehended offenders interviewed in a research storefront in East Harlem did not confirm the heavy drug use that these persons were reporting! Only after the EMIT tests were used was the claimed drug use verified by the urine tests (Wish et al. 1983b). Perhaps of primary significance is the finding from studies in Washington, D.C. and New York that not only the presence of a drug, but the **number** of drugs detected was related to criminal behavior. For all age groups, arrestees positive for two or more drugs (usually cocaine and opiates) had the greatest number of rearrests. Furthermore, 60% of the rearrests for multiple drug users were for offenses other than the sale or possession of drugs.



Measures rearrests in an 11-17 month period after the index arrest. These findings do not control for time at risk on the street. Differences would be expected to be more extreme, however, because drug users were somewhat more likely to be remanded after arraignment than were nonusers.

It is unknown what proportion of offenders who are found positive are seriously involved with drugs. For this reason, a positive urine test should be used with other information (self-reports, criminal justice records, or repeated urine testings) to determine whether the offender chronically abuses drugs and is in need of treatment.

Radioimmunoassay of hair (RIAH)

RIAH is an experimental procedure with potential for drug detection. As hair is formed in the scalp, the cells are nourished by the blood, and drugs present in the blood are deposited in the cells at the root level. One can extract the drugs from the hair and analyze them by radioimmunoassay. Researchers have found that the level of the drug taken is correlated with the amount deposited in the hair cells. Perhaps of most importance is that one can obtain a historical record of the level of drug use of the person. While hair at the scalp level contains evidence of current use, hair further from the root contains evidence of use months ago when it was formed. Thus, by analyzing sections of hair (especially in persons with long hair!), one can discern a trend in drug use over time (Thanepohn 1986; Witherspoon and Trapani 1983). Procedures are available for detecting the most commonly abused drugs.

One possible advantage of RIAH is that one cannot easily fake the test. For example, one cannot suspend use before a scheduled test to avoid detection. Once the drug is stored in the hair, it remains there permanently. And the technique of obtaining hair is non-invasive and less objectionable to some persons than that of obtaining urine. The analysis can provide evidence of the level and trend of use over time. In addition, if the test is inconclusive or a retest is required, one can more easily (than urine) obtain a similar sample for analysis. The largest drawbacks to the test include the fact that it requires raidioactive materials and the types of precautions usually needed in handling such substances, the cost (roughly $50 per drug tested), the turn-around time of approximately 24 hours, and the unavailability of standardized and accepted extraction techniques. In addition, there is some possibility that the content of the hair can be influenced by environmental contaminants (Puschel et al. 1983).

Even if current research confirms the utility of RIAH, the long turnaround time for the analysis and the cost, may prohibit the adoption of the method for large scale screening of offenders. In addition, it will take considerable time for the courts and the scientific community to acknowledge the validity of the new technique. If the technique is eventually accepted and the analysis time remains long, the technique will most likely be less useful than other techniques for testing arrestees pretrial, where the judge typically requires the results quickly at the time of arraignment. Perhaps the most valuable use for RIAH with offenders, will be for the confirmation of the results of other tests and for the verification of changes in the person's use.

Conclusion

We conclude that in a criminal justice setting, urine testing is the most feasible and accurate method now available for screening large numbers of offenders for drug use. Self-report and record information can be effectively used to verify and extend information about seriousness of use in persons who test positive. The newer RIAH methods offer promise for delineating patterns of drug use over time, if the method is valid, can be standardized, and gains acceptance from the scientific and judicial communities. We also conclude that:

- Fewer than one-half of the adults detained or supervised by the criminal justice system will voluntarily admit to recent use of illicit drugs;

- Those persons who do report current drug abuse problems or dependence tend to have serious problems and are a valid group for consideration for treatment;

- Urinalysis can be an effective tool for screening large numbers of offenders for recent drug use. However, the tests only indicate probable use and must be followed by confirmation of level of drug involvement. Confirmation can be achieved through repeated testing over time, confrontation and interview with the persons, and information obtained from records or reports from persons who know the detainee.

We have intentionally limited our discussion to the methods available for identifying drug abusers within the criminal justice system. Other research has examined the efficacy of various types of treatment for persons who have been referred from the criminal justice system. It is important to note, however, that because little systematic screening for drug abusers has occurred in the criminal justice system, most research has examined treatment process and outcome for the select group of offenders who were referred from the courts. Little is known, outside of the research from the pretrial testing program in Washington D.C. (Carver 1986), about how effective such interventions would be for the larger, more diverse group of treatment referrals that would result from a widescale urine screening program. Additional research into how best to match criminal justice referral clients to appropriate effective interventions will be necessary in order to fully utilize urine screening and monitoring as tools for the criminal justice system.

REFERENCES

Ball, John C., Roxen, Lawrence, Flueck, John A., and Nurco, David N. The criminality of heroin addicts when addicted and when off opiates. Pp. 39-66 in James A. Inciardi, ed., The Drugs-Crime Connection. Beverly Hills, Calif.: Sage Publications, 1981.

Blumstein, Alfred, Cohen J., Roth J.A. and Visher, C. A. Criminal Careers and "career criminals." Volume I. Washington, D.C.: National Academy Press, 1986.

Carver, John A.. Drugs and crime: controlling use and reducing risk through testing. NIJ Reports/SNI 199, September, 1986.

Chaiken, Jan and Chaiken, Marcia Varieties of Criminal Behavior. Santa Monica, Calif.: Rand Corporation, 1982.

Collins, James J., and Allison, Margret Legal coercion and retention in drug abuse treatment. Hospital and Community Psychiatry 14(12):1145-1149, 1983.

Collins, James J., Hubbard, Robert, and Rachal, J. Valley Expensive drug use and illegal income: a test of explanatory hypotheses. Criminology 23:743-764,1985.

Dembo, Richard, Wish, E.D., Getreu, A., Washburn, M., Schmeidler, J., Estrellita, B., and Blount, W. R. Further Examination of the Association Between Heavy Marijuana Use and Crime Among Youths Entering a Juvenile Detention Center. Presented at the Annual Meeting of the American Society of Criminology, Atlanta , November, 1986.

Dembo, Richard, Washburn, M., Wish, E.D., Yeung, H., Getreu, A., Berry, E. , and Blount, W. Heavy Marijuana Use and Crime Among Youths Entering a Juvenile Detention Center. Journal of Psychoactive Drugs: 19: 1987.

Elliott, Delbert S., and Huizinga, David The Relationship Between Delinquent Behavior and ADM Problems. Boulder, Colo.: Behavioral Research Institute,1984.

Forst, Brian, and Wish, Eric Drug use and crime: providing a missing link. Pp. 84-95 in Kenneth R. Feinberg, ed., Violent Crime in America. Washington, D.C.: National Policy Exchange, 1983.

Goldstein, Paul J. Homicide related to drug traffic. Bull. N. Y. Acad. Med. 62:509-516, 1986.

Goldstein, P. J. and Hunt, D.E. Health consequences of drug use. Final report to the Carter Center of Emory University, Atlanta, 1984.

Hansen, Hugh J., Caudill, Samuel P., Boone, D. Joe Crisis in drug testing: results of CDC blind study. JAMA, 253: 2382-2387, 1985.

Harrell, Adele V. Validation of self-report: The research record. In B.A. Rouse, N. Kozel and L. Richards (Eds.) Self-report methods of estimating drug use. NIDA research monograph #57. Washington D.C., U.S. Government Printing Office. 1985.

Hawks, Richard L. and C. Nora Chiang, eds. Urine testing for drugs of abuse. NIDA research monograph 1986.

Hunt, Dana, Lipton, Douglas S., and Spunt, Barry Patterns of criminal activity among methadone clients and current narcotics users not in treatment. Journal of Drug Issues 14:687-702, 1984.

Johnson, Bruce D., Goldstein, Paul, Preble, Edward, Schmeidler, James, Lipton, Douglas S., Spunt, Barry, and Miller, Thomas Taking Care of Business: The Economics of Crime by Heroin Abusers. Lexington, Mass.: Lexington Books, 1985.

Johnston, Loyd D., Bachman, J. G., and O'Malley, P.M. Drug use among Amewrican high school students 1975-77. National Institute on Drug Abuse, Washington, D.C.: U.S. Government Printing Office, 1977.

Marmor, Michael, Des Jarlais, Don C., Friedman, Samuel R., Lyden, Margaret, El-Sadr, Wafaa. The epidemic of acquired immunodeficiency syndrome (AIDS) and suggestions for its control in drug abusers. Journal of Substance Abuse Treatment, 1:237-247, 1984.

McGlothlin, William H. Drugs and crime. Pp. 357-365 in Robert L. DuPont, Avram Goldstein, and John O'Donnell, eds., Handbook on Drug Abuse. Rockville, Md.: National Institue on Drug Abuse, 1979.

McGlothlin, William H., Anglin, M. Douglas, and Wilson, Bruce D. An Evaluation of the California Civil Addict Program. Services Research Issues Series. Rockville, Md.: National Institute on Drug Abuse, 1977.

Morgan, John P. Problems of mass screening for misused drugs. Journal of Psychoactive Drugs 16(4):305-317,1984.

National Institue on Drug Abuse, Monitoring drug abuse in the community through a jail urine screening program. Washington, DC. GPO# (ADM) 80-903, 1979.

NIJ Reports. SNI 202, National Institute of Justice, March/April, 1987.

O'Donnell, John A. , Voss, Harwin L., Clayton, Richard, Slatin, Gerald T., and Room, Robin G. Young Men and Drugs--A Nationwide Survey. Research Monograph 5. Rockville, Md.: National Institute on Drug Abuse, 1976.

Puschel, K., Thomasch, P. and Arnold, W. Opiate levels in hair. Forensic Science International., 21, 181-186, 1983.

Robins, Lee N. The Vietnam drug user returns. Special Action Office Monograph, Series A, No. 2. Washington, DC.: U.S. Gonvernment Printing Office, 1974.

Science. Growing focus on criminal careers. Science, 233: 1377-1378, 1986.

Stitzer, Maxine and Mary E. McCaul. Criminal Justice Interventions with Drug and Alcohol Abusers: The Role of Compulsory Treatment. In Braukman, Curtis J. and Edward K. Morris, eds. in press. Behavioral Approaches to Crime and Delinquency. New York: Plenum Press.

Thanepohn, Susan. A new wrinkle: Testing hair for drugs. The U.S. Journal, 10, April, 1986.

Toborg, Mary, Bellassai, J.P. and Yezer, A.M.J. The Washington, D.C. urine testing program for arrestees and defendants awaiting trial: a summary of interim findings. Presented at the NIJ sponsored conference, Drugs and Crime: Detecting Use and Reducing Risk, Washington, D.C., June 5, 1986.

Wish, Eric D., Klumpp, K.A., Moorer, A.H., Brady, E. and Williams, K.M. An Analysis of Drugs and Crime Among Arrestees in the District of Columbia, Executive Summary. U.S. Department of Justice Publication, U.S. Government Printing Office (I982-36I-233/6346) December, I981.

Wish, Eric D. Urine testing of arrestees: A tool for reducing drug abuse and crime. Presented at the annual proceedings of the American Psychological Association, Washington, D.C., August, I982.

Wish, Eric D., Johnson, B., Strug, D., Anderson, K. and Miller, T. Concordance between self-reports of drug use and urinalysis test results from active unapprehended criminals, unpublished manuscript, 1983a.

Wish, Eric D., Strug D., Anderson, K., Miller, T. and Johnson, B. Are urine tests good indicators of the validity of self-reports of drug use? It depends on the test. Presented at the annual meeting of the American Society of Criminology, Denver, November, 1983b.

Wish, Eric D. PCP and crime: just another illicit drug? Presented at the NIDA Technical Review meeting on PCP, Rockville, MD, May, 1985. Published in NIDA Research Monograph 64, Phencyclidine: An Update, 1986a.

Wish, Eric D., Brady, E., and Cuadrado M. Urine testing of arrestees: findings from manhattan. Presented at the NIJ sponsored conference, Drugs and Crime: Detecting Use and Reducing Risk, Washington, D.C., June 5, 1986b.

Wish Eric D., and Johnson B.D. The impact of substance abuse on criminal careers. In Blumstein, A., Cohen J., and Christy A. Visher , eds., Criminal Careers and Career Criminals, Volume II, Washington, D.C.: National Academy Press, 1986c.

Wish, Eric D., Cuadrado, M., and Martorana, J. Estimates of drug use in intensive supervision probationers: results from a pilot study. Federal Probation, Vol L. (4) 1986d.

Wish, Eric D., Chedekel, M., Brady, E. and Cuadrado, M. Alcohol use and crime in arrestees in Manhattan. Presented at the American Academy of Forensic Sciences Annual Meeting, New Orleans, February 1986e.

Wish, Eric D. Identification of drug abusing offenders: A guide for practitioners. Presented at the National Research Council Workshop on Drugs and Crime, Atlanta, December 1986f.

Wish, Eric D. Drug use in arrestees in Manhattan: The dramatic increase from 1984 to 1986. Report released to the press, February, 1987.

Witherspoon, Lynn R., Trapani, Joseph S. Forensic radioimmunoassay--a new area. Journal of Nuclear Medicine, 20:796-797, 1983.

VOICE RECOGNITION

Harry Hollien
Institute for Advanced Study of the Communication Process
University of Florida, Gainesville, Florida

INTRODUCTION

Almost anyone who has normal hearing, and who has lived long enough, has had the experience of recognizing some unseen speaker -- usually someone familiar -- solely from listening to his or to her voice. It was from this common everyday experience that the myth of speaker identification was born. References to the process in novels, comic strips, the movies and television have resulted in a perpetuation and refinement of the myth to a point that, presently, many people believe such things as: 1) the speaker identification process is infallable -- or nearly so, 2) technologically we can carry out voice identification with exactitude, 3) "voiceprints" are the direct equivalent of fingerprints and so on. Therein lies the structure of the myth.

On the other hand, this myth, like practically all others, is based (at least in part) upon the truth. There is some validity to voice/speech identification and, at least, some of the fundamental relationships are understood. For example, while it is not yet known if every one of the five billion people in the world produce utterances that are so idiosyncratic they are unique from those of every other one of those billions of speakers, it <u>is</u> known that humans can discriminate auditorily between and among different speakers.

But what is known about the process of speaker identification? It has been established that anyone who attempts such tasks has, at least, some logic and research to support his or her efforts. It also is known that there are severe -- some very severe -- problems associated with the practical application of any method, technique or process of this kind. But first, some definitions.

The Speaker Identification Area

In reality there are three independent yet related problems within this area; speaker identifiation is only one of the three. They are speech recognition, speaker verification and speaker identification. Even though rather substantial progress has been made relative to the first of these problems -- and modest progress on the second -- the fact remains that there are no operating systems currently in existence that permit anything but the most limited speech/speaker recognition tasks to be carried out. But what are these three subareas?

Speech Recognition If it were possible for machines to decode spoken or tape recorded utterances, it also would be possible to automatically carry out such tasks as banking by telephone, controlling minimum security prisons with very small numbers of personnel, activating and controlling machinery which manipulates radio-active materials, operating drones/satellites by voiced commands, automatically typing spoken messages and so on. Yet, as Doddington (1980) points out, reasonably good speech recognition by machine currently is not possible. There are a number of reasons for this situation; prominent among them is the fact that, even when a limited speech recognition scheme is placed on-line, it very often

fails due to the fact that it is not speaker independent. In order to operate effectively, the device must recognize the talker and then proceed to analyze his or her speech patterns. To date, there are no systems that can successfully perform these functions for any except very small populations.

Speaker Verification. The problem of speaker verification is generally on a par with that of speech recognition. In this case, it is not necessary to interpret what the speaker says but rather to verify his or her identity and, in the basic speaker verification paradigm, the talkers usually want to be recognized. The potential uses for a working system of this type are virtually endless. Access to secure areas by voice analysis is one example; verification of the identity of an officer giving commands over a radio, walkie talkie -- or any channel where he cannot be identified by sight -- is another. So is the need to verify the identity of individuals who are speaking from aircraft, space capsules, hyperbaric chambers/habitats, tanks or other remote stations or locations. In any case, substantial research is being carried out in this area (in the U.S. especially by organizations such as the Bell Telephone Laboratories; Texas Instruments; Bolt, Beranek and Newman -- see, among others: Atal, 1972, 1974; Bricker, et al, 1966; Doddington, 1971; Doddington, et al, 1974; Furui, 1981; Makhoul and Wolf, 1973; Pruzanski, 1963; Pruzanski, et al, 1964; Rosenberg and Sambur, 1975; Schafer and Rabiner, 1970; Wolf, 1970; Wolf, et al, 1983). Here the task, while formidable, is straightforward. The individual talker ordinarily is cooperative (that is, unless he is an imposter) and, even though the speech sample cannot be contemporary, the equipment utilized is of high quality, is continually updated and the nature of the sample is

controlled. Then too, an extensive reference set can be developed on each talker. Nevertheless, rather substantial problems remain to be solved in this area and, as yet, there is not in existence, a fully operational system that will permit the verification of large populations of individuals solely from analysis of their voice samples. Worse yet, most speaker verification schemes rely on traditional signal analysis techniques; in turn, these approaches require high quality transmissions. Thus, if noise or distortion are present in the signal, the power of most speaker verification methods in seriously impaired.

Speaker Identification. Of the three problems cited, the most difficult one to solve is that of an unknown speaker's identity -- especially when he is talking in an environment that distorts the sample. The speech to be analyzed is not contemporary and the talker is usually uncooperative. He may attempt voice disguise or suffer from a number of intrusive conditions - i.e., the varying effects of health, ingested drugs, emotional states (especially fear or stress) and so on. System distortions (limited passband, harmonic distortion) and noise (intermittent, continuous, spike, broad-band, etc.) also can interfere with attempts to establish the identity of a talker. Worse yet, the identification task always involves "open sets", i.e., where the unknown may or may not be among the suspect/subject pool. This particular problem is quite serious because one member of any group always will be more like the unknown talker than will any of the others -- whether he actually is the "unknown" or not. Hence, the decision criteria utilized in speaker identification are of critical importance. Finally, the uses are many for a system which can be employed to identify an individual

from his voice. Who among the pilots or astronauts is the individual who spoke: can the person on the telephone be identified; was the individual who made the threats actually the one who committed the crime? Yet no fully developed speaker identification systems currently are available. Even the proponents of the so-called "voiceprint" technique are beginning to recognize its nearly total lack of validity. Further, while where are a few systems at various stages of development (including the one reviewed in this paper), none of the scientists involved are willing to give their approaches unqualified endorsements for all speakers and all conditions. Thus, while the need for an efficient approach here is substantial, no truly robust method is as yet on-line. Of the three problems cited above, it is quite possible that it is this third one which will be the most difficult to solve. Yet the consequences of a reasonable solution are of inestimable importance -- and to all three issues/areas.

Since this course is one in crime countermeasures, it is the third of these areas that is of importance to us. Hence, it will be the only one reviewed. There have been three general approaches to the problem/issue of speaker identification; they are, 1) aural/perceptual approaches, 2) the so called "voiceprint" method of subjective spectrum matching and 3) machine/computer aided techniques. They will be considered in turn.

AURAL/PERCEPTUAL APPROACHES TO SPEAKER IDENTIFICATION

The perceptual approaches to speaker identification can be

divided roughly into two areas: 1) their use in courts and by law enforcement agencies and 2) investigation of their nature by experimental research.

Use by Courts/Police

In reality at least primitive attempts at voice recognition by ear probably antedate recorded history. Moreover, it is known that there were some relevant discussions about this issue in the English courts several hundred years ago. Indeed the admissibility of aural/perceptual testimony there may be traced back at least to the year 1660 when voice identification was offered in the case of one William Hulet. It since has been generally accepted in the courts of both in the United States and Britain. To be specific, Mack vs. State (1907) refers to a trial in which a hitherto unknown, unseen, cross-racial defendant was identified as a rapist by his spoken two sentences: "I have got you now", and "I don't want your money." The Court's decision is explained by a sort of innate, experiential logic as follows: "... The manner, time and place of his assault upon her threw her instantly into the highest state of terror and alarm, when all of her senses and faculties were at the extreme of alert receptiveness, when there was nothing within her reach by which to identify her assailant but his voice. Who can deny that under these circumstances that voice so indelibly and vividly photographed itself upon the sensitive plate of her memory as that she could forever afterwards promptly and unerringly recognize it on hearing its tones again ...". In any case, there is a long history of admissibility and nonadmissibility of aural/perceptual identification in the court of several countries, as some judges agree with this decision while

others do not. However, the present state of affairs is one of some confusion; currently most courts will permit a witness to testify providing he or she can satisfy the presiding judge that they <u>really</u> know the person they are identifying -- i.e., that they are very familiar with his or her voice and speech.

Decisions of this type have led law enforcement groups to attempt the conduct of "auditory lineups". However, their approach has been subject to criticism both by Brandt (1977) and Michel (1980). Basically, what the police do is replicate the typical eyewitness lineup. They will take an exemplar provided by the suspect and put it in with a series of 3-6 other exemplars (spoken by foils or controls). Presumably, the witness listens to the voices and picks out the "correct" one. Some police even attempt to conduct this process live. However, as Brandt and Michel suggest -- and we will stress -- the police often utilize talkers that sound quite different from the subject. In any event, it takes little imagination to see the many ways even the most wellmeaning police could err in a situation such as this one.

The question arises -- do listeners have to know the speakers in order to make highly accurate judgments of this type? In one relevant study, Hollien, et al (1982) attempted to (1) estimate listeners' capabilities in this area and (2) assess the importance of the auditors being acquainted with the talkers. Speakers for this research were 10 adult males who recorded speech samples under three types of speaking conditions: (a) normal, (b) stress (electric shock) and (c) disquise. Three classes of listeners were utilized (a) a group of individuals who knew the talkers very well, (b) a group that did not know the talkers but who were trained to identify them and

(c) a group that neither knew the talkers nor understood the language spoken. As may be seen from consideration of Figure 1, the analyses indicate that the performances among the groups were significantly different. People who knew the talkers did quite well; indivuduals who did not, did poorly.

Yet a second question can be asked: does it help in the identification process of the listener is a trained professional. Two studies are relevant here. First, Shirt (1984) compared a group of professional level Phoneticians, to university students with no particular experience in listening to speech. She did not find statistically significant differences between the two groups even though the Phoneticians as a group scored higher in correct identifications than did the students. She concluded that training help some, perhaps, but not enough. On the other hand, Koster (1981) functionally tested both of the previously cited studies. He reported on the ability of five Phoneticians and 30 untrained auditors to identify 10 adult male talkers who they all knew very well. Three experiments were carried out here. The first involved direct identification of the talkers on the basis of a spoken passage, the other two focused on the identification of either two (in a field of four) or four (in a field of eight) previously identified speakers. In no instance did a Phonetician make an error. The errors for the non professional ranged from 0%-33% with overall error rates from 3%-9%. If the data from these (several) investigations are pooled, we are able to conclude that the training Phoneticians receive results in better identification of (at least) known voices (i.e., training in this speciality area does make a difference) and if an individual is quite familiar with the voice of

a talker, high (correct) levels of identification can be expected, whereas only relatively low level identifications can be expected if an auditor does not know the person talking.

Yet a third question can be asked: What is the decay rate for aural/perceptual speaker identification. Two sets of studies are relevant here. First, McGehee carried out two experiments (1937, 1944) in which she had auditors listen to talkers and then identify them within a group of other speakers at various times subsequent to the exposure. All speech samples in the first study were "live"; hence, she had all talkers (the subject and the foils) speak from behind an opaque curtain; she used recorded samples in the second study (1944). In any case, McGehee found that identifications of familiar voices were relatively high and the process extinguished rather slowly but extinguish it did. Moreover, identifications of the voice of people unfamiliar to the listener were quite poor, so poor in fact that it was not possible to determine just how fast the identifications were extinguished. In this regard, Hollien, et al (1983) reported the results of an experiment in which they investigated aural perceptual identifications of a previously unknown individual from a set of photographic and tape-recorded exemplars following a simulated crime in a classroom attended by 61 law students. The procedures (four in number) involved foils, sound alikes (Rothman, 1977) and identifications over time. The results demonstrated the aural/perceptual identifications to be relatively poor. No strong trends for latencies were observed, either for repeated trials or for procedures involving different initiation latencies; nor did confidence levels appear to be related to accuracy of judgement. Finally, when a similar sounding foil was included in

the identification task, there was a weak trend for the foil to be chosen more often in subsequent trials. In short, ear witness identification appears to be a much poorer perceptual procedure than eye witness identification.

A final study focused directly on the stress effects on speaker identification. This question relates to the Mack vs. State -- i.e., can victims do better at perceptual speaker identification than people who are not the target of a criminal? In this regard, Arts (1981; also reported in Atwood and Hollien, 1986) completed a study where an attempt was made to discover if stress (or arousal) enhanced or degraded aural perceptual speaker identification. A large group of young females was screened for potential sensitivity to stressors. The 15 most susceptible and the 15 least likely to be affected by stress (controls) were selcted as subjects. The "stress" group was presented 10 minutes of violent video stimuli (attacks on women, rape scenes, death of children) while a male voice read a threatening commentary; the controls saw a pastoral video sequence while hearing a male voice read neutral material. A procedure involving speaker recognition (of the male voice over time) was carried out. The presence and level of stress experienced by subjects during the experiment was monitored by interpretation of the output of a standard polygraph. It was observed that aroused women were able to make slightly -- but statistically nonsignificant -- better identifications than did the women who were not stressed, and they sustained these better identification scores over time. In short, it appears that the ability of an individual to identify another by voice alone decays over time -- and these results support the opinion that most earwitness testimony should by viewed by judges and juries

with much greater caution than has been the case in the past. Perhaps the human ear is not quite as efficient in speaker identification as is suggested by Hecker (1971).

Basic Aural/Perceptual Research

A rather substantial amount of basic research has been carried out on the relationships that hold when a listener attempts aural/perceptual speaker identification. These experiments are quite useful and for two reasons. First, they permit a better understanding of the requisits for acceptable speaker recognition and, secondly, they provide useful clues for individuals who are carrying out R and D on machine/computer approaches to speaker verification and/or identification. However, only a brief review of that literature will be included in this paper. A more direct consideration of these articles, and the references they contain, should provide the interested reader with a relatively complete overview of what is known relative to this issue.

Perhaps it would be of interest to initiate this section with Bricker and Pruzansky (1966) who reported 98% correct identification of familiar speakers by listeners when sentences were provided as stimuli; identification accuracy fell to only 56%, however, when isolated vowel samples were substituted. Iles (1972) reports similar results. These studies appear to support the Pollack et al (1954) experiments with speech sample duration; they suggested that identification accuracy improves with increasing duration up to about 1200 ms; for longer periods, accuracy did not appear to be related to duration, but rather to phonemic repertoire. Other investigators

(Compton, 1963; Cort & Murry, 1971; LaRiviere, 1971) also have studied the effects of utterance duration on the identification task. In their case, the evidence again suggests that levels of correct speaker identification correlate to utterance duration only for very brief samples and longer utterances are important primarily because they provide listeners with a larger sample of a talker's speech. These investigators (as well as Stevens et al, 1968) also observed that listeners needed longer speech samples in order to permit correct identification of even known speakers when they degraded the speech signal by various means -- for example, by increasing the number of speakers, by substituting whispered for normal speech, when different speakers employing different speech materials were used (Carbonell et al, 1965; Stuntz, 1963; Williams, 1964; Stevens et al, 1968). And, of course, any type of signal degradation reduced identification accuracy.

Other relationships have been established also. For example: several authors report that speaker disguise, dialects, non-contemparary samples and large numbers of speakers reduce identification accuracy (Iles, 1972; Hollien et al, 1982; Stevens et al, 1968). Further, Rothman (1977) reports data about "sound-alikes" and non-contemporary speech samples. He found that when non-contemporary samples of the same speakers were played, listeners exhibited 58% error rates -- accuracy was at the same low level when the speaker's voice was paired with a similar sounding one. Worse yet, but little research has been carried out on the effects of emotion, speaker disguise and system distortion upon speaker identification (Carbonell et al, 1965; Endress, Bambach & Flosser, 1971; Hecker et al, 1968; Reich & Duke, 1979; Simonov & Frolov, 1973;

Williams & Stevens, 1972) and in only a few of these cases have attempts been made to relate the events specifically to aural/perceptual approaches. As will be seen later, knowledge of these relationships will be useful to the investigators attempting develop machine speaker identification procedures.

On the other hand, some of the research reported in this area has focused on rather positive relationships; that is, it is suggested that there <u>are</u> certain features within the speech signal that both can be identified and which appear as natural elements associated with the production of these organized acoustic sounds. That there are (speech) characteristics within human utterances that we can extract for identification purposes is very important -- primarily because it also may be possible to process these parameters by machine and develop an automatic or (preferably) semiautomatic identification method that will be both valid and efficient.

One of the first of these identification linked features is mean speaking fundamental frequency or SFF (Compton, 1963; Iles, 1972; LaRiviere, 1971) -- an acoustical event heard as the pitch and pitch variability of voice. A second includes vowel formant frequency levels, ratios and transitions (Iles, 1972; Meltzer & Lehiste, 1977; Stevens et al, 1968). There is little question but that these features provide important cues in the perceptual identification of speakers. As a matter of fact, LaRiviere (1975) attempted to compare the relative importance of source and vocal tract transfer characteristics for speaker identification and found that these features contribute additively. In addition, phonemic effects on the identificaiton task have been investigated. It has been reported that perceptual identifications appear to vary as a function of (1)

the vowel produced, (2) consonant-vowel transitions and (3) inflections. Thus, it can be seen that there are certain features that relate to, or support, the aural-perceptual speaker identification process. They can be inferred from the prior experiments and comments listed plus the direct relationships discussed in the immediately preceeding paragraphs.

THE PROBLEM OF VOICEPRINTS

Early in this decade, the proponents of "voiceprints" were seen to claim that their approach to speaker identification had been accepted by Courts-of-Law in 25 of the states within the U.S., by two U.S. military courts plus two courts in Canada (Lundgren, 1976; Tosi, 1981). How could this situation have occured in countries as technologyically advanced as the United States and Canada? Perhaps more alarming (if the proponents of "voiceprints" are to be believed) yet other courts -- plus those in other countries -- soon will accept this procedure. In short, the method appears to be spreading somewhat even in the face of numerous setbacks and a general disapproval by the relevant scientific community.

The problem appears to be threefold. First, is the intra- vs interspeaker variability which the "voiceprinters" appear not to have solved (especially for their technique); the second is their distortion of the scientific community (which they define as only themselves) and the third is their unwillingness to have their techniques and examiners investigated and/or evaluated. But why has the actual scientific community not solved this problem?

Stated simply, speaker identification is one of those applied

areas that bridges the Phonetic Sciences and Engineering. In the ordinary course of events, a dispute about an applied technique such as "voiceprints/grams" would result in a flurry of laboratory inquiry -- and resolution. Indeed, differences in scientific opinion of this type are quite common. One needs only to attend any Phonetic Sciences congress or a convention of the Acoustical Society of America to discover that, on any given day, numerous scientific controversies are presented, discussed and/or debated. In any case, there is no question but that differences of opinion are very common in the flow of scientific life. Unfortunately, the cited controversy is not a simple instance of scientific difference-of-opinion. In this case, the proponents of the technique are producing a "product," hence, they have a proprietary interest in it. Small wonder then that they have argued that the "relevant" scientific community agrees with them in that they only include those individuals who do so. Thus, they function pretty much in the manner of any business or perhaps even a as cultists -- wherein only the true believer can evaluate or criticize their art or activities. On the other hand, if they are <u>not</u> a cult, they (or someone) should test their methods. But, since "voiceprints/grams" essentially are a "product", the typical scientist finds the issue somewhat difficult to handle. It would appear that these relationships are among those which have tended to discourage a larger number of appropriate investigations in this area.

In any case, logic, poor results and the research to follow should have relegated this archaic method to the dustbin where it belongs. Yet, "voiceprint/grams" <u>still</u> are employed by a few law enforcement agencies -- and even the FBI (Koenig, 1979, 1986) -- in

investigations anyway; they also have been used as evidence in criminal and civil trials. The problem, of course, is that this is a serious societal issue and one of some urgency. We need to know if the "voiceprint/gram" approach to speaker identification is a valid one and we need to know it now. We cannot afford the luxury of decades of leisurely scientific inquiry, an approach which is suitable for nearly all of the other scientific issues -- but not for this one. In sum, the seeming lack of concern by the scientific community is not as reprehensible as one might suspect. Rather it is the unusual nature of this issue, and the acknowledged responsibility on the part of the "voiceprint" proponents to demonstrate the validity of their technique, that has led to inappropriate perspectives on the part of many scientists.

An additional concern would appear to relate functionally to the several cited above. In the early days of "voiceprinting", the proponents of this technique insisted that an individual's speech characteristics were both invariant and unique. They either ignored (or were unaware) of the rather substantial amount of research which would argue that the speech of a given talker is quite variable (see Hecker, 1971 and Nolan, 1983 for discussions on this issue). Nor did they appear concerned (when they referred to the idiosyncratic nature of speech behavior), that their technique had to account for this personal uniqueness (or lack of it) with respect to all of the billions of people who live in the world today. To be fair, as the elegant and intricate relationships between inter- and intra-speaker variability began to emerge, the position of the "voiceprint" proponents became somewhat more guarded. They now admit to the variability of speech, even though they will not concede to the

possibility that there may be individuals who could be confused with one another; they further insist (without details) that their process takes these problems into account. For example, they indicate that they only make definite identifications or eliminations in about 30-40% of the cases (Tosi, et al, 1972) but for other reasons. While it would seem that a process that admittedly does not work 60-70% of the time not a very good one, the "voiceprint" proponents are quite adamant in their opinion that this relationship somehow demonstrates that they are correct when they do make a decision.

What is a Voiceprint?

The process that has been referred to as "voiceprinting" has not been particularly well defined; it also appears to be one that tends to change over time. For example, from a longitudinal study of their testimony in the courts, the techniques they use, their opinions and so on tend to reveal a rather substantial (and continual) drift. It varies from Kersta's (no date) matching of 10 exact words to Truby's (1976) insistance that there can be no set rules.

Nevertheless, no matter what the definition, the core of this process has been, and still is, some sort of pattern-matching procedure of the configurations seen on time-frequency-amplitude (t-f-a) spectrograms -- a technique which is somewhat archaic -- at least in the light of modern-day technology. Unfortunately, the "voiceprint" enthusiasts apparently are not aware of -- or choose to ignore for the sake of their consumers -- the limitations of this process and the ways in which patterns produced by this device can be distorted. From time-to-time, they even have argued its infallibility (Crown vs Medvedew, 1976; Kersta, 1962; People

(California) vs Lawton, Gardener and Jackson, 1973; Truby, 1976).

As is well-known, t-f-a sound spectrography is based on a device by which relatively narrow (45 Hz) or wide (300 Hz) bandpass filters sweep the frequency range of a segment of speech (approximately 2.4 seconds in duration for commercial units of this type) and produce an analog record of the events processed (time on the horizontal axis, frequency on the vertical and the relative darkness of the markings constitute an estimate of intensity). Of the three dimensions, the first (time) is the most accurate. The second (frequency), however, tends to be somewhat distorted as it is represented by a linear rather than log scale (on the spectrogram). Moreover, most sound spectrograms used in "voiceprinting" utilize broadband filtering, a process which tends to remove (among other features) representation of the actual partials within the phonated speech wave. Instead, what is seen is a rough outline of energy concentrations. If vowels are taken as an example, the areas of resonance (or vowel formants as they are called) appear as black bars. Thus, energy concentrations are shown as outlines but the specific details of the acoustic wave (i.e., the actual partials) are lost. Of course, it is conceded that some useful features of the speech act can be observed and measured by this process but, in a very real sense, these configurations are artificial because energy is seen where it does not exist, and removed where it does.

Probably the greatest weakness of this particular type of sound spectrography relates to the third feature -- that of speech "intensity". Spectrographs of the t-f-a type provide little accurate information about the energy patterns of the speech sounds (even when "sectioned". Thus, as might be inferred from this review, it is

relatively easy to (accidently ?) modify the patterns seen on a particular spectrogram. As anyone who has made a number of these records will concede, problems such as changes in calibration, variation in amplitude (at any stage within the process), filtering of any type, noise, internal distortion and/or any background signal can markedly vary the patterns seen on a specific spectrogram. Finally, it should be noted that a second procedure was added to the overall approach during the 1970's. This additional task requires the "voiceprint examiner" to listen to the voice of the criminal and compare it to exemplars prepared by the suspect or suspects. Thus, a possible useful dimension has been added to the approach as it now includes judgments by the "examiner" as to whether or not the two voices sound similar or different. Even though they suggest that the process in important, neither the exact procedures they employ in this technique nor research fundamental to it have been reported by the "voiceprint" proponents. Moreover, the reader is cautioned to refer back to the discussion on aural/perceptual speaker identification for a reasonable perspective here. Also relevant are the hidden dangers in the aural-perceptual approach by a single listener and how these types of judgements must be structured if they are to be valid.

Research on Voiceprints

Research by the Proponents. As with the marketing of any product, it is incumbent for the relevant business to demonstrate that its clains are valid. The "voiceprint/gram" proponents should do the same. So far they have only reported 4-5 studies. The first,

and most important was that by Tosi et al (1972). This research is a little difficult to follow as it consists of a number of laboratory sub-studies combined into a relatively large project. Moreover, some of the experimental conditions varied over the investigational period (for example, there appeared to by a mid-project reduction in both the number of "examiners" and the number of words used in the matches).

Basically, Tosi studied talker populations of between ten and forty individuals (drawn from a group of 250); his "examiners" consisted of between one and three individuals (drawn from a group of twenty-nine). Tosi claims that his 250 talkers represent a total population of 25,000 males and thus, gives the impression that a substantial population was evaluated when in reality, the groups he studied were of a size conventional for research of this type. Briefly, Tosi tried to identify the optinum number of words, utterences, recording conditions, contexts and speakers for the "voiceprint" approach, as well as the effect of closed/open trials and contemporary/noncontemporary utterances. He claims to have demonstrated a 99% correct hit-rate for his research. Yet his results were obtained under only the most optimum conditions -- and certainly are ones that bear little relationship to the forensic model. For example, just a shift to contemporary/noncontemporary matches introduced a 18% error to his approach.

Few other studies have been published by the "voiceprint" proponents -- although Smrkoviski (1975) claims to have contrasted his speech with that of his twin brother (he says he could tell them apart). Hall (1975) studied Rich Little mimicking six male celebrities (none of them cooperated however) and, while he did not

use "voiceprints", he (incredibly) concludes that they are useful. Finally, Hennessey (1970) studied "voiceprints" in a business environment. He used two examiners and a variety of talkers (some Aisan) and reports 30-41% errors. None-the-less, he lauds the technique. Thus, because Tosi's study is laboratory limited and the others have very high error rates, it can only be concluded that the voiceprint proponents provide neither data on the validity or on the reliability of their method. However, others also have studied this issue.

Relevant Research on "Voiceprints". As might be expected, research in this area also has been carried out by other individuals and a substantial number of investigations can be cited -- especially by investigators who have studied variables that were as relevant, and often even more relevant, to the forensic model than were Tosi's. In an important study, Stevens, et al, (1968) compared the ability of subjects to make speaker identifications spectrographically and by the aural/perceptual method. In carrying out this research, they found that error rates resulting from spectrographic examinations ranged from 21% to 47%. They also found that subjects consistently achieved lower error rates when identifying speakers on the basis of the aural/perceptual method. Young and Campbell (1967) antedated Tosi in the testing of Kersta's claims; they reported far greater error rates than did either Kersta or Tosi. Hazen (1973) also studied the process utilizing both closed and open sets as well as identifications from same and different contexts; his error rates were high also Hazen concluded that "spectral similarities due to intraspeaker consistency are not apparent enough to outweigh the similarities due to a different phonetic context." Obrecht (1975)

became curious about statements by Nash concerning the similarity of fingerprints and "voiceprints" and carried out a study in which he reports that examiners with experience in fingerprint analysis were no better at speaker identification than those who lacked such a background. Moreover, Endress, et al, (1971) have reported that spectrographic patterns and fundamental frequency vary substantially over time and with attempts at voice disguise and Hollien and McGlone (1976) and McGlone, et al (1977) agree. Indeed, they discovered that, when subjects disjuised their voices, very substantial changes occurred in f0 as well as in the spectrographic and temporal patterning of the speech. Another recent study serves to underscore the disguise problem; it is by one carried out to study effect of selected vocal disguises on spectrographic speaker identification. Reich, et al (1976) revealed that these conditions resulted in error rates varying from approximately 50% to nearly 78%; they also report error rates of 40% and greater when the voice was undisguised. Finally, Rothman (1975) who used highly skilled "examiners", reported an overall (correct) identification mean of 20% on sound-alikes. He obtained the best identification scores (39%) when his examiners compared the same -- but non-contemporary -- phrase; for a contigous/contemporary phrase, the mean correct identifications were 24% and for contiguous/non-contemporary phrases, he obtained mean scores of only a little over 6%.

It is interesting to note that, in none of the investigations cited above, were the "examiners" able to achieve the very high levels of correct identification reported by Kersta and Tosi; indeed, no investigator has ever mustered the 99% correct identification levels Tosi and Kersta claim possible. Admittedly, in some

instances, the individuals used as "examiners" were not as highly trained for these tasks as the "voiceprint" proponents suggest is necessary. However, in practically all instances, the "examiners" were at least as skillful and well-trained as those utilized by Tosi; indeed, in other instances, they were extremely experienced and highly educated in both the Phonetic Sciences and in identification tasks. How, then, does one account for the extremely high levels of identification reported by Tosi (and Kersta) and the uniformly lower scores obtained by all other investigators? Unfortunately, this question must remain unanswered, at least at present.

The "Voiceprint Examiner"

Perhaps it is of limited interest to extensively review the problem of the "voiceprint examiner" -- primarily because 1) there are so few of them, 2) their training and apprenticeship are shrouded in mystery and 3) none of them ever has been objectively tested. Some reference about the requisites for such "examiners" and the processes by which they operate, have been suggested by Black, et al, (1973), Tosi, et al (1972), and Truby (1976). Perhaps these conditions are best iterated by Black, et al, (1973) who indicate that "voiceprint examiners" should:

a) Complete a two-year apprenticeship and academic training in Audiology and Speech Sciences.

b) Be entitled to five alternate decisions after each examination, namely: positive identifcation, positive elimination, probability of identification, probability of elimination and no opinion one way or the other.

c) Be entitled to use as much time and as many voice samples as

deemed necessary.

d) Be held responsible for the positive decisions reached after an examination.

Yet numerous questions can be directed at this simplistic description. Of the background and training: is training and/or experience in law enforcement necessary? If so, why, and, what are the minimum standards? What field experience is necessary? Moreover, is college training necessary, and why? What major/minors, degrees, levels should be required -- also what courses/labs are necessary? While these questions should be answered in detail, none have been provided. And what about the apprenticeship itself. For example, what is the exact length and nature of the "voiceprint/gram" training program? What are the prerequisites for this training and who teaches it? How is talent/progress assessed? What skills are necessary to graduate and how are they assessed? With respect to the internship itself: what activities does this two-year experience include? What are the specific goals and tasks involved? How is the apprentice supervised by the sponsor? Who are the sponsors? Are the "voiceprint/gram" related tasks consistent from apprentice to apprentice and/or are they standardized? How many of these tasks are there; what is the minimum proficiency level that the apprentice must achieve and how is the quality of his or her work assessed? Many, many other questions could be asked. Few answers have been provided!

Conclusions About "Voiceprints/Grams"

There is little question but that confusion exists relative to the nature and merit of the "voiceprint/gram" technique of speaker identification. The two major criticisms that can be leveled at it

are that: 1) insufficient research has been carried out on the method and, hence, it is impossible to determine whether or not it is a valid technique and 2) the training and competencies of the "voiceprint/gram examiners" are largely a mystery. Perhaps the results of the "computer aided" "voiceprint" project, that has been carried out over a rather long period of years in Los Angeles, will shed some light on the problem of pattern matching by spectrograms. If, it does, the comments above may have to be reevaluated. However, in the interim, it appears that the only hope for success in the speaker recognition area -- and especially relative to speaker identification -- appears to be that of machine recognition. That is, since aural/perceptual (human) approaches appear impractical (for extensive use in the field, anyway), the only reasonable solution to the problem would seem to be the development of some sort of human interactive or semiautomatic -- computer aided -- recognition procedure. An approach to this problem follows.

SPEAKER IDENTIFICATION BY MACHINE

As has been stated, speaker recognition consists of two parts: verification and identification. Of these subparts, nearly 90% of the research has been focused on verification. The work going on there (not just at the 3-4 sites listed above) is quite advanced; indeed, it can be considered near State-of-the-Science in its sophistication. Most of the approaches are based on high level signal analysis and there is every indication that some sort of successful (verification) operating system will become available in the near future -- probably in less than a decade. In any case, both the approaches being applied and the personnel involved are top

flight.

The issue being addressed by this paper, however, is one of speaker identification -- with all the distortions and problems cited above. There are of course, some individuals within the speaker verification area who venture to solve some of the problems (noise, distortion, stress, etc.) encountered in both forms of speaker recognition. Notable among this group are Koster at Trier University (West Germany) and Wolf at BB and N. However, most scientists and engineers in the verification area concentrate on the very formidable challenge they face there rather than wander into identification. Finally, there are a few -- a very few -- scientific groups who are concentrating their efforts on the speaker identification problem. They may be found, primarily, at our Institute and in the USSR and Poland; however, a strong program is being carried out at the West German Bundeskriminalamt under Kunzel and there are a few small programs elsewhere.

The Machine Approach at IASCP

Our response to the cited problem was to evaluate a number of acoustic and temporal parameters within the human speech signal in order to study the basic identificaiton problem (i.e., the relationship between intra- and interspeaker variability. We did so in the light of the potential (speaker/system) distortions that occur in the speaker identification milieu. While doing so, we discovered, as expected, that traditional approaches to signal processing were rendered functionally inoperable in the identification situation -- and also in the verification environment when similar distortions occurred. At this juncture, we shifted our focus and began the

investigation of a selected group of natural features, (Hollien, 1985; Hollien, et al, 1987; Yang, et al, 1986) within the speech signal which are thought to be potentially idiosyncratic of an individual speaker (see for example: Atal, 1972; Bricker and Pruzansky, 1966; Calinski, et al, 1970; Coleman, 1973; Compton, 1963; Fairbanks and Pronovost, 1939; Fairbanks and Hoaglin, 1941; Glenn and Kleiner, 1976; Goldstein, 1976; Hecker, 1971; Iles, 1972; Ingremann, 1968; Jassem, 1968; LaRiviere, 1975; Pollack, et al, 1954; Schwartz, 1968; Stevens, 1971). Test vectors were generated from this research and were evaluated singly and in combination: 1) in the laboratory (including simulated field conditions) and 2) in the field (attempts are made to "solve" simulated - but structured - crimes or security problems under operational conditions). Many experiments -- both successful and unsuccessful -- were carried out during the primary laboratory phase of the process. Most of our basic information has been generated by these studies. However, it is by the second process that our particular speaker identification system is being refined for operational use. As may be seen in Figure 2, the process described above is servomechanistic in nature. It provides for the continued evaluation of the vectors developed and the reanalysis of their robustness as they are up-graded. We believe that this approach - or variations of it (see Figure 3) - is/are very important in the proper development of a method for speaker identification. Given that it has not yet been shown (conclusively) that intraspeaker variability is less than is interspeaker variability in every case, the robustness of any approach must be demonstrated by its developers. Thus, this process (as seen in Figures 2 and 3) is the only one which will insure that appropraite experiments - and enough

of them - will be completed prior to operational use of a system; i.e., that the approach will be validated before it is used. The semiautomatic system that has resulted from efforts along these lines will be described below.

The Vectors Employed

The vectors that constitute the SAUSI approach have been chosen on the basis of: 1) high probability of discriminating among speakers, 2) enhanced utility when combined with other factors, 3) resistance to distortion, 4) availability and 5) compatability with computer processing. Those currently in use are as follows.

The Speaker Fundamental Frequency Vector (SFF). The perception of vocal pitch has been shown to be a cue for speaker recognition; however, to date, acoustic analysis of this speech feature has been a little marginal. We believe that our recent successes with this feature have resulted from the up-grading of the parameters we have used. That is, our current SFF vector is based on measures of central tendency and variability plus the frequency of occurence within semitone intervals. The SFF parameters now include: 1) SFFM, 2) SFFSD, 3) the number of semitone intervals containing energy and 4) the number of waves in each of 28 ST interval bins. SFF data is obtained by analysis of the speech signal via the IASCP Fundamental Frequency Indicator (FFI-8) coupled to our paired PDP-11/23 computers.

The Long-Term Speech Spectra Vector (LTS). Research results can be used to demonstrate that LTS will predict the identity of speakers at

very high levels (98-100%) of accuracy even for relatively large subject groups - at least in the laboratroy (Doherty, 1976; Furiu, 1978; Hollien and Majewski, 1977; Kosiel, 1973; Zalewski et al, 1975). We also have been able to demonstrate that LTS is resistant to the effects of speaker stress and limited passband conditions. The power spectra of speech/voice quite clearly provides good information about a person's general voice quality and such quality ordinarily is a stable identification cue. The approach we utilize provides 40 parameters for development of the LTS vector: they are generated by a Princeton Model 4512 FFT spectrum analyzer coupled to one of our 11/23 computers.

The Vowel Formant Tracking Vector (VFT). Much use has been made of vowel formant center frequencies, bandwidths and transitions by individuals using t-f-a sound spectrographic techniques ("voiceprints") for speaker identification. While their approach is not a very sophistricated one, the research completed suggests that vowel formant characteristics can be important to the identification task. The SAUSI VFT vector consists of an 48 parameter cluster made up of a number of center frequency and transition measures for each of the first two formants of four selected vowels (/i,a,ae,u/) within a test utterance. A high-speed Fourier analysis hybrid system currently is utilized with specific vowel formant frequency windows are preprogrammed so as to make this system operable. Experiments to date suggest that this vector is a robust one.

The Temporal Analysis Vector (TED). Only modest research in the speaker identification area has focused on any of the temporal

very high levels (98-100%) of accuracy even for relatively large subject groups - at least in the laboratroy (Doherty, 1976; Furiu, 1978; Hollien and Majewski, 1977; Kosiel, 1973; Zalewski et al, 1975). We also have been able to demonstrate that LTS is resistant to the effects of speaker stress and limited passband conditions. The power spectra of speech/voice quite clearly provides good information about a person's general voice quality and such quality ordinarily is a stable identification cue. The approach we utilize provides 40 parameters for development of the LTS vector: they are generated by a Princeton Model 4512 FFT spectrum analyzer coupled to one of our 11/23 computers.

The Vowel Formant Tracking Vector (VFT). Much use has been made of vowel formant center frequencies, bandwidths and transitions by individuals using t-f-a sound spectrographic techniques ("voiceprints") for speaker identification. While their approach is not a very sophistricated one, the research completed suggests that vowel formant characteristics can be important to the identification task. The SAUSI VFT vector consists of an 48 parameter cluster made up of a number of center frequency and transition measures for each of the first two formants of four selected vowels (/i,a,ae,u/) within a test utterance. A high-speed Fourier analysis hybrid system currently is utilized with specific vowel formant frequency windows are preprogrammed so as to make this system operable. Experiments to date suggest that this vector is a robust one.

The Temporal Analysis Vector (TED). Only modest research in the speaker identification area has focused on any of the temporal

parameters that can be extracted from the speech wave (see Johnson, et al, 1984). Nevertheless, proposody is an important identification cue; there is strong logic that there are many elements within this domain that can be identified, measured and utilized for recognition purposes. Our vector here is composed of several sets of temporal parameters that have resulted from our research; each set is based on: 1) the total time of the sample and 2) a series of data points obtained from the sample as it is sectioned into 10 equal levels. Thus, the TED vector is made up of several sets of parameters which include: (1) Total Speech Time (TST) - the period (in msec) it takes the speaker to utter a predetermined message; (2) Speaking Time Ratio (S/T) - a measure of the total time acoustic energy is present during a specific utterance: (3) Silent Interval (SI) - silent periods or pauses (in msec) within the utterance and (4) Speech Rate (SR) - the amount of speech material completed within a particular time frame. Each of the three TED features (TST is a base measure) are, in turn, made up of several parameter sets. That is, data for each are obtained at 10 interval levels (above a predetermined base) for the entire sample. Hence, there will be an S/T10, S/T20, S/T30 and so on. Data for this vector are obtained by use of a rectifier coupled to one of the PDP-11/23 A/D converters, plus processing software.

Experimental Approach

The Data-Base. Most of the SAUSI research utilizes a data-base we have established for this purpose at IASCP - it consists of over 1500 recordings of 357 speakers (males = 233; females = 124) variously producing 24 classes of utterances. Experimental samples include

(depending upon the subset) normal reading/speaking, digits, free/controlled disquise, telephone transmissions, varying dialects and induced stress (two types); moreover, any type of noise can be mixed with these recordings. While these are the experimental samples utilized in the basic testing of our vectors, samples for advanced testing are developed specifically for that particular experiment on drawn from a second data base of 105 male and 21 female voices obtained from actual cases (of several types; no identification of the actual talker is possible of course).

Procedures. The actual procedures utilized can be understood by reconsideration of Figures 2-3. As can be seen, the vectors all are eveluated singly and in all possible combinations first in the laboratory and then in the field. To be specific, the vectors first are evaluated alone in both laboratory discrimination and identification tasks utilizing relatively large subject populations and in the presence of both system (limited passband, noise, etc.) and talker (disguise, stress, etc.) distortions. To date, we have found that the levels of identification have closely approached 100% only for the LTS vector and for multiple vector analyses; however, the other vectors are beginning to provide very high identification levels also. There is now every indication that they can be used as a multiple-vector profile -- and the conditions under which each vector is robust are emerging. In any case, the experiments are being replicated on the basis of the profile concept. Additionally, the sensitivity of a variety of mathematical distances (Euclidean and Steinhaus among them) are being evaluated. The field experiments take a different form; they generally are of two types: military

related and law enforcement related. The military type field research is structured in an attempt to establish the identity of talkers when their spoken messages are received over standard communications gear and the received signal is mixed with "typical" noice (transport, tanks, aircraft and similar). Foils are 20-25 individuals including several "sound alikes". Finally, since we already have completed substantial research with "simu-crime" procedures in the law enforcement milieu (plus 11 actual - or "real life" - evaluations in the field), one of our early experiments will be described. In this instance, speech materials representing a series of "crimes" were generated by "unknown talkers" - i.e., male law enforcement agents simulating criminals. They extemporaneously produced the spoken material on the basis of their experience with the particular type of case; they then simulated speech materials for the (known) exemplars which were drawn from the text of the original call. A number of different "crimes" were simulated with the "knowns" and foils drawn from a group of 12-15 cooperating agents. For purposes of this research, the correct "unknown" always was included among the "knowns" (closed sets) and attempts were made to include (among the foils) controls who sounded like the "unknown" talker. All calls were made over a telephone circuit with the recordings made on a "typical" police type cassette tape recorder. The exemplars were recorded in a small interrogations room typical of those used in regular police work -- and by an individual acting as an investigator who obtained them (during the interview) over an open microphone coupled to the tape recorder. The true identity of the "criminals" was logged but not revealed until all analysis procedures were completed and the decisions made. Correct identifications

ranging from 70-90% were found and subsequent field experiments of this type have produced still better identifications (most close to or at 100%). The SAUSI procedure also provided accurate matches (or nonmatches) in the 11 "real life" trials but, of course, data of that type are quite subjective.

Research on SAUSI

It is not the purpose of this paper to review the 500 plus experiments we have carried out on our system (SAUSI or Semiautomatic Speaker Identification system). Rather, its characteristics have been outlined to illustrate what one approach to the speaker identification task might be like and to provide a very small amount of data to demonstrate the output of this type and how it can be used/evalated.

Moreover, it should be remembered that our approcah addresses the very severe limitations imposed upon the identification task by the forensic model (i.e., one referent; one test sample). Coupled to this rather harsh research design, we initialy chose to force matches (or non-matches) from the large field of (26) voices -- i.e., the known plus 25 foils (or controls) repeated for all subjects -- and to utilize the nearest neighbor statistical approach. In any case, many investigations were carried out with the signal degraded in numerous ways; and the vector changed, upgraded and/or improved. The experiments to follow should serve to illustrate this process.

An early experiment demonstrating the effect of combining the vectors (used at that time) into pairs is shown in Table 1. As would be expected, we were most interested in what would happen to the identification levels to LTS and SFF when they were directly combined

with each other and with other vectors. As can be seen by examination of the table, one of the results of this design is that sometimes the levels of correct identification are reduced by multiple vector processing. However, there appear to be reasonable explanations for this outcome. First, data found in the research literature has demonstrated again and again that, when vectors are merged on a simple basis, the number of parameters within these multiple vectors begin to exceed the diminishing returns rule. That is, the system moves onto the negative shope of its performance curve and this situation is only exacerbated by continual addition of parameters. Thus, instead of improving performance, the addition of new parameters induces confusions that reduce overall vector effectiveness. In any case, we now are aware that, as more vectors are combined, the total number of parameters will have to grow very slowly, be kept constant or, quite possibly, reduced -- and at what point these changes must take place. One solution is to systematically include and exclude various parameters within a given vector (and vector combination) and continue the process until the particular vector/parameter configuration is optimized. Another potential solution is to normalize the distance (Euclidean and Steinhaus) data and then combine these values mathematically and this is one of the several processes that currently we are stressing.

Two additional evaluations are provided in order to illustrate some of the more practical tests (and more recent ones) that have been carried out. In the first of these two cases (a fairly early one), the speech of a known talker (k) was contrasted to nine other individuals. Speaker U was believed to be K but the recording was made in the field and was of relatively poor quality. The eight

foils were drawn variously from field recordings and from our data-base (sound-alikes of K were sought). Four SAUSI vectors were applied singly and in all combinations. As can be seen in Table 2, U was selected as K in all cases except one - in that case, U was the third choice. When the statistical probability was calculated, the test indicated that there was a 87% chance that U was K, a 35% chance that F1 as K and (decreasing to chance levels) the other foils were K. It was concluded that SAUSI was able to identify the "suspect" (U) as the criminal (K). However, it was shown here that the INT vector (one based on analysis of the intensity of speech) was in need of restructuring. (It was replaced by VFT and currently is being revised).

The second example of a field evaluation (Table 3) involves an open set as the actual criminal was not known to be among the suspects (however, K <u>was</u> the prime suspect). The basic sample of the unknown (U) was derived from a 20 minute conversation he had over the telephone with a second person. Moreover, all speech was in a foreign language, and the principals used low, often soft, conspiretal voices. There were three exemplars of the prime suspect. The first (KI) was taken from the audio portion of a television tape of K giving a public address in a large hall. The second tape recording was made under circumstances more like the original telephone call (K2N) with the third recording (K2F) made from K2N by processing it through a telephone bandpass. Because there were several exemplars, only five foils (or controls) were utilized (all were native speakers of the language employed by U and K) -- with foil K4 especially selected as a person who sounded a great deal like the unknown. Three vectors were used: LTS, VFT and TED (the SFF

hardware was being repaired at the time of this experiment) and first U, and then K2F were compared with all other eight samples. All resulting distances were normalized and converted to functions or, or distances from, the target. As can be seen from the overall values appearing on Table 3, U, K2F and K1 all clustered around each other with only K2N a little marginal. None of the foils -- including K4 - were competitors. Soon after the report to this effect was submitted to the agency requesting it, it was learned that K had admitted making the phone call in question.

In summary, it must be remembered that, in the illustrative set of subprojects described, we have tested SAUSI under the most stringent of possible conditions. In one case with: 1) a relatively small (statistically anyway) population, 2) only one reference sample per subject, 3) a single test sample per subject and 4) noise and telephone bandpass distortions present. In the other (field) cases, a typical forensic model was utilized with the samples noisy, (telephone) bandpassed, noncontemporary, language independent and so on. Moreover, it must be remembered that it was only with the last of the two field evaluations that the (new) normalized distance procedure was utilized. Nevertheless, identification levels which, at worst, were many orders of magnitude above chance were obtained.

In short, substantial progress has been made in our semiautomatic speaker identification system; we expect inprovements to continue. Nonetheless, even though this (SAUSI) system is one of the leading approaches currently avaialble, it is not possible to state that there is any system presently in existence that is complete and operational.

ACKNOWLEDGEMENT

The author wishes to thank the United States Justice Department, the U.S. Army and the Dreyfus Fondation for their support of the several research programs described. I also wish to thank Drs. M.P. Gelfer, J.W. Hicks, Jr., P.A. Hollien, R. Huntley, L. Oliver and M. Yang for assistance with these project.

REFERENCES

Aarts, N.W. (1984) The Effects of Listener Stress on Perceptual Speaker Identification, Unpublished MA Thesis, University of Florida.

Atal, B.S. (1972) Automatic Speaker Recognition Based on Pitch Contours, J. Acoust. Soc. Amer., 52:1687-1697.

Atal, B.S. (1974) Effectiveness of Linear Prediction Characteristics of the Speech Wave for Automatic Speaker Identification and Verification, J. Acoust. Soc. Amer., 55:1304-1312.

Atwood, W. and Hollien, H. (1986) Stress Monitoring by Polygraph for Research Purposes, Polygraph 15:47-56.

Black, J.W., Lashbrook, W., Nash, W., Oyer, H.J., Pedrey, C., Tosi, O.I. and Truby, H. (1973) Reply to Speaker Identification by Speech Spectrograms: Some Further Observations, J. Acoust. Soc. Amer., 54:535-537.

Bricker, P.D., Gnanadesikan, R., Mathews, M.V., Pruzansky, S., Tukey P.A., Wachter, K.W. and Warner, J.L. (1971) Statistical Techniques for Talker Identification, The Bell System Technical Journal, 50:1427-1450.

Bricker, P.D. and Pruzansky, S. (1966) Effects of Stimulus Content and Duration on Talker Identification, J. Acoust. Soc. Amer., 40:1441-1450.

Calinski, T., Jassem, W. and Kaczmarck, Z.(1970) Investigation of Vowel Formant Frequencies as Personal Voice Characteristics by Means of Multivariate Analysis of Variance, in Speech Analysis and Synthesis, (W. Jassem, Ed.), Warsaw, Poland 2:7-40.

Carbonell, J.R., Stevens, K.N., Williams, C.E. and Woods, B. (1965) Speaker Identification by a Matching-From-Samples Technique, J. Acoust. Soc. Amer., 40:1205-1206.

Coleman, R.O. (1973) Speaker Identification in the Absence of Intersubject Differences in Glottal Source Characteristics, J. Acoust. Soc. Amer., 53: 1741-1743.

Compton, A.J. (1963) Effects of Filtering and Vocal Duration Upon the Identification of Speakers Aurally, J. Acoust. Soc. Amer., 35:1748-1752.

Cort, S. and Murry, T. (1972) Aural Identification of Children's Voices, J. Acoust. Soc. Amer., 51:131(A).

Crown vs Medvedew (1976) Provincial Judges Court (Criminal Division) Brandon, Manitoba, Canada (transcript of testimony).

Das, S.K. and Mohn, W.S. (1971) A Scheme for Speech Processing in Automatic Speaker Verification, IEEE Trans. Audio. Electroacoust., AU-19:32-43.

Doddington, G.R. (1974) A Method of Speaker Verification, Ph.D. Dissertation, University of Wisconsin.

Doddington, G.R. (1974) A New Method of Speaker Verification, J. Acoust. Soc. Amer., 49:139(A).

Doddington, G.R. (1974) Speaker Verification, Technical Report RADC-TR-UI-963700-F, Rome Air Develop. Ctr., Griffiss AFB, New York.

Doddington, G.R. (1980) Whither Speech Recognition?, in Trends in Speech Recognition, Prentice-Hall, Inc., Englewood Cliffs, NJ, 556-561.

Doddington, G.R., Hyrick, B. and Beek, B. (1974) Some Results on Speaker Verification Using Amplitude Spectra, J. Acoust. Soc. Amer., 55:463(A).

Doherty, E.T. (1976) An Evaluation of Selected Acoustic Parameters for Use in Speaker Identification, J. Phonetics, 4:321-326.

Endress, W., Bambach, W. and Flossler, G. (1971) Voice Spectrograms as a Function of Age, Voice Disguise and Voice Imitation, J. Acoust. Soc. Amer., 49:1842-1848.

Fairbanks, G. and Hoaglin, L.W. (1941) An Experimental Study of the Durational Characteristics of the Voice During the Expression of Emotion, Speech Mono., 8:85-90.

Fairbanks, G. and Pronovost, W. (1939) An Experimental Study of the Pitch Characteristics of the Voice During the Expression of Emotion, Speech Momo., 6:87-104.

Floyd, W. (1964) Voice Identification Techniques, Report RADC-TDR-64-312, Rome Air Develop. Ctr., Griffiss AFB, New York.

Furui, S. (1978) Effects of Long-Term Spectral Variability on Speaker Recognition, J. Acoust. Soc. Amer., 64:S183.

Furui, S. (1981) Cepstral Analysis Technique for Speaker Verification, IEEE Trans. ASSP, ASSP-29:254-272.

Glenn, J.W. and Kleiner, N. (1976) Speaker Identification Based on Nasal Phonation, JASA, 43:368-372.

Goldstein, U.G. (1976) Speaker-Identifying Features Based on Formant Tracks, J. Acoust. Soc. Amer., 59:176-182.

Hall, M. (1975) Spectrographic Analysis of Interspeaker and Intraspeaker Variabilities of Professional Mimicry, MA Thesis, Michigan State University.

Hazen, B.M. (1973) Effects of Differing Phonetic Contexts on Spectrographic Speaker Identification, J. Acoust. Soc. Amer., 54:650-660.

Hecker, M.H.L., Stevens, K.N., von Bismarck, G. and Williams, C.E. (1968) Manifestations of Task-Induced Stress in the Acoustic Speech?????

Hecker, M.H.L. (1971) Speaker Recognition: An Interpretive Survey of the Literature, Am. Speech Hear. Assoc. Mono., 16.

Hennessy, J.J. (1970) An Analog of Voiceprint Identification, MA Thesis, Michigan State University.

Hollien, H. (1985) Natural Speech Vectors in Speaker Identification, Proc., Speech Tech. '85, New York, Media Dimensions Inc. 331-334.

Hollien, H., Bennett, G.T. and Gelfer, M.P. (1983) Criminal Identification Comparison: Aural vs. Visual Identification Resulting from a Simulated Crime, J. Forensic Sciences, 28:208-221.

Hollien, H., Childers, D.G. and Doherty, E.T. (1977) Semi-Automatic Speaker Identification System (SAUSI), Proceedings, IEEE International Conference on Acoustics, Speech and Signal Processing, 768-771.

Hollien, H., Gelfer, M.P. and Huntley, R. (1987) The Use of Natural Speech Vectors in Speaker Identification, in Neue Tend. Angewandten Phon. III, (V. A. Borowski and V-P. Koster, Eds.), Hamburg, Buske A6.

Hollien, H. and McGlone, R.E. (1976) An Evaluation of the "Voiceprint" Technique of Speaker Recognition, Proceedings, Carnahan Conference on Crime Countermeasures, 30-45, 1976; reprinted in Nat. J. Crim. Def., 2, 117-130, 1976 and in Course Handbook, The Instit. Contin. Legal Ed., Ann Arbor, Michigan, 391-404.

Hollien, H. and Majewski, W. (1977) Speaker Identification by Long-Term Spectra Under Normal and Distorted Speech Conditions, J. Acoust. Soc. Amer., 62:975-980.

Hollien, H., Majewski, W. and Doherty, E.T. (1982) Perceptual Identification of Voices Under Normal, Stress and Disguised Speaking Conditions, J. Phonetics, 10:139-148.

lles, M. (1972) Speaker Identification as a Function of Fundamental Frequency and Resonant Frequencies, Ph.D. Dissertation, University of Florida.

Ingemann, F. (1968) Identification of the Speaker's Sex from Voiceless Fricatives, J. Acoust. Soc. Amer., 44:1142-1144.

Jassem, W. (1968) Formant Frequencies as Cues to Speaker Discrimination, in Speech Analysis and Synthesis, (W. Jassem, Ed.) Warsaw, 1:9-41.

Johnson, C.C., Hollien, H. and Hicks, J.W. (1984) Speaker Identification Utilizing Selected Temporal Speech Features, J. Phonetics, 12:319-327.

Kersta, L.G., Instruction Manual/Procedure for Voiceprint Examinations (with acknowledgment to F. H. East), Voiceprint Lab., Somerville, New Jersey.

Kersta, L.G. (1962) Voiceprint Identification, Nature, 196:1253-1257.

Koenig, B. (1980) Speaker Identification (Part I), FBI Law Enforcement Bulletin, 49:1-4.

Koenig, B. (1986) Spectrographic Voice Identification: A Forensic Survey, Letter to the Editor, J. Acoust. Soc. Amer., 79:2088-2090.

Kosiel, U. (1973) Statistical Analysis of Speaker-Dependent Differences in the Long-Term Average Spectrum of Polish Speech, in: Speech Analysis and Synthesis, (W. Jassem, Ed.), Warsaw, 3:180-208.

Koster, J.-P. (1981) Auditive Sprechererkennung bei Experten und Naiven, in Festschrift Wangler, 52:171-180.

LaRiviere, C.L. (1971) Some Acoustic and Perceptual Correlates of Speaker Identification, Ph.D. Dissertation, University of Florida.

LaRiviere, C.L. (1974) Speaker Identification from Turbulent Portions of Fricatives, Phonetica, 29:246-252.

LaRiviere, C.L. (1975) Contributions of Fundamental Frequency and Formant Frequencies to Speaker Identification, Phonetica, 31:185-197.

Li, K.P., Dammann, J.E. and Chapman, W.D. (1966) Experimental Studies in Speaker Verification Using an Adaptive System, J. Acoust. Soc. Amer., 40:966-978.

Luck, J.E. (1969) Automatic Speaker Verification Using Cepstral Measurements, J. Acoust. Soc. Amer., 46:1026-1032.

Lundgren, F.A. (1976) Message From the President, International Association of Voice Identification, undated but presumably late 1976.

Mac vs. State, 54 Fla., 55, 44 So. 706 (1907, citing 5 Howell's State Trials 1186.

Majewski, W., Basztura, C. and Hollien, H. (1976) Speaker Identification by Means of Short-term Analysis of Zero Crossings of the Speech Wave, Materially XXIII Otwartega Seminarium Z Akusty Ki, WISLA Wrzesien, 225-226.

Makhoul, J. and Wolf, J. (1973) The Use of a Two-Pole Linear Prediction Model in Speech Recognition, Bolt, Beranek and Newman Report No. 2537, 1-21.

McGehee, F. (1937) The Reliability of the Identification of the Human Voice, J. Gen. Psychol., 17:249-271.

McGehee, F. (1944) An Experimental Study in Voice Recognition, J. Gen. Psychol., 31:53-65.

McGlone, R.E., Hollien, P.A. and Hollien, H. (1977) Acoustic Analysis of Voice Disguise Related to Voice Identification, Proceed., Intern. Conf. on Crime Countermeasures, Oxford, England, (July 25-29).

Meltzer, D. and Lehiste, I. (1972) Vowel and Speaker Identification in Natural and Synthetic Speech, J. Acoust. Soc. Amer., 51:S131.

Michel, J.F. (1980) Use of a Voice Lineup, Convention Abstracts, American Academy of Forensic Sciences, 937.

Nolan, J.F. (1983) The Phonetic Basis of Speaker Recognition, Cambridge, UK University Press.

Obrecht, D.H. (1975) Fingerprints and Voiceprint Identification, Proceedings, Eighth International Congress of Phonetic Sciences, Leeds, in press.

People (California) vs Lawton, Gardener and Jackson (1973) Superior Court, Riverside County, Case No. Cr. 9138, (transcript of testimony).

Pollack, I., Pickett, J.M. and Sumby, W.H. (1954) On the Identification of Speakers by Voice, J. Acoust. Soc. Amer., 26:403-412.

Pruzansky, S. (1963) Pattern Matching Procedure for Automatic Talker Recognition, J. Acoust. Soc. Amer., 35:354-358.

Pruzansky, S. and Mathews, M.V. (1964) Talker Recognition Procedure Based on Analysis of Variance, J. Acoust. Soc. Amer., 36:2041-2047.

Reich, A.R. and Duke, J.E. (1979) Effects of Selected Vocal Disguise Upon Speaker Identification by Listening, J. Acoust. Soc. Amer., 66:1023.

Reich, A.R., Moll, K.L. and Curtis, J.F. (1976) Effects of Selected Vocal Disguises Upon Spectrographic Speaker Identification, J. Acoust. Soc. Amer., 60:919-925.

Rosenberg, A.E. (1973) Listener Performance in Speaker Verification Tasks, IEEE Trans, Audio. Electroacoust., AU-21:221-225.

Rosenberg, A.E. and Sambur, M.R. (1975) New Techniques for Automatic Speaker Verification, IEEE Trans. ASSP, ASSP-23:169-176.

Rothman, H.B. (1975) Perceptual (Aural) and Spectrographic Investigation of Speaker Homogeneity, J. Acoust. Soc. Amer., 58:S107(A).

Rothman, H.B. (1977) A Perceptual (Aural) and Spectrographic Identification of Talkers with Similar Sounding Voices, Proc.,Inter. Conf. Crime Countermeasurers, Oxford, England, 37-42.

Sambur, M.R. (1973) Speaker Recognition and Verification Using Linear Prediction Analysis, QPR No. 108, MIT, 261-268.

Sambur, M.R. (1975) Selection of Acoustic Features for Speaker Identification, IEEE Trans. Acoustics, Speech and Signal Process., ASSP-23:176-192.

Sambur, M.R. (1976) Text Independent Speaker Recognition Using Orthogonal Linear Prediction, Proceedings, IEEE Conf. Acoustics, Speech and Signal Process., 727-729.

Schafer, R.W. and Rabiner, L.R. (1970) System for Automatic Formant Analysis of Voiced Speech, JASA, 47:634-648.

Schwartz, M.F. (1969) Identification of Speaker Sex From Isolated Voiceless Fricatives, J. Acoust. Soc. Amer., 43:1178-1179.

Shirt, M. (1983) Effect of Phonetics Training on Speaker Identification By Ear, paper presented at joint ISPhS-ICPhS Meeting on Speaker Identification, August, Utrecht, The Netherlands.

Shirt, M. (1984) An Auditory Speaker Recognition Experiment, Proceed., 1st Conf. Police Appl. Speech, Tape Record. Analysis, IOC, London, 71-74.

Smrkovski, L.L. (1975) Collaborative Study of Speaker Identification by the Voiceprint Method, Journal of the AOAC, 48:453-456.

Stevens, K.N. (1971) Sources of Inter- and Intra-Speaker Variability in the Acoustic Properties of Speech Sounds, Proceedings of the Seventh International Congress of Phonetic Sciences, Montreal, 206-232.

Stevens, K.N., Williams, C.E., Carbonnell, J.R. and Woods, D. (1968) Speaker Authentication and Identification: A Comparison of Spectrographic and Auditory Presentation of Speech Materials, J. Acoust. Soc. Amer., 44:1596-1607.

Stuntz, A.E. (1963) Speech Intelligibility and Talker Recognition Tests of Air Force Communication Systems, Report ESD-TDR-63-224, Air Force Systems Command, Hanscom Field.

Tosi, O. (1979) Voice Identification: Theory and Legal Applications, Baltimore, University Park Press.

Tosi, O., Oyer, H.J., Lashbrook, W., Pedrey, C., Nichol, J. and Nash, W. (1972) Experiment on Voice Identification, J. Acoust. Soc. Amer., 51:2030-2043.

Truby, H.M. (1976) "Voiceprinting" A Critical Review Brief presented to California Supreme Court (re: People vs Kelly) on behalf of the International Association of Voice Identification, 1-44.

Williams, C.E. (1964) The Effects of Selected Factors on the Aural Identification of Speakers, Tech. Doc. Opt. ESD-TDR-65-153, Electron. Syst. Div., USAF, Hanscom Field.

Williams, C.E. and Stevens, K.N. (1972) Emotions and Speech: Some Acoustical Correlates, J. Acoust. Soc. Amer., 52:1238-1250.

Wolf, J.J. (1972) Efficient Acoustic Parameters for Speaker Recognition, J. Acoust. Soc. Amer., 51:2044-2055.

Wolf, J.J., Krasner, M., Karnofsky, K., Schwartz, R. and Roucos, S. (1983) Further Investigations of Probabilistic Methods for Text-Independent Speaker Identification, IEEE ICASSP, Boston, MA, 2:551-554, (April).

Yang, M.C.K., Hollien, H. and Huntley, R. (1986) A Speaker Identification System for Field Use, Speech Tech-86, New York, Media Dimensions, Pub., 277-280.

Young, M.A. and Campbell, R.A. (1967) Effects of Context on Talker Identification, J. Acoust. Soc. Amer., 42:1250-1254.

Zalewski, J., Majewski, W. and Hollien, H. (1975) Cross-Correlation Between Long-Term Speech Spectra as a Criterion for Speaker Identification, Acustica, 34:20-24.

Table 1. Percent correct classification when individual vectors are combined into multiple vectors.

Condition	Males			Females		
Vector	1	2	3	1	2	3
Normal/Normal						
SFF/LTS	38	54	65	23	35	46
INT/LTS	46	54	58	38	50	62
TED/LTS	15	19	27	12	27	27
SFF/INT	31	42	42	19	19	27
SFF/TED	15	19	31	11	23	23
INT/TED	15	19	23	11	23	23
Noise/Normal						
SFF/LTS	15	27	31	42	50	62
INT/LTS	15	23	27	35	46	59
TED/LTS	23	31	46	15	27	31
SFF/INT	23	38	54	35	46	58
SFF/TED	15	27	42	15	27	35
INT/TED	15	31	38	11	27	27
Bandpass/Normal						
SFF/LTS	4	8	12	4	8	19
INT/LTS	8	12	15	0	8	15
TED/LTS	4	12	19	4	4	15
SFF/INT	4	8	12	8	8	15
SFF/TED	4	11	19	4	11	15
INT/TED	4	8	19	4	4	15
Noise/Noise						
SFF/LTS	42	69	81	31	35	42
INT/LTS	46	58	65	31	46	58
TED/LTS	15	15	23	15	19	19
SFF/INT	27	54	62	19	31	35
SFF/TED	15	19	27	8	19	19
INT/TED	15	31	39	4	19	19
Bandpass/Bandpass						
SFF/LTS	35	65	73	73	73	85
INT/LTS	23	27	35	19	31	42
TED/LTS	12	23	42	15	31	38
SFF/INT	39	62	73	35	39	58
SFF/TED	19	35	35	19	31	35
INT/TED	11	27	31	15	27	35

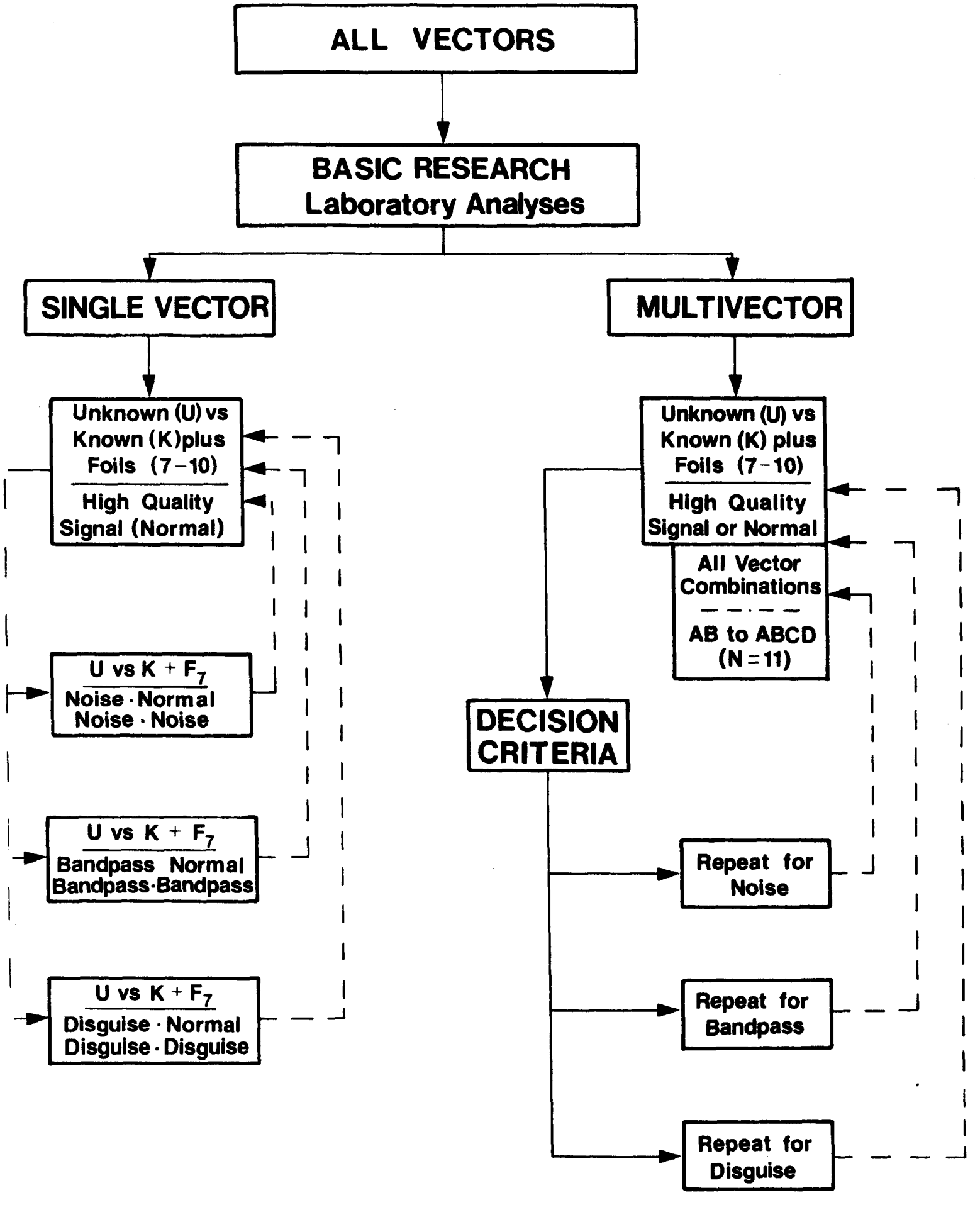
Table 2. A field test of four early SAUSI vectors by the three nearest neighbor ranking procedure. A known talker was contrasted to that talker in the field (U) plus eight foils (F).

VECTOR	SPEAKER								
	U	F1	F2	F3	F4	F5	F6	F7	F8
SFF	1	—	2	—	—	3	—	—	—
LTS	1	3	2	—	—	—	—	—	—
TED	1	—	—	2	—	3	—	—	—
INT	3	—	—	2	1	—	—	—	—
SFF/LTS	1	3	2	—	—	—	—	—	—
SFF/TED	1	—	—	2	—	3	—	—	—
SFF/INT	1	—	2	—	—	3	—	—	—
LTS/TED	1	—	—	—	3	2	—	—	—
LTS/INT	1	3	2	—	—	—	—	—	—
TED/INT	1	—	—	2	3	—	—	—	—
SFF/LTS/TED	1	—	—	—	3	2	—	—	—
SFF/LTS/INT	1	3	2	—	—	—	—	—	—
SFF/TED/INT	1	—	—	2	—	3	—	—	—
LTS/TED/INT	1	—	—	—	3	2	—	—	—
ALL VECTORS	1	—	—	—	3	2	—	—	—
% probability subject is K	87	C	28	23	23	35	C	C	C

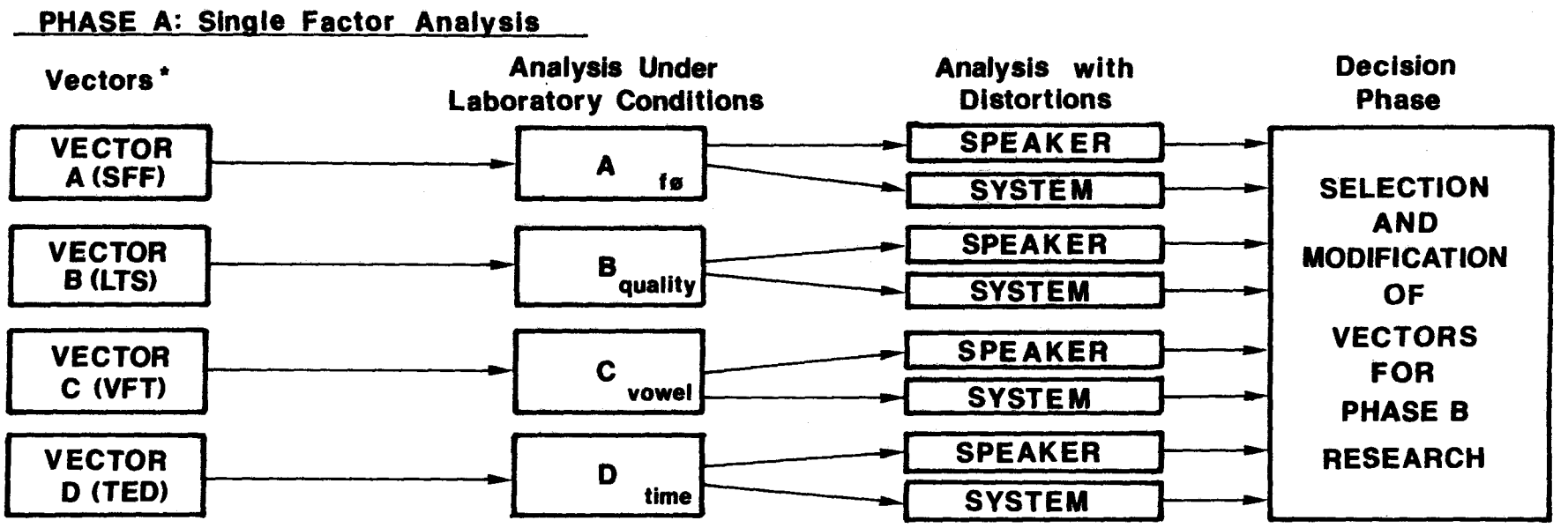
(C = chance or near chance)

Table 3. Summary table of normalized distances based on the closet match when the unknown talker is compared to himself, the knowns and foils (controls) — and when K2F is contrasted to the other individuals in a like manner. Three vectors were employed; all values are distances from the closest match.

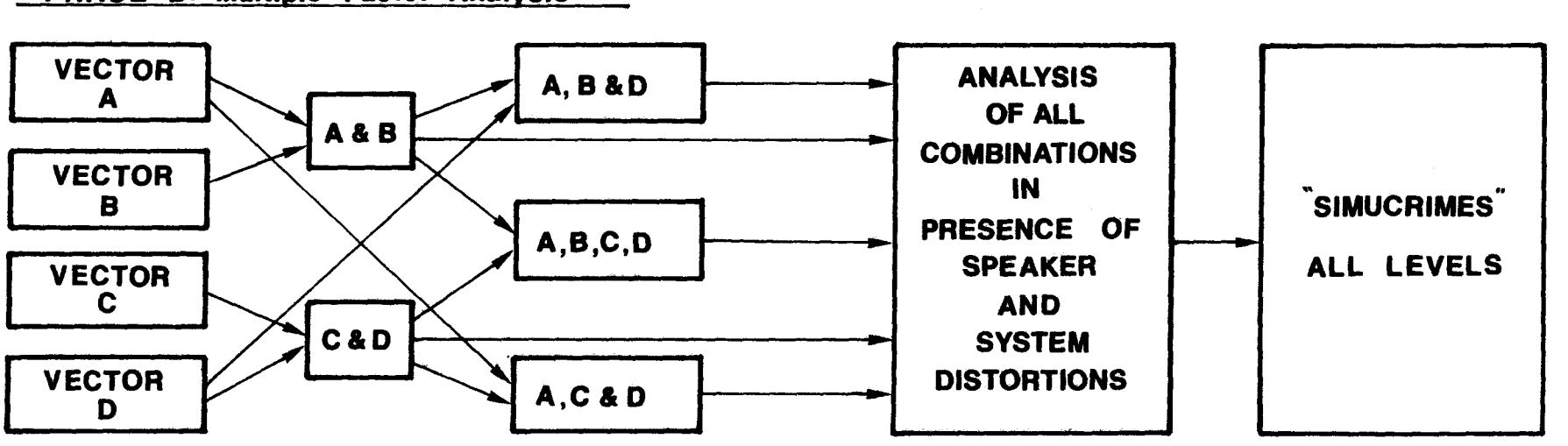
Test/Vector	U	K2F	K2N	K-1	F1	F2	F3	F4	F5
Unknown									
LTS	0.127	—	0.116	0.649	1.559	1.973	1.487	1.468	3.214
TED	--	0.005	0.032	0.008	0.014	0.011	0.012	0.010	0.014
VFT	0.216	1.173	0.216	0.628	2.174	0.216	—	2.628	0.381
TOTAL	0.343	1.178	0.364	1.285	3.747	2.200	1.499	4.106	3.609
K2F									
LTS	0.547	—	1.897	0.494	2.138	2.487	1.632	1.202	3.286
TED	--	0.002	0.020	0.006	0.011	0.008	0.009	0.008	0.011
VFT	2.146	—	2.146	1.303	0.001	2.146	2.622	0.214	0.535
TOTAL	2.693	0.002	4.063	1.803	2.150	4.641	4.263	1.424	3.832
Overall									
Distance	3.036	1.180	4.427	3.088	5.897	6.841	5.762	5.530	7.441
Rank	2	1	4	3	7	8	6	5	9


ALL VECTORS
BASIC RESEARCH
Laboratory Analyses
SINGLE VECTOR
MULTIVECTOR
Unknown (U) vs Known (K) plus Foils (7–10)
High Quality Signal (Normal)
U vs K + F7
Noise · Normal
Noise · Noise
U vs K + F7
Bandpass Normal
Bandpass · Bandpass
U vs K + F7
Disguise · Normal
Disguise · Disguise
Unknown (U) vs Known (K) plus Foils (7–10)
High Quality Signal or Normal
All Vector Combinations
AB to ABCD
(N = 11)
DECISION CRITERIA
Repeat for Noise
Repeat for Bandpass
Repeat for Disguise

Summary of Approach to the Problem



* Plus others



** Illustrative only as each vector will be studied in all possible combinations.

DNA Technology and DNA Fingerprinting in Forensic Science

By

R.E. Williams[1+], G.G. Shutler and R.G. Korneluk[3]

[1]Division of Biological Sciences
National Research Council of Canada
100 Sussex Drive
Ottawa, Ontario, Canada
K1A 0R6

[2]Central Forensic Laboratory
R.C.M.P.
P.O. Box 8885
Ottawa, Ontario, Canada
K1G 3M8

[3]Division of Genetics
Childrens Hospital of Eastern Ontario
401 Smyth Road
Ottawa, Ontario, Canada
K1H 8L1

[+] To whom correspondence may be addressed.

A. Introduction

In the early 1950's a minor revolution occurred in biology. A structure for DNA (deoxyribonucleic acid) was described which accounted for many of the then-known properties of DNA (1). An accompanying set of hypotheses called the central dogma was also ennunciated (1-3). In it the concept of DNA transcription to RNA and thence translation into protein was proposed. The concept implied that one gene would give rise to one enzyme. This was subsequently modified to encompass all proteins and thus the one gene-one protein concept was born. The ensuing years have seen a vast increase in mankind's knowledge of the structure of DNA, its conformational behaviour, its biosynthesis (synthesis, replication and processing) and its role in forming the genetic basis of many species, including humans.

At the technological level many of the advances made in the understanding of DNA have only been possible through the use of procedures which employ highly radioactive DNA fragments. The fragments are usually made radioactive by incorporation of the β-emitter ^{32}P atom into the sugar-phosphate backbone of the DNA polymer. The availability of these highly radioactive fragments has meant that it has become possible to search for and locate specific genes occurring in the genomes of many different species. This development has also meant that, where the identification of biological specimens previously relied on the presence, absence or variances of the proteins or

carbohydrates in the sample, it has become possible to locate the gene from which the proteins or carbohydrates arose. In principle, it is possible to go through a genome, gene by gene, and determine the genetic make- up of the DNA of the particular organism under investigation.

To give some idea of the degree of difficulty of searching for a single gene in the genome of a species, let us consider the case of a single gene comprised of about 1000 base pairs (bp), i.e. a gene of about 1 kilobases. This would encode a protein of about 30,000 molecular weight considering that every three base pairs could potentially designate an amino acid of average molecular weight (i.e. about 110 daltons). A search for this sequence in even the smallest, most primitive, replicating structure known, a virus, is possible since most viral DNAs range from 5 kb to 200 kb in size (Table 1).

In self-replicating systems, the degree of difficulty of searching for a single gene copy mounts. In bacterial systems it rises by about 2-3 orders of magnitude. The gene becomes now only one of 800 to 4000 contained in the bacterial genome. In eukaryotic systems, i.e. fungi, yeasts, an extremely sensitive assay system is necessary since the single gene copy must be located amongst the 10-15,000 present. In the human genome an enormous jump in the degree of difficulty of locating the single gene occurs. The search necessitates the location of 1 gene in 2.9×10^6 fragments of about 1,000 bps in length. This is equivalent to searching for the proverbial needle in a haystack. In spite of this difficulty, the application of DNA

technology to the human genome is proceeding at a rapid pace (4,5). Gene markers for many diseases are being sought and found (6-10). It has even been suggested that a map of the total human genome be made (11). A project of this scale would be equivalent to the megaprojects (atom-smashers) proposed by the high energy physicists.

Forensic science has not been untouched by all this DNA-related activity. In the past few years, DNA has fallen as the last bastion of macromolecular structures being used to investigate fluids derived from humans. This has occurred not so much because many single genes have been isolated, thereby allowing for the typing and identification of human DNA, but because of the discovery that several highly repetitive sequences in human DNA seem to be inherited in an individual specific manner.

It is the purpose of the present communication to indicate how DNA technology is being applied in the area of forensic science. In order to provide some background, the technology of how DNA is isolated, handled and processed will be reviewed. The subject of DNA probes will then be briefly discussed and their application in the forensic science area will be described. Finally, some idea of what is required to implement this type of technology will be given along with some indication of the direction this technology will take in the future.

B. DNA Technology

In application three steps are required before DNA can be used or tested. These are outlined in Figs. 1-3.

1. DNA Handling

Before use the DNA has to be isolated and cleared of extraneous RNA, proteins, carbohydrates, lipids and other contaminants (12). Usually a combination of detergents and enzyme treatments are applied to free up the DNA and remove contaminants. The detergent most frequently used is sodium dodecylsulfate while the enzyme treatments usually employed broad-specificity proteases such as pronase or proteinase K.

The DNA is then purposefully cut into smaller fragments by using restriction endonucleases (12-16). These enzymes cut the DNA at specific base sequences to leave either a sticky end i.e. an end with a few unpaired bases or a blunt-end i.e. an end with all bases paired.

The site cleaved by the restriction enzyme is quite specific. In small pieces of DNA e.g. bacterial plasmids, this can mean only a limited number of fragments will be produced. In large pieces of DNA, multiple cleavage sites are usually present. The fragments produced are separated by eletrophoresis in agarose gels (usually horizontal submarine gels). The separation is by size and, for DNA where a limited restricted number of restriction enzyme cleavage sites are present, this cleavage results in only a small number of bands. In the case of human DNA many fragments are usually produced resulting in a

gel which has the DNA smeared from one end to the other as visualized by ethidium bromide DNA-specific dye staining.

After separation, the DNA is immobilized by transfer to a membrane made of either cellulose nitrate or cationically charged nylon. This step is done in order to make the subsequent hybridization and detection steps more convenient. The transfer from the wet gel is done by either fluid absorption or electroblotting. Both work equally well and each has its own set of advantages and disadvantages. For example, simple blotting allows for the capture of most fragments but it is a slow process (>24 hours). Electroblotting is somewhat faster but suffers from the fact that fragment transfer rates differ and occasionally fragments may be lost.

The binding to the support membrane is initially only by electrostatic attachment (cationic nylon) or weak covalent bonds (cellulose nitrate). These bonds are usually strengthened by a DNA-denaturing, heat process (baking). More recently a photochemical process (i.e. fixation of DNA to the membrane by ultraviolet irradiation) has been suggested as an alternative to this baking process.

The whole process of DNA transfer and immobilization on a membrane is called Southern transfer after its inventor, E.M. Southern (17).

2. DNA Hybridization

The DNA helix consists of two single-stranded polynucleotide fragments. The two polymer chains all held in

place by the required adenine-thymine (A-T) (low strength), guanine-cytosine (G-C) (high strength) associations. Strand separation requires an energy input, usually heat. The process can be followed by observing changes in the ultraviolet absorption spectrum (Fig. 2a). The temperature at which strand separation occurs is determined by the G-C content of the two strands and is termed the melting temperature (Tm) (Fig. 2b). Reassociation of the separated strands occurs when the temperature is dropped (Fig. 2c). The extent and rate of association is controlled by the level of homology (similarity of nucleotide composition) found between the two strands. A high degree of homology (good base pair AT/GC matching) leads to a rapid and extensive reannealling of the chains and restoration of the original ultraviolet spectrum. The extent of homology of sequences contained in two strands can be assessed by this process. The process can be carried out at equilibrium by placing the two separated strands at a temperature just at the Tm. This will lead to strand reassociation related to the degree of homology between the chains. The overall process of strand reassociation, also known as DNA hybridization, is influenced by other factors e.g. salt type and concentration, solution pH, polymer additives and water activity (a_w) (18). By adjusting these parameters two highly homologous strands will exhibit on almost complete reassociation of the two strands. Under these restrictive conditions, also termed high stringency conditions, the extent of homology between two chains can be

assessed. These operations are usually carried out at temperatures around 65-70°C. The addition of a neutral organic solvent, formamide, can also be done to allow the DNA hybridization to take place at lower, more manageable temperatures (40-45°C).

3. DNA Detection

In practice the association of fragments is followed by radiolabelling the DNA sequence of interest and determining its presence or absence when the fragments are brought together. In practice an immobilized fragment of DNA is probed for the presence of a particular sequence by hybridizing it with the complementary radiolabelled sequence. Labelling of the complementary fragment is done by using highly radioactively labelled ^{32}P-containing compounds (4,000-8,000 Ci/mM). Several methods for incorporating the radiolabelled precursors into the fragment are used (Fig. 3) (19-25).

The ends of the chains can be labelled with phosphate in a dephosphorylation-phosphorylation sequence, involving 5' addition of phosphate employing radiolabelled γ ^{32}P ATP and polynucleotide kinase, while 3' additions can be done using α ^{32}P ddATP and terminal transferase. These methods, while satisfactory for the labelling of small fragments, usually do not give probes of sufficiently high specific activity for multikilobase probes.

In order to get labelled DNA of sufficient specific activity the addition of nucleotides to the polynucleotide

chains is the preferred method. This addition can be done: 1) by insertion of nucleotides into the sticky ends created by restriction enzyme cleavage by using terminal transferase or T_4 DNA polymerase and radiolabelled nucleotides; 2) by tailing the polynucleotide chain with T_4 DNA polymerase and only one radiolabelled nucleotide; 3) by using multiprimers (short hexanucleotide sequences of random composition) and radiolabelled nucleotide(s) on the separated strands in the presence of the large fragment of E. coli DNA polymerase 1 (Klenow fragment); 4) by nick translation whereby the endo- and exonuclease activity associated with DNA polymerase (pol 1) is used to nick and remove nucleotides while the DNA polymerase activity reinserts them into the chain.

The detection of the hybridization is by liquid scintillation counting or autoradiography. Hybridizations done on large filters or in a dot-blot apparatus in a microtiter format can be assessed by removal of the test area and counting in the normal liquid scintillation media. Dot-blot hybridizations and hybridizations after electrophoresis transfer can also be assayed by autoradiography using X-ray film and exposures ranging from a few hours to a week. These exposures are usually done at -70°C with an intensifying screen to improve the signal-to-background ratio. The intensity of the signal is controlled by both the specific activity of the probe and its concentration on the membrane along with normal self-quenching of the signal observed.

C. DNA Probes

The search for a specific gene or polynucleotide sequence in the human genome requires two steps. The first is the cleavage of the genome into manageable fragments using one or more restriction enzymes. Even though in situ hybridization and separation of large sized fragments in pulsed field electrophoresis systems is possible, fragments of smaller, more manageable size are separated in the electrophoresis systems now used. Normally fragments ranging in size between 0.5 kb and 20 kb are separated on the agarose gels (0.8% → 1.2% w/v composition). Fragments in this size range are readily produced by restriction enzyme cleavage (12-16). Because of its size the cleavage of human genomic DNA by any of the restriction enzymes available produces a host of fragments in the 0.5 to 20 kb size. Many of the fragments overlap when separated by the usual electrophoresis procedures. Thus simple separation on an agarose gel for gene location is not sufficient. A second step is required in order to locate the specific gene sequence being sought. This step is aimed at differentiating the many overlapping bands. A certain degree of selectivity is required. For this purpose a probe, or more specifically, a segment of the sought after DNA, is used to hybridize with each of the separated bands. Thus, Southern transfers are hybridized with the radiolabelled probe sequence and the presence or absence of the sequence sought is determined by autoradiography of the membrane after thorough washing to remove molecules with non-specific binding character.

Specific banding patterns can result from the process of radioactive probe DNA-target DNA hybridization. Variations amongst individuals in the specific banding patterns are due to changes in the number and location of the restriction enzyme cleavage sites or actual deletion or amplification of the target sequence. The process of altering banding patterns related to the use of various restriction enzymes is termed restriction fragment length polymorphism (RFLP). A simple version of the pattern shifts encountered is illustrated in Figs. 4 and 5. Single probe site patterns shift location in a manner directly related to the fragment size produced. Where two probe sites are close together a more complex pattern results. Restriction enzyme cuts made directly within the probed sequence (Fig. 5) can result in the formation of two bands, depending on the probe length and the position of the cleavage site.

A test of restriction enzymne cleavage site loss, gain or shift can be made by using the restriction enzymes Msp II, a CCGG sequence cutter, and Taq I, a TCGA sequence cutter (26). Banding pattern shifts generated by the use of these two enzymes are compared. The shifting patterns are usually related to a base pair substitution at the enzyme cleavage site. This is a very short range affect unlike the situation where an entire gene sequence has had insertions, deletions or rearrangements occuring in it. These insertions, deletions or rearrangements can only be checked by using a probe, better still several probes, whose pattern of inheritance has been checked.

"Which probes can be used?" is one of the most important questions associated with RFLP work (26). Probes may be taken from a library of probes prepared for completely different purposes. They may also be generated by isolation of a smaller fragment of the total genome e.g. isolation of fragments from a single chromosome or from somatic cell hybrids (i.e. animal cells containing a limited amount of human chromosomal material). The small gene fragments can be used directly or can be further fragmented to obtain a fragment that detects an RFLP.

RFLP's can also be searched for by preparing probes to specific genes (26-36). To date, however, most DNA polymorphisms which have resulted from the use of a single copy probe have been of the type associated with the loss, gain or shift of a restriction enzyme cleavage site, i.e. a single point mutation, and not from the insertion, deletion or rearrangement of an entire gene (37).

D. . Forensic Applications

Until fairly recently the biological revolution associated with handling and manipulating DNA had not touched the forensic science area. Most identification assays of a biochemical nature relied on proteins and carbohydrates (38). The use of DNA remained very much in the background. Much of the work being done on human DNA was being aimed at the isolation of specific genes and determining the linkage between various diseases and the structure of the genome (27,28,39,40).

Until quite recently the technology being developed seemed of limited use since it offered no apparent improvement, either in accuracy or time, in establishing identification of body fluid samples. In spite of this several examples of the use of DNA probes for identification of body fluids have appeared (41-44).

A probe originating from the HRAS-1 gene, a sequence localized on the short arm of chromosome 11 near the insulin gene, and a probe of the D14S1 locus of the teleomeric region of the long arm of chromosome 14 which has been closely linked to immunoglobulin gene, have both been applied to the RFLP examination of blood and sperm as well as paternity analysis (41-43). Single RFLP bands and a limited range of multiple RFLP bands were generated. Band identification was by band size and identified to the nearest 40 bp in 2.6 kb sequences and the nearest 60 bp in 4.0 kb sequences.

Probes of the simple oligonucleotide sequence $(GA^{T}_{C}A)_{n}$, n = 2-5, the so-called simple quadruplet repeats (sqr) which were originally found in female specific satellite DNA and subsequently shown to be conserved in the eukaryotes, have also been shown to generate an RFLP banding pattern in Alu I and Mbo I digested human DNA (44). A $(GATA)_5$ oligonucleotide appeared to be an optimum probe length and generated a maximum number of bands under the conditions used. DNA from seven unrelated Caucasians, two Asians and one African were examined in this case.

The limited number of bands revealed by these probes suggest that these types of probes can be used under only very

specific circumstances. Even considering the limited number of bands scored, probabilities of identity calculated for these samples suggest that DNA analysis has a place to play in the identification of body fluid samples. A multiple band structure would be more desirable for identifying samples since many cross comparisons could be made thereby reducing the probability of a mismatch being made in samples. One of the first reports of such a multiple banded pattern appeared in the literature in 1985. A.W. Jeffrey and colleagues described the use of a specific sequence of DNA which, upon hybridization with restriction enzyme-cut DNA from blood, produced a multibanded pattern (45). The large number of bands produced suggested that such a probe might have utility in specimen identification since the pattern seemingly was individual specific (46).

The specific sequence used originated from a tandem-repetitive minisatellite region located within the human myoglobin gene (47,48). It was isolated and cloned as shown in Fig. 6 (45). The hypervariable minisatellite region from which the sequence was derived is similar to those previously found in other gene sequences (45). A subset of the minisatellites have cores 10-16 bp long and may be a signal for the gene recombination required to generate these hypervariable regions (45,49,50).

Southern blot analysis of Hinf I or Hae III cleaved human DNA detected multiple hypervariable DNA fragments (45). Jeffrey's and colleagues have developed two repeated sequence

core probes. Each generates a different pattern of bands which seem to be individual specific and show somatic and germ-line stability. Two large families have been studied with two of the developed probes and segregation analysis of the banding pattern done. Up to 34 autosomal hypervariable loci were scored and their suitability for linkage analysis was suggested (51-53).

A total number of about 60 hypervariable loci were detected by both probes used. Most seemed genetically unlinked, stability inherited and scattered over the entire human genome. It was estimated that, although the areas used may be recombinatoral hotspots (49,52), the estimated rates of unequal exchange occurring at long loci was not sufficient to disturb any linkage between the minisatellite locus and the neighbouring gene.

An example of DNA fingerprint analysis gathered in our laboratories using this type of probe is given in Fig. 7. The multiband pattern developed by the three specimens is quite evident and the effect of changing the restriction enzyme used (Hinf I to ScrF I) is also easily seen. An improvement of the discrimination between bands in the smaller fragment region (2-5 kb area on the gel) is achieved by the use of Dra I in combination with either Hinf I or ScrF I.

The forensic application of these DNA fingerprints (54) was suggested since the probability of chance association was calculated to approach absolute certainty ($<3\times10^{-11}$ with

probe 33.15 and $<<5x10^{-19}$ with probe 33.6). The probes were subsequently applied in an immigration case to provide positive identification and the probability of association was calculated using 61 bands as identifiers (55). Using the basic data, the likelihood of prior probabilities were also computed (56).

This particular example and the large volume of commentary arising from it (56-61) has drawn attention to the possibility of wider application of this type of technology to the rapid identification of individuals. In one of the commentaries (57) a table of percent chance of positive identification was included. In it the total for all combined, presently-used assays (some 19 in number, including HLA analysis) was 99.7%. The results obtained to date using a single DNA fingerprint analysis are as indicated above, far better.

In use the minisatellite probe did not appear to pick up bands originating from the X or Y chromosome. Probes with Y chromosome specificity have recently become available (62-66). In general, probes fall into one of several categories i.e. those with one or very few copies per cell (about 50% of all sequences), those having several hundred copies per cell (about 20% of all sequences), those having 10^3-10^5 copies per cell (about 15% of all sequences) and those with more than 10^6 copies per cell (the remaining 15%). To be Y-specific, sequences have to fall into the single or low copy number categories. They must also have high homology with the

sequences on the Y-chromosomal DNA. Although high stringency hybridizations and washes ensure high homology, with repetitive sequences this may not be the case so that an absolutely true indication of the repetitive element homology may not readily be ascertained. Most of the Y-specific probes have some cross-reaction with X-chromosomal DNA. Some, however, are true single copy sequences having high Y homology. One of the more recently described probes is that described by Ngo and collaborators (66). An example of the good sex typing results we have obtained with this probe is given in Fig. 8.

The application of a Y-specific probe would permit sex typing to be readily done on a variety of body fluids which are at present typed only with difficulty (e.g. vaginal fluids).

Implementing DNA fingerprinting analysis requires that several steps be followed. They are outlined in Table 2. Sample retrival from various body fluids is an important aspect of the sampling procedure. Sufficient material of the required quality must be recovered for assay. In general, for fresh samples or those recently deposited i.e. less than a few hours old, present little problem in recovering adequate material is encountered. A blood sample containing 0.5-10 µg of DNA i.e. about 10-100 µl whole blood is nominally required per RFLP analysis.

At present, the affect of retriving aged samples has been only tested under a limited set of conditions. The observations suggest that, in samples of test material aged over

a several week period, progressively less DNA is recovered using a standard DNA extraction procedure. The recovered DNA is, however, of reasonable quality since the resulting banding pattern remains essentially the same as that found for fresh samples.

Sample extraction from material deposited on various surfaces has not, to date, been widely investigated. Blood has been deposited on glass and aged for up to 28 days with no apparent change in banding pattern (pAW101, EcoRI cleavage and pLM0.8 probes, Taq I cleavage) (41). Sperm DNA, was received from several sites, (swabs lavage and from clothing) and tested with the same probes (42). It was shown that the RFLP banding pattern was the same as that generated by freshly drawn blood. Although the initial work has suggested no influence of age or collection site on the RFLP banding pattern only a limited number of samples, few surfaces, probes and restriction enzymes have been tested. Further work will, thus be required.

Storage is also another important aspect of the sampling procedure. Most samples will require storage at -70°C to impede further degradation. The storage could be the specimen as collected or as the partially processed material. Although high molecular weight DNA does not readily degrade when stored at ultra low temperature the affects of very long term storage over several years are not known.

The extraction of relatively intact DNA suitable for "fingerprinting" or genetic identity testing from liquid blood

samples is generally not a problem. The DNA containing cells are ruptured and then, by a series of solvent extractions, the protein removed without fragmenting the DNA. Once the DNA is purified, the restriction enzyme being used can locate all of its cutting sites. If there was failure to completely remove the protein or traces of solvent from the DNA, the restriction enzyme produces a partial digestion of its cutting sites which can alter the RFLP pattern normally produced.

In bloodstains the cells are already ruptured and it would seem an easy matter to extract its DNA contents. However, this is not always the case as the proteins in the bloodstain must first be treated by a protease digestion step. Once in an aqueous solution, the DNA can be purified using the normal solvent extraction protocol used for liquid blood. Contrary to a liquid blood sample in the clinical laboratory, the quantity of DNA in a blood or body fluid stain is a limiting factor. Often associated with critical forensic evidence are small volumes of the questioned body fluid stain (i.e. a blood smeared knife blade, a discrete bloodstain on a suspect's clothing, a vaginal swab taken longer than 12 hours after a sexual assault). Each time there is a protein removing solvent step, an amount of DNA is lost in the interface between the aqueous DNA containing solution and the organic protein-containing solvent. Generally in clinical laboratories, three or four extractions are used for purifying DNA extracted from 5 mls of liquid blood. For bloodstains, the equivalent volume of blood

is likely to be 10 to 100 microlitres. Thus to obtain adequate sensitivity a compromise must be made between quantity and quality that potentially could alter the genetic identity-testing result. Although not optimum, Gill et al. reported that two phenol chloroform extraction steps were used to purify stain extracted DNA. The extraction of quality DNA from human semen in post-coital vaginal swabs requires elimination of the vaginal origin DNA before genetic identity information can be generated on the semen donor. A protocol used by Gill et al. successfully ruptured the vaginal cells and extracted their DNA by using a non-specific, protein digesting enzyme (proteinase K) in the absence of a chemical reducing agent. The sulfur rich proteins on the sperm head fail to digest until this chemical is added. Once added to the reaction the sperm DNA will then go into solution and can be recovered free of vaginal origin DNA by solvent extraction.

In the next step, a restriction enzyme choice must be made. Several enzymes have been tried. They are: Eco RI, Taq I, Msp I, Alu I, Mbo I, Hae III and Hinf I. Their origin and the cleavage site is given in Table 3. Two leave blunt ends (Alu I and Hae III) while the others generate sticky ends of variable length. The enzyme choice depends on the cleavage site within genes being processed, the RFLP fragment pattern of cleavage in the DNA being processed, the extent of methylation of the genetic information and the hybridizing probe being used. An Msp I/Taq I combination has been suggested to eliminate site

modification factors. Most cleavages done where minisatellites banding patterns have been investigated have used Hae III or Hinf I. The SerFI/Dra I combination described here (fig. 7) also seems to give good band discrimination in both the small and large fragment size regions.

The membrane used to immobilize the restriction fragments produced must be chosen. In general, nitrocellulose membranes work well for large size fragments. Cationic nylon membranes work well for the smaller sized fragments (several hundred base pairs and lower). Sample size and availability might restrict the number of trials possible and thus some generalized protocol will be needed to ensure optimum immobilization under most conditions.

Next on the list is probe choice. To date, the minisatellite probe developed by Jeffreys seems to give the highest and most rapid discrimination between samples. Other, more specific gene probes likely will be required to back up the original data. The number of choices will also be influenced by the availability of the material being screened. Too little material will require that a judicious choice in probes be made in order to maximize the information content. At present though, none of the probes are readily available for off-the-shelf use save for one (see M13 below). This might require that probes be constructed in-house, sometimes under license.

Data collection and analysis is being done by hand, for the most part, and involves by-eye comparison of

autoradiogrammes. Band migration distances are taken into account. Band intensities can only be taken into account if the material has been shown to be terminally digested. Partial digestion of the sample, be it because of poor protein removal or poor activity of the restriction enzyme, could lead to an erroneous interpretation of the results if band intensity on a single digest is considered. No attempts at automation of data collection by digitization have, as yet, been reported.

The cost of implementing a service has not been directly determined. In several reports it has been suggested that, for low volume users, a cost of 250-300 $US per analysis needs to be charged to have a profitable operation (61). To some this might not sound like an excessive cost, however, their are several factors which have to be taken into account when costing out such a service. They are outlined in Table 4. The equipment required and building requirements are those frequently, but not always, encountered in other operations where biochemical analyses are being done.

Operating costs can be high since DNA-processing enzymes are low volume usage items having a relatively high stocking cost (100 $US per stock unit). Even though only small amounts are required per assay, most enzymes have low stability when frozen and thawed thus requiring frequent stock replacement. A major expense is also incurred in the provision of radiolabelled nucleotides and labelling kits. With a ^{32}P half-life of 14 days it is evident that frequent replenishment

of radiolabel stocks must also be made. A radiolabel disposal protocol must also be implemented to handle the wastes being generated. Membrane transfer products (nitrocellulose or modified nylon) and special electrophoretic DNA-grade agarose constitute some of the further expenses incurred.

One of the major expenses to be incurred will be that associated with salaries. Most personnel being hired will have backgrounds in the molecular biology area. The great competition amongst the genetic engineering companies and those companies now entering the protein engineering area have meant that, quite frequently, Ph.D. level personnel will have to be hired to do the work. A high level understanding of the problems and pitfalls in the analysis is required and this is gained usually through experience, implying that several years of training at an advanced level will be required. As advancements in interpretational skills are made and a better understanding of the genetic basis of the banding patterns is acquired, along with protocol standardization and the automation of many steps, it can be expected that some of the burden can be shifted to the technical level thus lowering overall salary costs.

E. Future Directions

As seen above the use of systems for fingerprinting of human genomic DNA appears to have a great future in the area of forensic investigations. Work done to date certainly implies that DNA fingerprinting analyses have the potential to replace

many of the protein and carbohydrate-based assays being done today. However, future developments in both the technological and non-technological areas will be needed before this DNA-based technology finds its rightful place in forensic science.

1. Technological Developments

Many conditions need to be met before any genetically-based marker system becomes part of the medico-legal community's tools. Some of the conditions required have been alluded to in a recent paper (68). They are as follows: 1) The true genetic character of the systems being used to date will have to be ascertained; 2) Interpretation of the results will require that population gene frequencies and linkages (69-70) will need to be assessed; 3) Nomenclature systems will have to be set-up to permit data recording and communication of results in as non-pictorial fashion; 4) Standardization of protocols, methodology, apparatus, reagents and markers will be required; 5) Reproducibility and reliability of the results will also have to be tested through blind trials.

To meet all these conditions will require considerable effort and several recent developments will have an impact on the future course of the work. Developments in laboratory equipment and processing protocols are underway. Much of the specialized equipment needed is already available but recent additions include: a high temperature washer/hybridization system and an apparatus for preparing a Southern blot and an apparatus to extract high molecular weight genomic DNA.

The development of non-radiolabelled systems is now underway (71-74). Most are based on a biotin-avidin reaction scheme with detection by an enzyme amplification assay (Fig. 9). One, based on the HLA gene system, is already available (Cetus). Newer systems based on fluorescent, chemi- and bioluminence systems are being developed. A new system for labelling DNA by direct reaction has recently been described (75). At present, these non-radioactive labels apply to systems with high copy numbers since sensitivity of the assay does not yet approach that of the radiolabelled systems. New developments in substrate/enzyme combinations, based on coupling alkaline phosphatase and a tetrazolium to formazan conversion (76,77) (c.f. BRL-Blugene^{R}), suggest that the sensitivity limits can, however, be pushed even lower. Work done in our laboratories in this area has just begun to test these lower limits. For very low copy numbers application of gene amplification schemes will be required. One such scheme, the polymerase chain reaction, has been described recently (78,79) (Fig. 10).

The availability of alternate gene markers of a more specific nature will be needed in order to meet the conditions of genetic inheritance of the RFLP banding pattern. Work on sorting out suitable markers for the various loci involved in the minisatellite pattern has begun (51,80). Recently, ten oligomeric sequences derived from the tandem repeat regions of the myoglobin gene, the zeta-globin pseudo gene, the insulin gene and the X-gene of hepatitus B virus have been used to

develop single copy probes for use in defining the allelic character of many of the bands seen in the band patterns developed using minisatellite probes (81).

Alternate gene markers will also likely become available as more and more genes become available. One of the most likely sources of new gene markers will be those derived from the Major Histocompatibility Complex (MHC) and, more specifically, from the Human Leucocyte Antigen (HLA) system (82). A vast literature on this system is available, i.e. 1600 identified loci (825 directly linked to chromosomes). This system has already been put to use in defining linkage between various gene loci and several diseases. It is not possible in the present communication to touch on all the history of the system and attempt to unravel the many interwoven strands which led to the present day concept of this system. The reader is referred to a recent summary of the vast literature on this subject (83) and leading references to the organization of the HLA genes (84-86).

Although most, RFLP patterns have been generated by probes isolated from sequences associated with conventional gene markers other, more novel sources may be found. In fact, a recent report may speed the practical application DNA technology in forensic science. It was found that a multiple banding pattern could be developed by probing mammalian DNA with the phage vector M-13. Hypervariable minisatellites were detected and traced to two clusters of a GC rich, 15 bp sequence located

in the protein III gene of this bacteriophage (87). This phage is readily available and testing of the multiple banding pattern produced by the use of this system should rapidly proceed.

2. Non-technical Developments

Many of the legal and ethical aspects of this technology have not been addressed. Patent protection for many of the probes is being sought, including the M13 phage. Whether they all will be granted will remain to be seen. If they are granted, then implementation will be slowed while licensing arrangements are worked out or other probes are being sought.

In the legal system, cases using DNA technology have just now had their first exposure. Apart from two paternity cases no other uses have been reported. The rights of the defense or prosecution to use the technology could been challenged (88). In line with recent suggestions that this type of technology be used in the granting or refusing of life insurance policies has also raised the problem of confidentiality of results. This certainly will be a problem where direct links between the banding pattern and various lethal diseases or even the presence of a lethal virus such as the retrovirus HIV (AIDS-virus) has been found.

In the Canadian context, a person can refuse to provide a blood sample even when they have been charged with a major criminal offense. Thus in the case where the perpetrator of the offense has deposited DNA containing body fluid stain

evidence but refuses to give a blood standard for the investigation, the prosecution evidence could be rendered ineffective unless the proper standard can be acquired.

In spite of the fact that this technology is in its infancy and many problems need to be resolved, the future application of this technology based on the use of DNA certainly looks to be assured.

References

1. J.D. Watson and J. Tooze. The DNA Story. A Documentary History of Gene Cloning. W.H. Freeman, San Francisco, 1981.

2. J.D. Watson, N.H. Hopkins, J.W. Roberts, J. Argetsinger-Steitz and A.M. Weiner. Molecular Biology of the Gene, 4th Edition, Vol. 1. Benjamin/Cummings, Menlo Park, California, 1987.

3. J.D. Watson. Molecular Biology of the Gene, 3rd Edition. W.H. Benjamin, Menlo Park, California, 1976.

4. H.J. Evans. New trends in human genetic research - an introduction and overview. Experientia 42: 1069-1075 (1986).

5. B.H. Anderton. Progress in molecular pathology: Alzheimer's disease. Nature 325: 658-659 (1987).

6. X. Estivill, M. Farrall, P.J. Scambler, G.M. Bell, K.M.F. Hawley, N.J. Lench, G.P. Bates, H.C. Kruyer, P.A. Frederick, P. Stanier, E.K. Watson, R. Williamson and B.J. Wainwright. A candidate for the cystic fibrosis locus isolated by selection for methylation-free islands. Nature 326: 840-845 (1987).

7. D. Goldbaber, M.I. Lerman, O.W. McBride, U. Saffiotti and D.C. Gajdusek. Characterization and chromosomal localization of a cDNA encoding brain amyloid of Alzheimer's Disease. Science 235: 877-880 (1987).

8. R.E Tanzi, J.F. Gusella, P.C. Watkins, G.A.P. Bruns, P. St. George-Hyslop, M.L. Van Keuren, D. Patterson, S. Pagan, D.M. Kurnet and R.L. Neve. Amyloid β-protein gene: cDNA, mRNA distribution and genetic linkage near the Alzheimer locus. Science 235: 880-884 (1987).

9. P.H. St. George-Hyslop, R.E. Tanzi, R.J. Polinsky, J.L. Haines, L. Nee, P.C. Watkins, R.H. Myers, R.G. Feldman, D. Pollen, D. Drachman, J. Growdon, A. Bruni, J.-F. Foncin, D. Salmon, P. Frommelt, L. Amaducci, S. Sorbi, S. Piacentini, G.D. Stewart, W.J. Hobbs, P.M. Conneally and J.F. Gusella. The genetic defect causing familiar Alzheimer's Disease maps on chromosome 21. Science 235: 885-890 (1987).

10. S. Hodgkinson, R. Sherrington, H. Gurling, R. Marchbanks, S. Reeders, J. Mallet, M. McInnes, H. Petursson and J. Brynjalfsson. Molecular genetic evidence for heterogeneity in manic depression. Nature 325: 805-806 (1987).

11. D.E. Koshland, Jr. Sequencing the human genome. Science 236: 505 (1987).

12. T. Maniatis, E.F. Fritsch and J. Sambrook. Molecular cloning, a laboratory manual. Cold Spring Harbor Laboratory, Cold Spring Harbor, N.Y. 1982.

13. J.G. Chirikjian. Gene Amplification and Analysis, Vol. 1. Restriction Endonucleases. Elsevier/North Holland, New York, 1984.

14. R.J. Roberts. Restriction and modification enzymes and their recognition sequences. Nucleic Acid Res. 11: r135-r167 (1983).

15. R.J. Roberts. Directory of restriction endonucleases. Methods in Enzymology (R. Wu, ed.) 68: 27-41 (1979).

16. A.A. Szalay, C.J. MacKey and W.H.R. Langridge. Restriction endonucleases and their applications. Enzyme Microb. Technol. 1: 154-164 (1979).

17. E.M. Southern. Detection of specific sequences among DNA fragments separated by gel electrophoresis. J. Mol. Biol. 98, 503-517 (1975).

18. G.A. Beltz, K.A. Jacobs, T.H. Eickbush, P.T. Cherbas and F.C. Kafatos. Isolation of multigene families and determination of homologies by filter hybridization methods. Methods in Enzymology (R. Wu, L. Grossman and K. Moldave, eds.) 100: 266-285 (1983).

19. P.W.J. Rigby, M. Dieckmann, C. Rhodes and P. Berg. Labelling deoxyribonucleic acid to high specific activity in vitro by nick translation with DNA polymerase 1. J. Mol. Biol. 113, 237-251 (1977).

20. T. Nelson and D. Brutlag. Addition of homopolymers to the 3'-ends of duplex DNA with terminal transferase methods in enzymology (R. Wu, ed.) 68: 41-50 (1979).

21. S.I. Yousaf, A.R. Carroll and B.E. Clarke. A new and improved method for 3'-end labelling DNA using [α-^{32}P]-ddTATP. Gene 27: 309-313 (1984).

22. A.P. Feinberg and B. Vogelstein. A technique for radiolabeling DNA restriction endonuclease fragments to high specific activity. Anal. Biochem. 132: 6-13 (1983). Addendum ibid. 137: 266-267 (1984).

23. J.R. Lillehaug, R.K. Kleppe and K. Kleppe. Phosphorylation of double-stranded DNA's by T_4 polynucleotide kinase. Biochemistry 15: 1858-1865 (1976).

24. J.R. Lillehaug and K. Kleppe. Effect of salts and polyamines on T_4 polynucleotide kinase. Biochem. 14: 1221-1229 (1975).

25. K.L. Berkner and W.R. Folk. Polynucleotide kinase exchange reaction. Quantitative assay for restriction endonuclease-generated 5'-phosphoryl termini in DNA's. J. Biol. Chem. 252: 3176-3184 (1977).

26. M.H. Skolnick and R. White. Strategies for detecting and characterizing restriction fragment length polymorphisms (RFLP's). Cytogenet. Cell. Genet. 32: 58-67 (1982).

27. R. White. DNA sequence polymorphisms revitalize linkage approaches in human genetics. Trends in Genet. 1: 177-181 (1985).

28. D.T. Kingsbury. DNA probes in the diagnosis of genetic and infectious diseases. Trends in Biotechnol. 5: 107-111 (1987).

29. D. Botstein, R.L. White, M. Skolnick and R.W. Davis. Construction of a genetic linkage map in man using restriction fragment length polymorphism. Ann. J. Hum. Genet. 32: 314-331 (1980).

30. M.H. Skolnick, H.F. Willard and L.A. Menlove. Report of the committee on human gene mapping by recombinant DNA techniques. Cytogenet. Cell. Genet. 40: 210-273 (1985).

31. S.E.Y. Goodbourn, D.R. Higgs, J.B. Clegg and D.J. Weatherall. Molecular bases of length polymorphism in the human ζ-globin gene complex. Proc. Natl. Acad. Sci. U.S. 80: 5022-5026 (1983).

32. M. Goossens and Y.Y. Kan. DNA analysis in the diagnosis of hemoglobin disorders. Methods in Enzymology 76: 805-817 (1981).

33. S.H. Ortkin. The duplicated human α-globin genes lie close together in cellular DNA. Proc. Natl. Acad. Sci. U.S. 75: 5950-5954 (1978).

34. A.J. Jeffreys. DNA sequence variants in the Gγ, Aγ, σ and β-globin genes of man. Cell 18: 1-10 (1979).

35. Y.W. Kan and A.M. Dozy. Polymorphism of DNA sequence adjacent to human β-globin structural gene: relationship to sickle mutation. Proc. Natl. Acad. Sci. 75: 5631-5635 (1978).

36. J.F. Gusella, C. Keys, A. Varsanyi-Breiner, F.-T. Kao, C. Jones, T.T. Puck and D. Housman: Isolation and localization of DNA segments from specific human chromosomes. Proc. Natl. Acad. Sci. 77: 2829-2833 (1980).

37. D. Barker, M. Schafer and R. White. Restriction sites containing CpG show a higher frequency of polymorphism in human DNA. Cell 36: 131-138 (1984).

38. D.J.H. Brock and O. Mayo. The biochemical genetics of man. 2nd Edition, Academic Press, New York, 1978.

39. H.J. Evans. New trends in genetic research - An introduction and overview. Experientia 42: 1069-1075 (1986).

40. C.T. Caskey. Disease diagnosis by recombinant DNA methods. Science 236: 1223-1229 (1987).

41. E. Kanter, M. Baird, R. Shaler and I. Balazs. Analysis of restriction fragment length polymorphisms in deoxynucleic acid (DNA) recovered from dried bloodstains. J. Forensic Sci. 31: 403-408 (1986).

42. A. Giusti, M. Baird, S. Pasquale, I. Balazs and J. Glassberg. Application of deoxynucleic acid (DNA) polymorphisms to the analysis of DNA recovered from sperm. J. Forensic Sci. 31: 409-417 (1986).

43. M. Baird, I. Balazs, A. Giusti, L. Miyazaki, L. Nicholas, K. Wexler, E. Kanter, J. Glassberg, F. Allen, P. Rubinstein and L. Sussman. Allele frequency distribution of two highly polymorphic DNA sequences in three ethnic groups and its application to the determination of paternity. Am. J. Hum. Genet. 39: 489-501 (1986).

44. S. Ali, C.R. Müller and J.T. Epplen. DNA fingerprinting by oligonucleotide probes specific for simple repeats. Hum. Genet. 74: 239-243 (1986).

45. A.J. Jeffrey, V. Wilson and S.L Thein. Hypervariable 'minisatellite' regions in human DNA. Nature 314: 67-73 (1985).

46. A.J. Jeffreys, V. Wilson and S. Thein. Individual-specific 'fingerprints' of human DNA. Nature 316, 76-79 (1985).

47. P. Weller, A.J. Jeffreys, V. Wilson and A. Blanchetot. Organization of the human myoglobin gene. The EMBO Journal 3: 439-446 (1984).

48. A.J. Jeffreys. DNA sequence variants in the $^{G}\gamma$-, $^{A}\gamma$-, σ- and β-globin genes of man. Cell. 18: 1-10 (1979).

49. M. Steinmetz, Y. Uematsu and K.F. Lindahl. Hotspots of homologous recombination in mammalian genomes. Trends in Genetics, 3: 7-10 (1987).

50. C.M. Radding. Homologous pairing and strand exchange in genetic recombination. Ann. Rev. Genet. 16: 405-437 (1982).

51. Z. Wong, V. Wilson, A.J. Jeffreys and S.L. Thein. Cloning a selected fragment from a human DNA 'fingerprint': isolation of an extremely polymorphic minisatellite. Nucleic Acids Res. 14: 4605-4616 (1986).

52. A.J. Jeffreys. Hypervariable DNA and genetic fingerprinting in, DNA probes. Applications in Genetic and Infectious Disease and Cancer (L.S. Lerman, ed.), Current Commun. Molecular Biol. Cold Spring Harbour, pp. 57-61, 1986.

53. A.J. Jeffreys, V. Wilson; S.L. Thein, D.J. Weatherall and B.A.J. Ponder. DNA 'fingerprints' and segregation analysis of multiple markers in human pedigrees. Am. J. Hum. Genet. 39: 11-24 (1986).

54. P. Gill, A.J. Jeffreys and D.J. Werrett. Forensic application of DNA 'fingerprints'. Nature 318: 577-579 (1985).

55. A.J. Jeffreys, J.F.Y. Brookfield and R. Semeonoff. Positive identification of an immigration test-case using DNA fingerprints. Nature 317: 818-819 (1985).

56. W.G. Hill. DNA fingerprint analysis in immigration test-cases (a commentary). Nature 322: 290-291 (1986).

57. B.E. Dodd. DNA fingerprinting in matters of family and crime. Nature 318: 506-507 (1985).

58. R. Lewin. DNA fingerprints in health and disease. Science 233: 521-522 (1986).

59. C. Vincent. Les sondes à ADN dans les services d'immigration et les prétoires. Biofutur 45: 61-62 (1986).

60. P.H. Whitehead. Biochemical techniques in forensic science. Trends in Biological Science 10: 299-302 (1985). See also commentary, Trends in Biol. Sci. 11: 68-69 (1986).

61. P. Newmark. DNA fingerprints go commercial. Nature 321: 104 (1986).

62. S.P. Daiger and R. Chakraborty. Mapping the human Y chromosome. Prog. Topics in Cytogenetics, 93-124 (1985).

63. U. Müller, U. Tontravaki, A. Monaco, H. Stroh, L.M. Kunkel and S.A. Latt. Repeated DNA sequences in the distal long arm of the human Y chromosome. Hum. Gen. 74: 24-29 (1986).

64. U. Müller, T. Donlon, M. Schmid, N. Fitch, C.-L. Richer, M. Lalande and S.A. Latt. Deletion mapping of the testis determining locus with DNA probes in 46, xx males and in 46 xy and 46, x dic(Y) females. Nucleic Acids Res. 14: 6489-6505 (1986).

65. U. Müller, T.A. Donlon, S.M. Kunkel, M. Lalande and S.A. Latt. Y-190, a DNA probe for the sensitive detection of Y-derived marker chromosomes and mosaicism. Hum. Genet. 75: 109-113 (1987).

66. K.Y. Ngo, G. Vergnaud, C. Johnsson, G. Lucotte and J. Weissenbach. A DNA probe detecting multiple haplotypes of the human Y chromosome. Am. J. Hum. Genet. 38: 407-418 (1986).

67. P. Newmark. DNA fingerprinting at a price at ICI's UK Laboratory (commentary). Nature 327: 548 (1987).

68. G.F. Sensabaugh. Forensic biology - is recombinant DNA technology in its future. J. Forensic Sci. 31: 393-396 (1986).

69. R. White and J.-M. Lalouel. Investigation of genetic linkage in human families. Adv. Human Genet. 16: 121-228 (1987).

70. P.M. Conneally and M.L. Rivas. Linkage analysis in man. Adv. Human Genet. 12: 209-266 (1982).

71. L. Gardner. Non-radioactive DNA labeling: Detection of specific DNA and RNA sequences on nitrocellulose and *in situ* hybridizations. Biotechniques 1: 38-41 (1983).

72. P.R. Langer, A.A. Waldrop and D.C. Ward. Enzymatic synthesis of biotin-labelled polynucleotides: Novel nucleic acid affinity probes. Proc. Natl. Acad. Sci. USA 78: 6633-6637 (1981).

73. J.J. Leary, D.J. Brigati and D.C. Ward. Sensitive colorimetric methods for visualizing biotin-labelled probes hybridized to DNA or RNA on nitrocellulose filters in Chromosomes and Cancer. (G. Ullman, ed.). Academic Press, New York. pp. 273-290 (1983).

74. J.J. Leary, D.J. Brigati and D.C. Ward. Rapid and sensitive colorimetric method for visualizing biotin-labelled DNA probes hybridized to DNA or RNA immobilized on nitrocellulose bio-blots. Proc. Natl. Acad. Sci. USA 80: 4045-4049 (1983).

75. E. Ziomek, P. Stepien and R.E Williams. An enzyme-based DNA probe system. Ann. N.Y. Acad. Sci. 745: 000-000 (1987) (in press).

76. S. Gatley. Enzyme amplification and its relevance as a non-isotopic detection system for use with nucleic acid probes in DNA probes - A new technology in its development and application. IBC Technical Services London, 1985. p. 18-29.

77. C.H. Self. Enzyme amplification- A general method applied to provide an immunoassisted assay for placental alkaline phosphatase. J. Immunol. Methods 76: 389-393 (1985).

78. K. Mullis, F. Falsona, S. Scharf, R. Saiki, G. Horn and H. Erlich. Specific enzymatic amplification of DNA *in vitro*: The polymerase chain reaction. Cold Spring Harbour Symposia in Quantitative Biology (Molecular Biology of *Homo sapiens*) 51: 263-273 (1986).

79. H.A. Erlich, G.T. Horn, R.K. Saiki, S.J. Scharf, K.B. Mulles and T. Bugawan. Genetic analysis using enzymatic amplification of specific genomic sequences. Current Comm. Mol. Biol. (DNA Probes, Applications in Genetic and Infectious Disease and Cancer, L.S. Lerman, ed.). Cold Spring Harbor Laboratory. Cold Spring Harbor, 107-112, 1986.

80. Y. Nakamura, C. Fuber, R. Wolff, T. Holm, P. O'Connel, M. Leppert and R. White. Characterization of a human 'minisatellite' sequence. Nucleic Acids Res. 15: 2537-2547 (1987).

81. Y. Nakamura, M. Leppert, P. O'Connell, R. Wolff, T. Holm, M. Culver, C. Martin, E. Fujimoto, M. Hoff, E. Kumlin and R. White. Variable number of tandem repeat (VNTR) markers for human gene mapping. Science 235: 1616-1622 (1987).

82. D.B. Amos and D.D. Kosty. HLA - A central immunoglobulin. agency of man. Adv. Human Genetics 10: 137-208 (1980).

83. J. Klein. Natural history of the major histocompatibility complex. Wiley - Interscience, New York, 1986.

84. M. Vaiman, P. Chardon and D. Cohen. DNA polymorphism in the major histocompatibility complex of man and various form animals. Animal Genetics 17: 113-133 (1986).

85. B. Mach, J. Gorski, P. Rollini, C. Berte, I. Amaldi, J. Berdoz and C. Ucla. Polymorphism and regulation of HLA class II genes of the major histocompatibility complex. Cold Spring Harbor Symposia on Quantitative Biology (Molecular Biology of Homo sapiens) 51: 67-74 (1986).

86. J.L. Strominger. Human major histocompatibility complex genes: Class 1 antigens and tumor necrosis factors. Cold Spring Harbor Symopsia on Quantitative Biology (Molecular Biology of Homo sapiens) 51: 63-66 (1986).

87. G. Vassart, M. Georges, R. Monsieur, H. Brocas, A.S. Lequarre and D. Christophe. A sequence in M13 phage detects hypervariable minisatellites in human and animal DNA. Science 235: 683-684 (1987).

88. P. Newmark. Dispute over who should do DNA fingerprinting in murder hunt. Nature 325: 97 (1987).

Table 1

Genome Size of Various Organisms and the Discrimination Required to Search for a Single Gene

Organism Genome	Genome Size (kb)	Single Gene Copies per Genome
Virus		
Polyoma/SV40	5.1	1:5.1
λ Phage	48.6	1:48.6
Vaccinia	190	1:190
Bacteria		
Mycoplasma	760	1:760
E. coli	4,000	1:4,000
Eukaryotes		
Yeast	13,500	1:13,500
Drosophila	165,000	1:165,000
Human	2,900,000	1:2,900,000

a. Calculated in kilobases where 1 kilobase (kb) equals 1000 base pairs (bp).

b. Calculated by assuming a one gene-one protein hypothesis and a protein or subunit composition of 300 amino acids. This would require that the gene be 1 kb in size.

Table 2

Steps Required in Implementing DNA
DNA Fingerprinting Analysis

1. Sample Retrival/Storage

2. Sample Preparation/Handling

   a. Restriction Enzyme Choice

   b. Immobilization Membrane Choice

   c. DNA Probe Choice

3. Data Collection/Analysis/Presentation

Table 3

Restriction Enzymes used in DNA Fingerprinting Analysis

Enzyme	Microbial Source
Alu I 5' AG↓CT 3' TC↑GA	Arthrobacter luteus
Eco RI GA↓ATTC CTT AAG↑	Escherichia coli RY13
Hae III GG↓CC CC↑GG	Haemophilus aegyptius
Hinf I G↓ANTC CTNA↑G	Haemophilus influenzae R_f
Mbo I ↓GATC GTAG↑	Moraxella bovis
Msp I C↓CGG GCC↑C	Moraxella sp.
Taq I T↓CGA AGC↑T	Thermus aquaticus YT1
Dra I TTT↓AAA AAA↑TTT	Deinococcus radiophilus
ScrF I CC↓NGG GGN↑CC	Streptococcus cremoris F

Table 4

Factors Influencing the Cost of Implementing a DNA Fingerprinting Service

Physical Plant	-	photographic darkroom
	-	radiochemical lab
	-	fumehoods
Equipment	-	electrophoretic
	-	radiochemical detection
	-	storage freezers
Operating Costs	-	radiochemical supplies
	-	biochemical supplies (enzymes, probes)
	-	membrane transfer products
	-	electrophoretic supplies (agarose)
Salary Costs	-	personnel
		-Ph.D. level
		-Technical level

Figure Captions

Fig. 1. Handling DNA - Preparation of DNA for Hybridization - Southern Transfer.

Fig. 2. DNA Strand Separation and Hybridization Monitoring by Changes in the Ultraviolet Absorption Spectrum.

Fig. 3. Radiolabelling DNA. Phosphate (A) and Nucleotide (B) Additions.

Fig. 4. RFLP Banding Patterns Resulting from Loss, Shift or Gain of Restriction Enzyme Cleavage Site. Single (A) and double probe (B) site binding.

Fig. 5. RFLP Banding Patterns Resulting from Restriction Enzyme Cleavage within the Probed Sequence.

Fig. 6. Producing the Minisatellite Probe from the Myoglobin Gene (45).

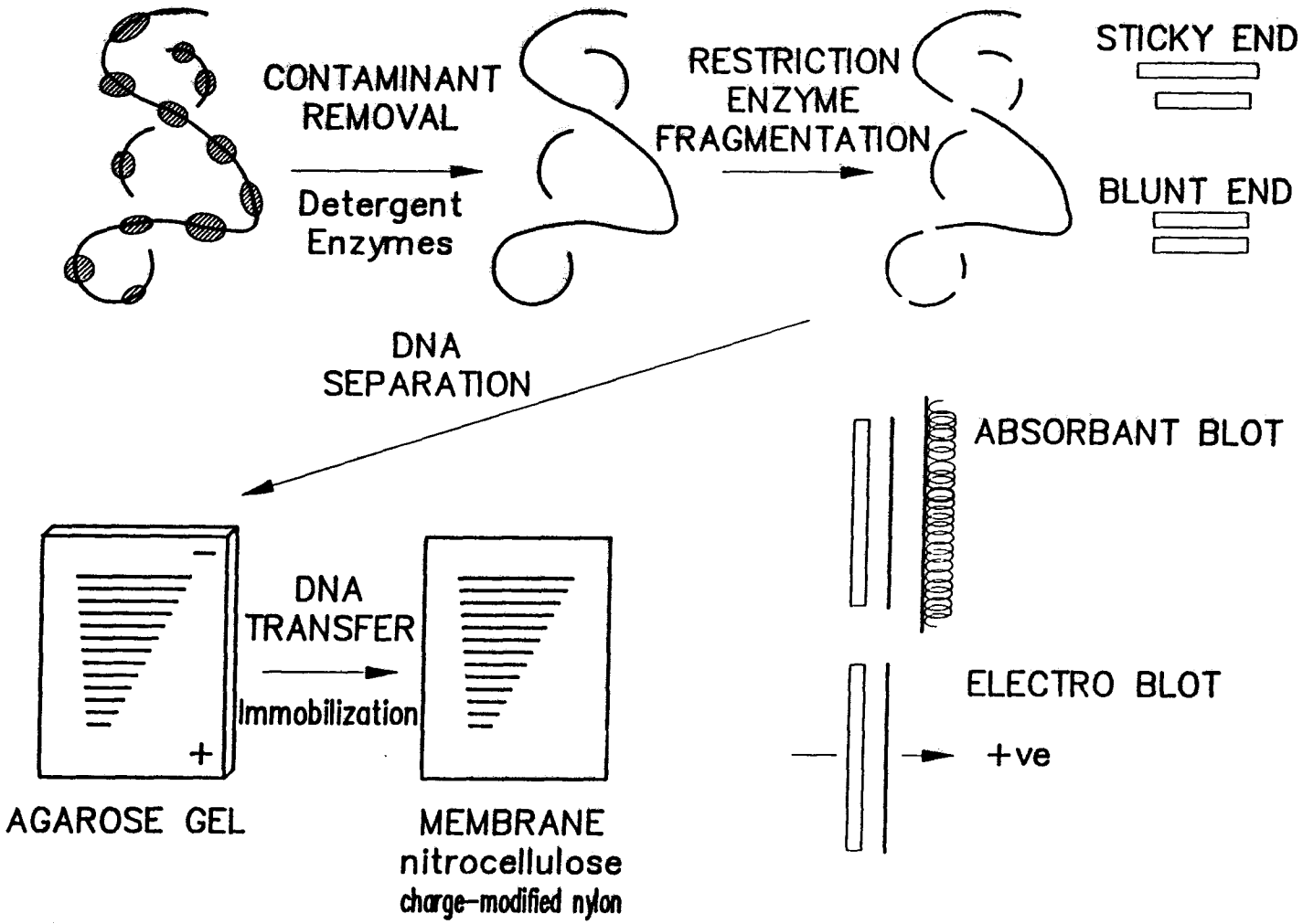
Fig. 7. DNA Fingerprinting using a Minisatellite Probe. Southern blot analysis of human genomic DNA isolated from blood was conducted as follows: restriction enzymes Hinf I and ScrF I were used separately and in

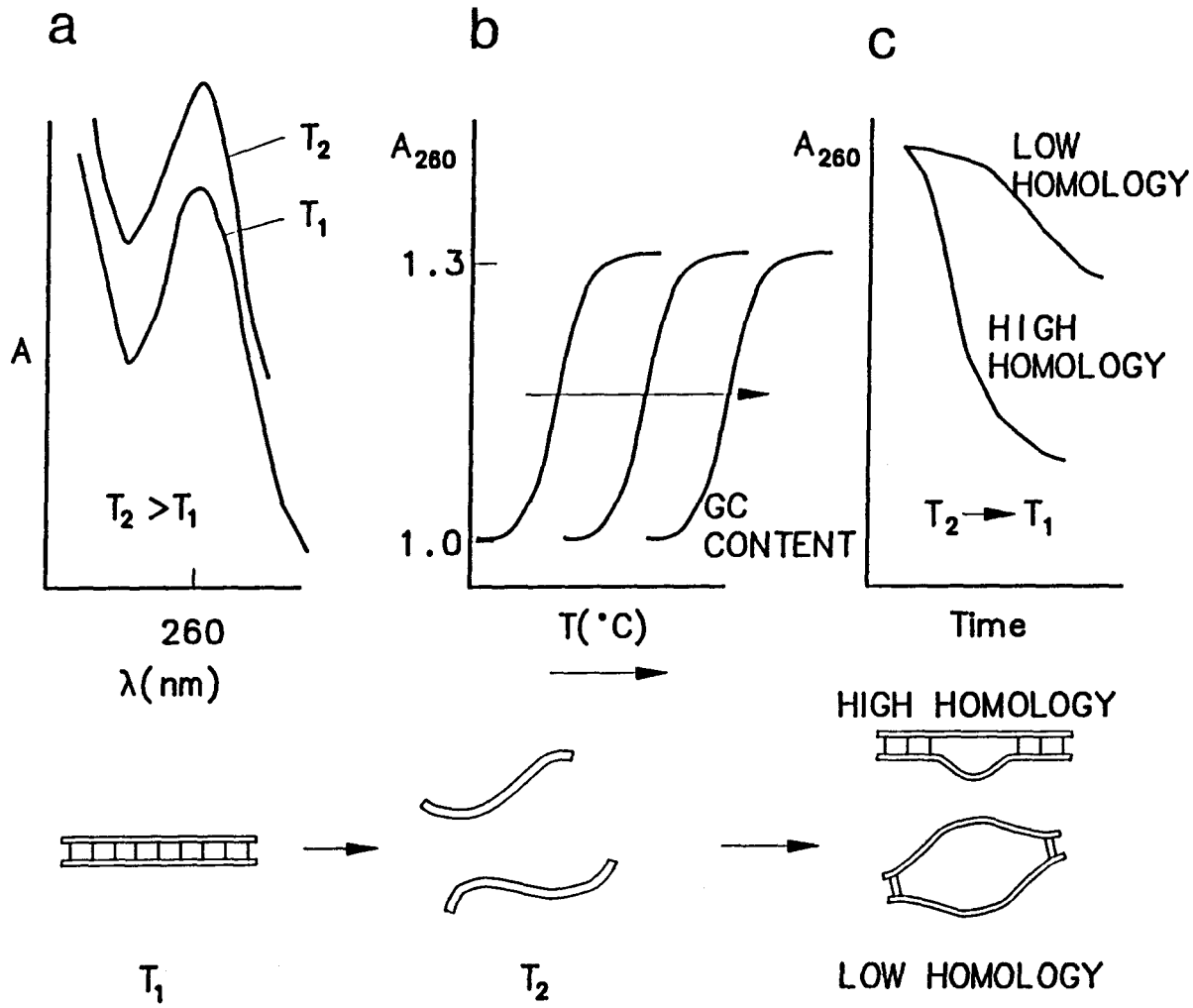
combination with Dra I to digest 2 micrograms of DNA from 3 individuals. The digests were separated by electrophoresis in an agarose gel, blotted onto a nitrocellulose filter, and hybridized with a ^{32}P-labeled, oligonucleotide "minisatellite" probe (kindly supplied by Dr. Peter Duck, Meiogenics, Ottawa, Canada). Washing under relatively stringent conditions revealed a highly polymorphic DNA "Fingerprint" pattern.

Fig. 8. Sex Typing with the 94f Probe. Family pedigrees are illustrated using Southern blot analysis of human genomic DNA isolated from blood. The restriction enzyme Taq I was used to digest 2 micrograms of DNA from family individuals. The digests were separated by electrophoresis in an agarose gel, blotted onto a nitrocellulose filter, and hybridized with a ^{32}P-labeled Y chromosome specific DNA probe 49f (kindly supplied by Dr. Jean Weissenbach, Institut Pasteur, France). Following a similar protocol to Ngo et al. (Am. J. Hum. Genet. 38: 407-418 (1986)) a male specific DNA "Fingerprinting" pattern was observed . In the pedigree fathers ( ) and sons ( ) have identical patterns while mothers (o) and daughters (o) show only 1 common band.

Fig. 9. Nonradioactive, Enzyme-based Labelling and Detection of DNA Hybrids (71,75).

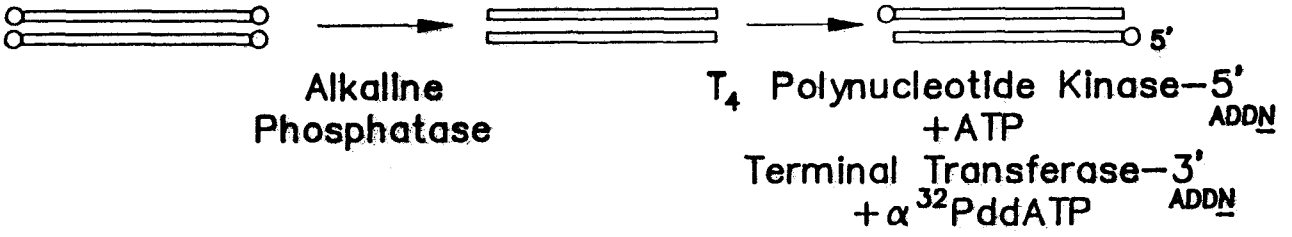
Fig. 10. Enzymatic Template Amplification. The polymerase chain reaction (78,79).


CONTAMINANT
REMOVAL
Detergent
Enzymes
RESTRICTION
ENZYME
FRAGMENTATION
STICKY END
BLUNT END
DNA
SEPARATION
ABSORBANT BLOT
DNA
TRANSFER
Immobilization
ELECTRO BLOT
+ve
AGAROSE GEL
MEMBRANE
nitrocellulose
charge-modified nylon

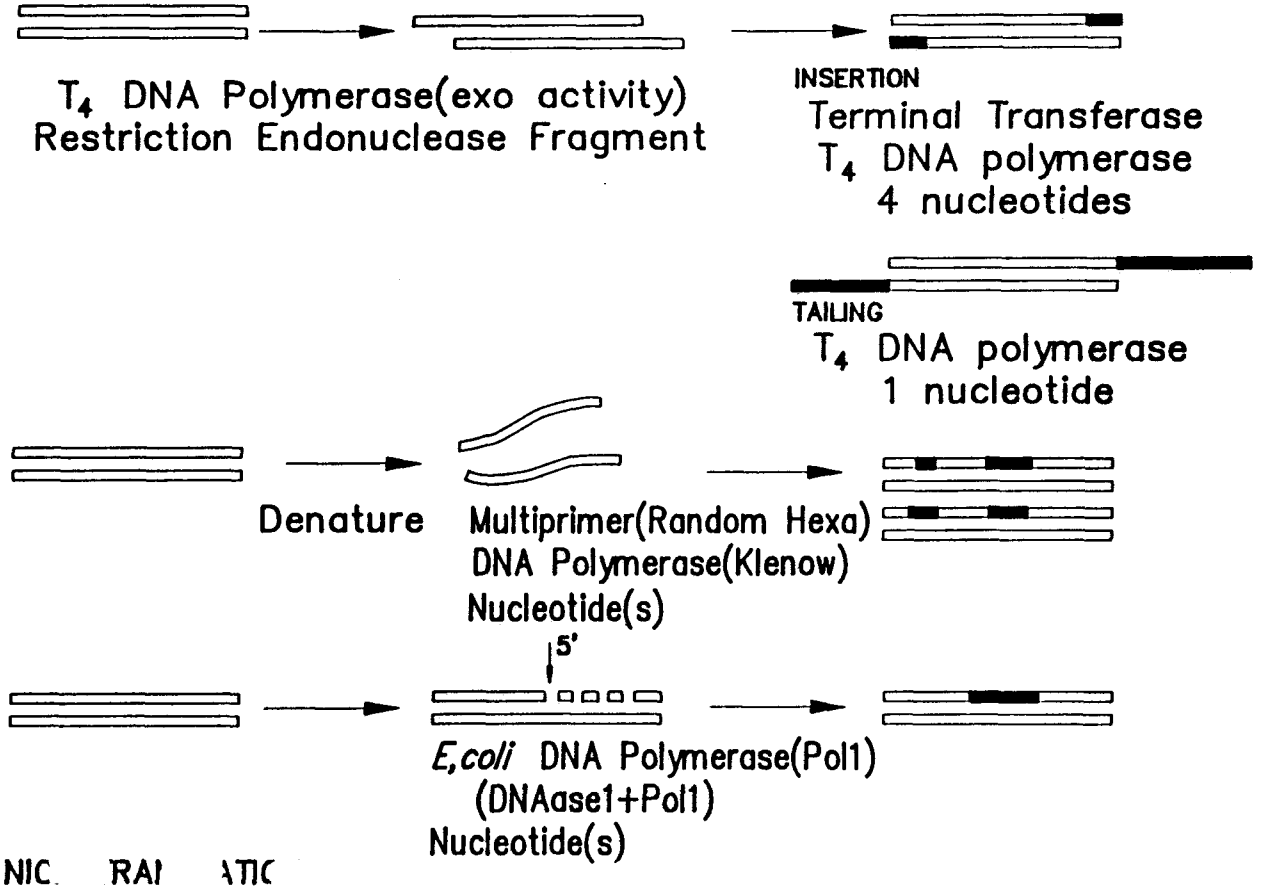

a
b
c
A
T_2
T_1
$T_2 > T_1$
260
λ(nm)
A_{260}
1.3
1.0
GC
CONTENT
T(°C)
A_{260}
LOW
HOMOLOGY
HIGH
HOMOLOGY
$T_2 \rightarrow T_1$
Time
HIGH HOMOLOGY
T_1
T_2
LOW HOMOLOGY

RADIOLABELLING DNA

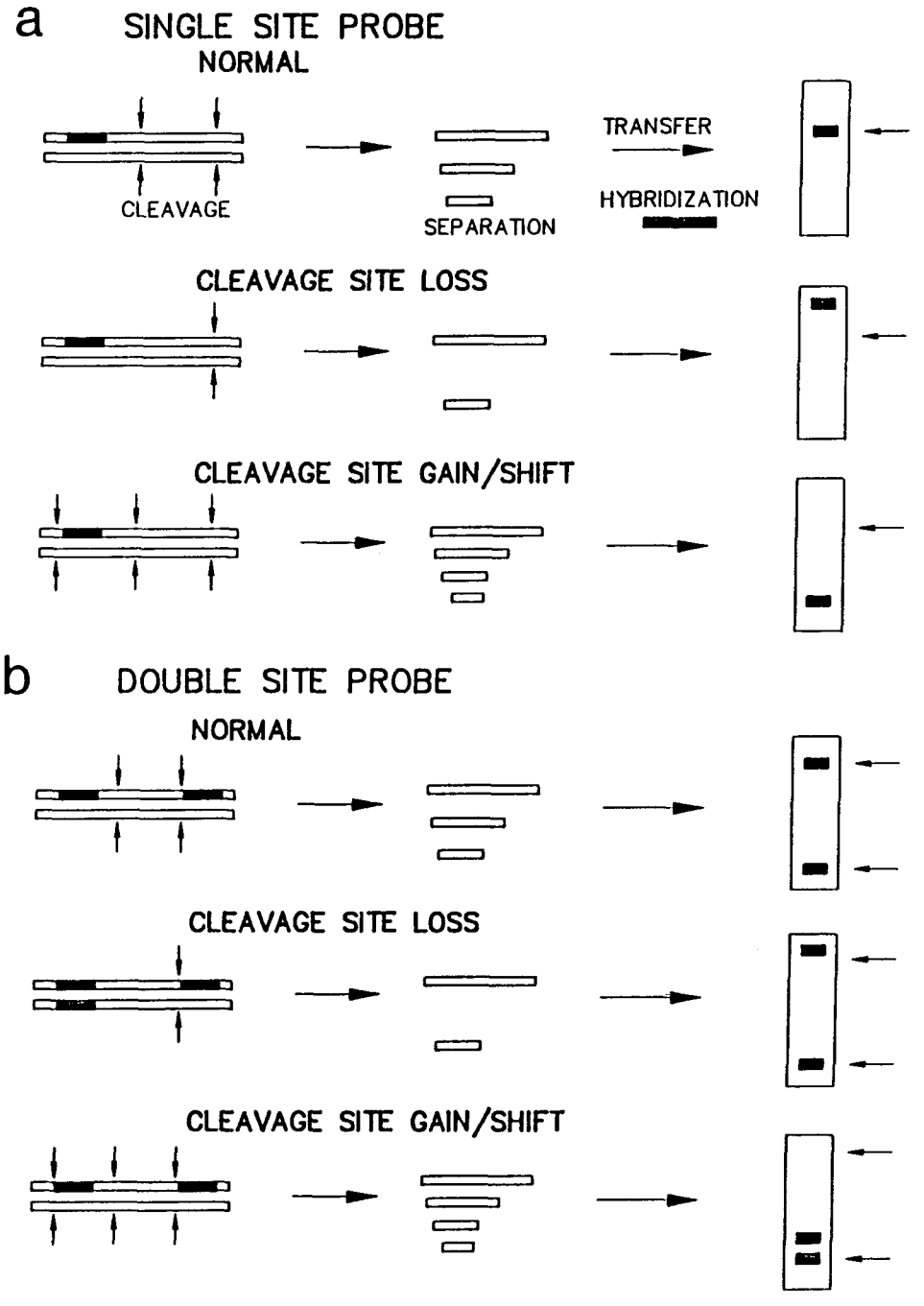
A. Phosphate Addition



B. Nucleotide Addition



NIC RAI ATIC



DR. WILLIAMS HIA 1290-4

16mer

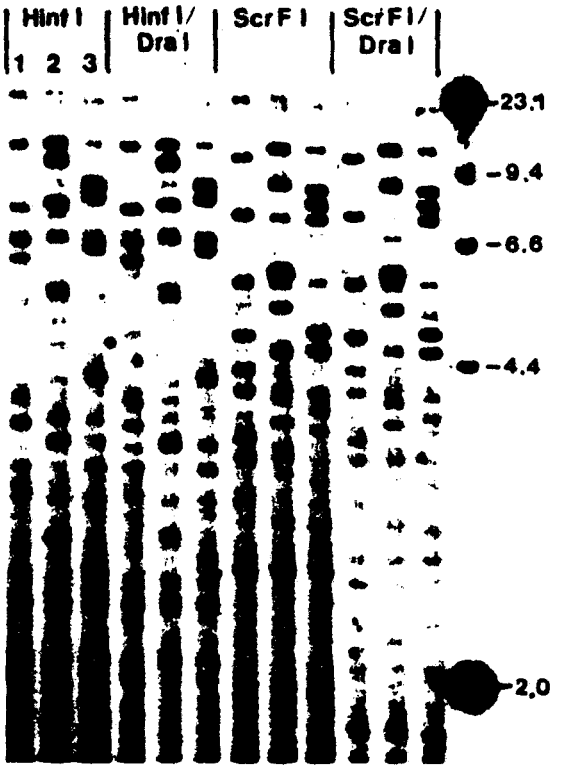


Figure. Southern blot analysis of human genomic DNA isolated from blood was conducted as follow. Restriction enzymes Hinf I and ScrF I were used separately and in combination with Dra I to digest 2 micrograms of DNA from 3 individuals. The digests were separated by electrophoresis in an agarose gel, blotted onto a nitrocellulose filter, and hybridized with a ^{32}p-labeled, oligonucleotide "minisatellite" probe (Kindly supplied by Dr. Peter Duck, Meiogenics, Ottawa, Canada). Washing under relatively stringent conditions revealed a highly polymorphic DNA "Fingerprint" pattern.

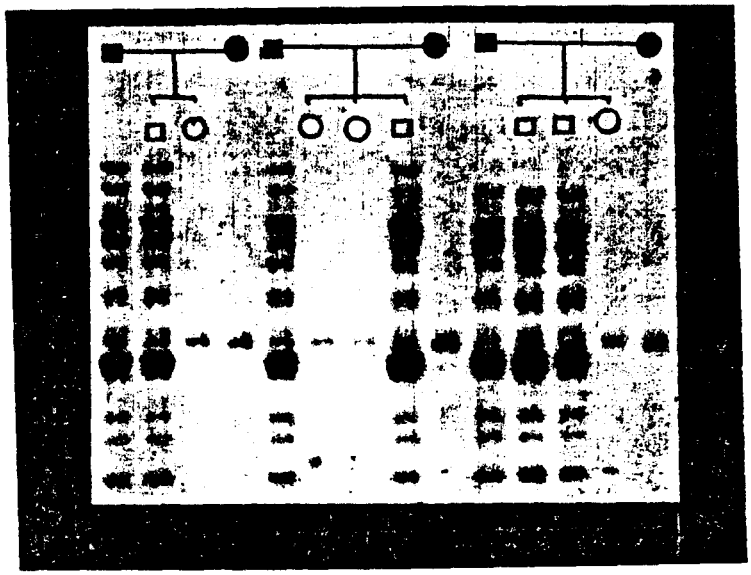
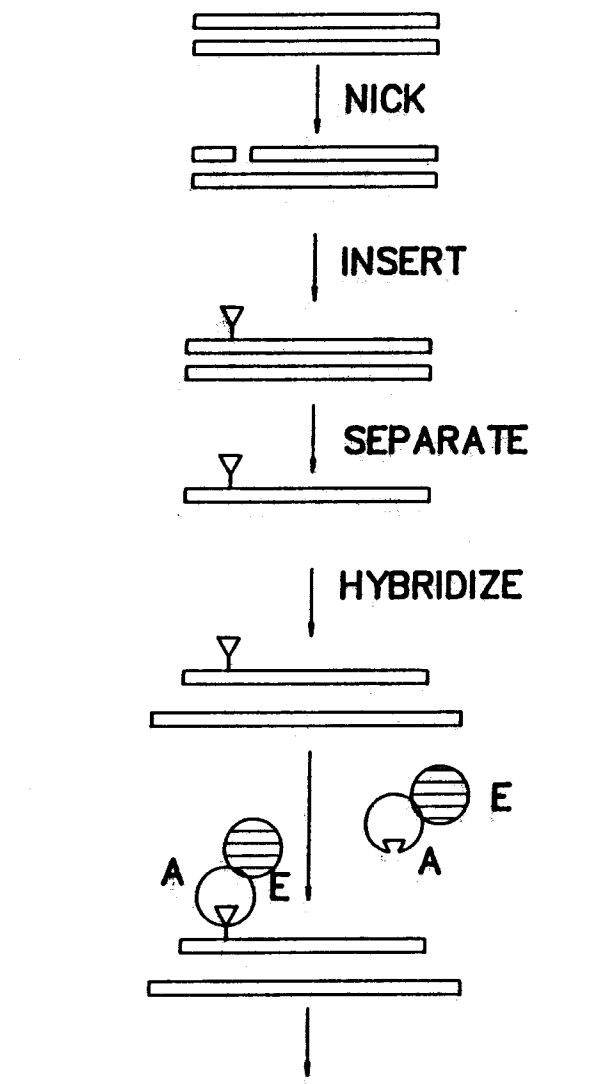
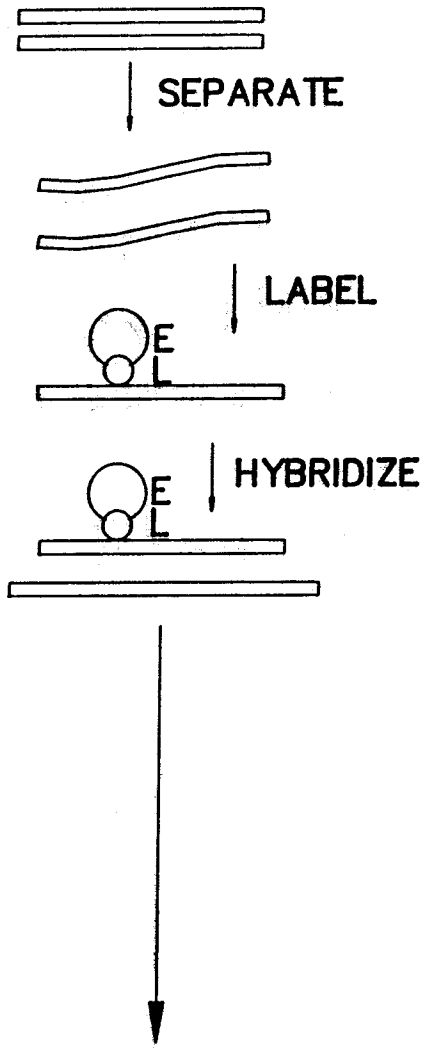


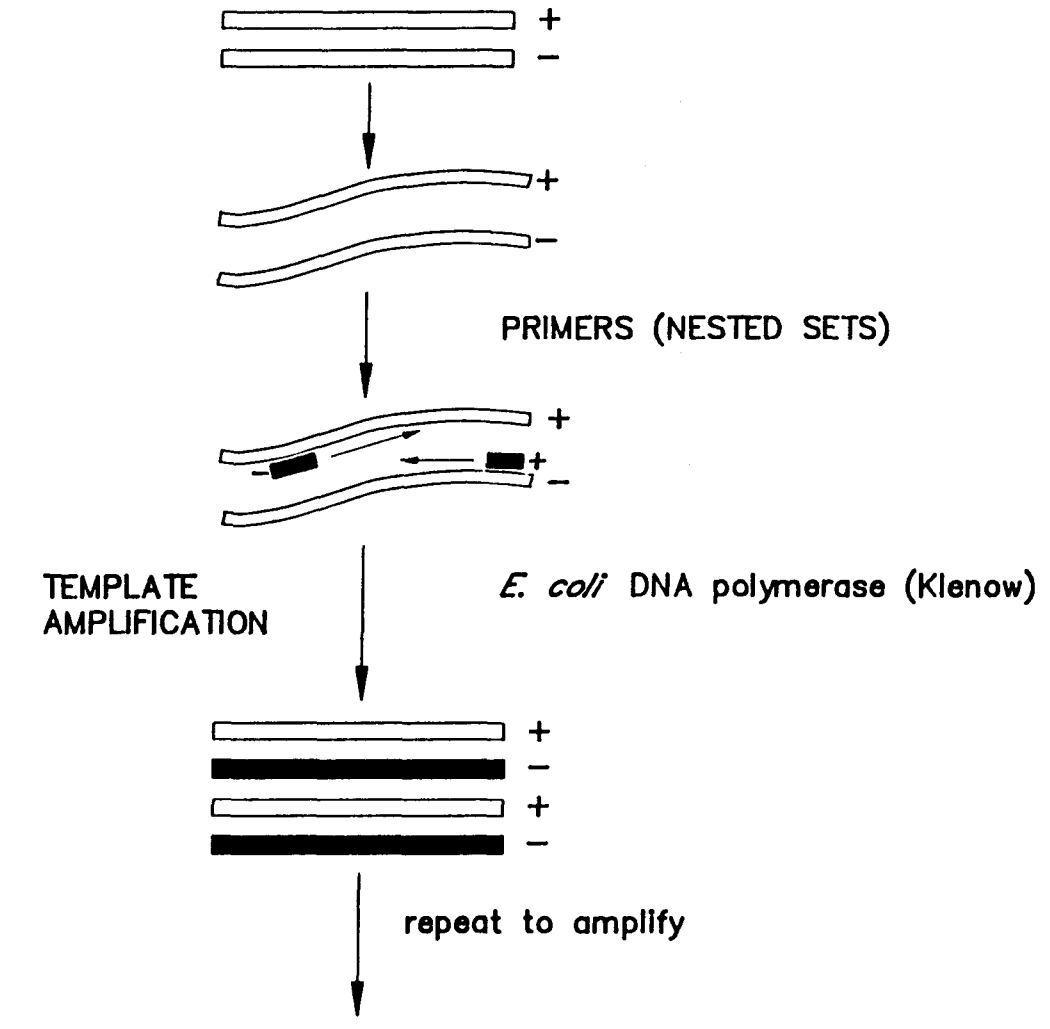
Figure . Family pedigrees are illustrated using Southern blot analysis of human genomic DNA isolated from blood. The restriction enzyme Taq I was used to digest 2 micrograms of DNA from family individuals. The digests were separated by electrophoresis in an agarose gel, blotted onto a nitrocellulose filter, and hybridized with a ^{32}P-labeled Y chromosome specific DNA probe 49f (kindly supplied by Dr. Jean Weissenbach, Institut Pasteur, France). Following a similar protocol to Ngo et al (Am. J. Hum. Genet. 38, 407-418, 1986) a male specific DNA "Fingerprinting" pattern was observed. In the pedigree fathers (■) and sons (□) have identical patterns while mothers (●) and daughters (○) show only 1 common band.

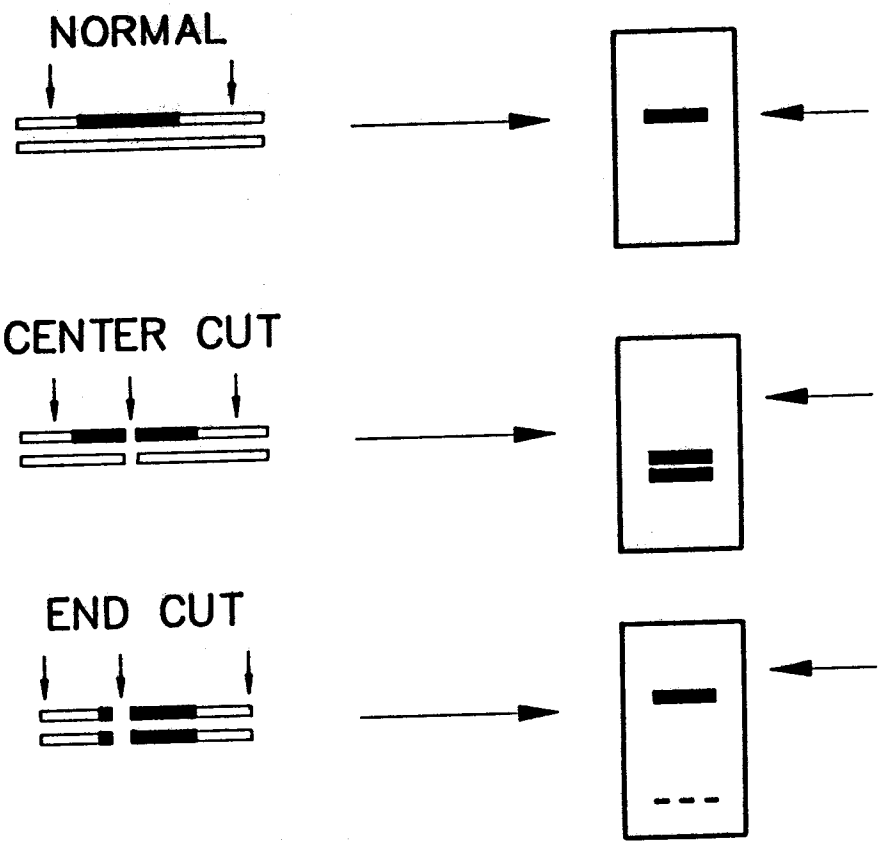


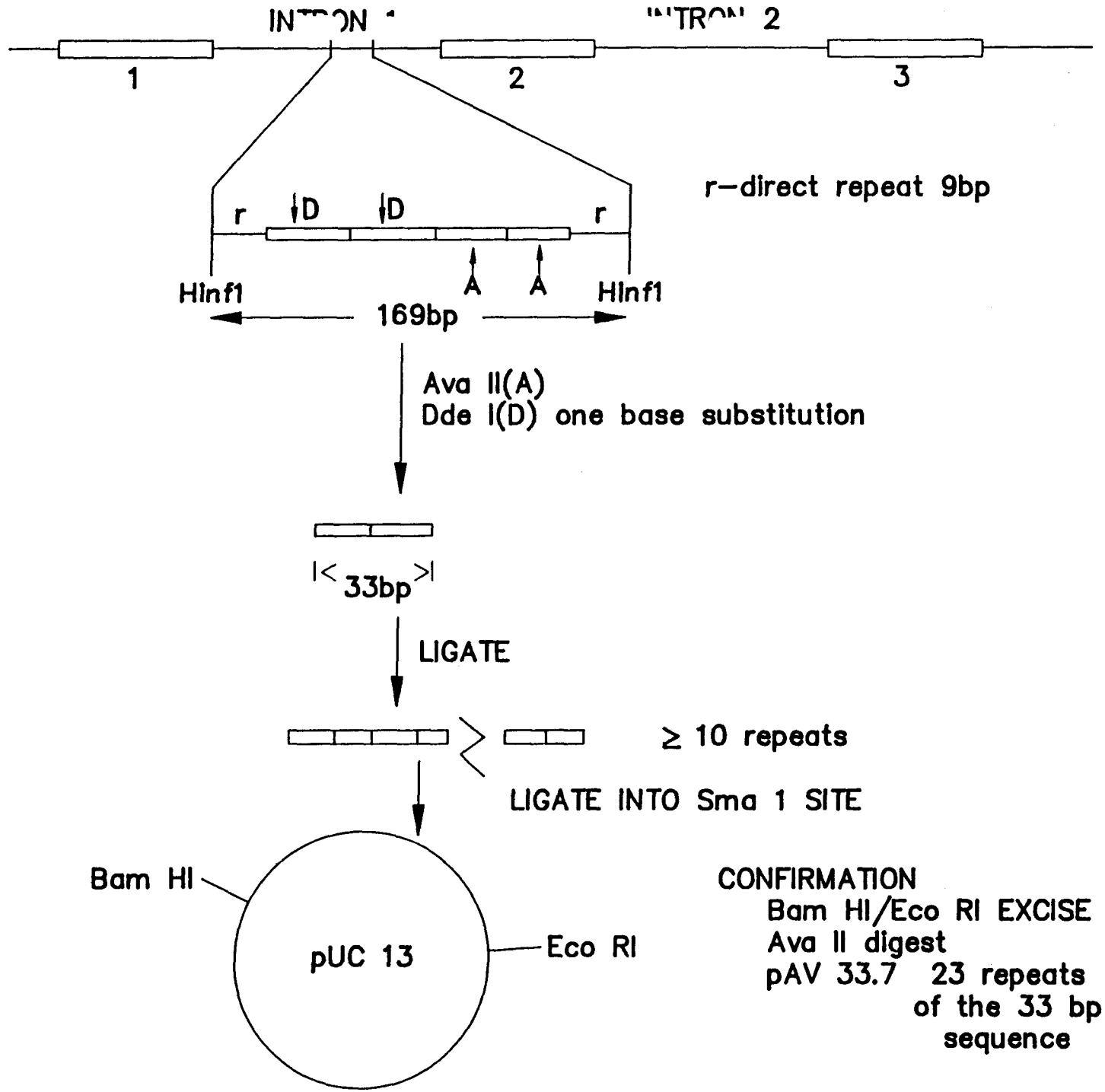
BIOTIN(▽)–AVIDIN(A)–ENZYME(E)
DEVELOPMENT



ENZYME(E)–LINKER(L)
DEVELOPMENT


+
−
+
−
PRIMERS (NESTED SETS)
+
+
−
TEMPLATE
AMPLIFICATION
E. coli DNA polymerase (Klenow)
+
−
+
−
repeat to amplify
POLYMERASE CHAIN REACTION (PCR)


NORMAL
CENTER CUT
END CUT


INTRON 2
1
2
3
r-direct repeat 9bp
r
D
D
r
A
A
HInf1
HInf1
169bp
Ava II(A)
Dde I(D) one base substitution
33bp
LIGATE
≥ 10 repeats
LIGATE INTO Sma 1 SITE
Bam HI
pUC 13
Eco RI
CONFIRMATION
Bam HI/Eco RI EXCISE
Ava II digest
pAV 33.7 23 repeats
of the 33 bp
sequence

INDIVIDUAL IDENTIFICATION BY HYPERVARIABLE REPETITIVE REGIONS OF HUMAN DNA . EXPERIENCES OF THE INSTITUTE OF LEGAL MEDICINE IN GENOA. ***

Giacomo CANEPA *

Francesco DE STEFANO **

---

* Director of the Institute of Legal Medicine and of the Internatinal Centre for Clinical Criminology, University of Genoa (Italy). President of the International Society of Criminology.

** Assistant at the Institute of Legal Medicine, University of Genoa.

*** Report to the 38° International Course in Criminilogy - Montréal (Canada), August 17-21, 1987.
The work was funded by Ministry of Education (40%) within a plan of National prominent interest.

Introduction

The problems of individual identification from the forensic haemogeneticist's point of view are concerned with theoretical approach and practical application of the techniques in paternity testing and investigations on stains, because of their great importance in solving many cases of social and human significance.

From the first discoveries of blood groups (1-3) an ever increasing amount of proteins in forensic laboratories has been used with the object of reaching individual identification of stains or paternity.

But in spite of higher and higher chances of better detection,the certainty of exclusion was never overlooked; positive identification in this field being nothing more than an estimate of greater or less probability. It is in fact impossible to indicate with certainty the origin of a blooodstain or the paternity of a putative father and only in the field of exclusion, from first observation of a double one (4) have many steps been taken.

INDIVIDUAL IDENTIFICATION

a) Polymorphic proteins

As was previously remarked , individual identification of blood or semen stains or organic tissues represents one of the most important aspects of forensic laboratory work.

When in the early 20th century Landsteiner discovered blood groups in the ABO system (1), and with Levine conducted new important investigations in this field (2,3), the existence of an "individuality of blood" by identification of blood group antigens was supposed.

In spite of numerous investigations and subsequent discoveries it soon became clear that individuality remained a distant prospect, and this was even more the case with tests on blood or semen stains and individual identification of organic tissues.

From Landsteiner's first studies many steps, of course have been taken and much more about the peculiarity of red cell surface, anzymes, serum proteins and HLA has become known.

Only a few of these proteins (better known as "genetic markers") of some usefulness may be considered in testing blood or semen stains or fresh semen.

In fact, for identifying bloodstains a few blood group marker systems and polymorphic proteins (ABO, Rh, Gm and few enzymes) may be investigated only if the stain is big enough

and no more than a few weeks old. It is in fact well known that proteins are highly unstable and easily run up against denaturation and degrading because of ageing and by the operation of chemical or physical agents (5). We must furthermore bear in mind that erroneous results may be produced by bacterial activity, particularly in ABO detection (6).

As far as identification of genetic markers in semen is concerned, they are reduced due to the action of proteolityc enzymes (7) and at present only four or five systems are in common use. In every case considerable caution must be used because analysed samples may be contaminated (8) and the individual property to be a secretor or a non-secretor of ABH substances in body fluids must be checked.

It is therefore clear that there are many problems pertinent to individual identification through investigations on red cell surface antigens, enzymes, serum proteins and, where possible, on white cells surface antigens.

On the other hand, even in the fortunate case of detection of a rare protein the study of blood group genetic markers can give us no more than an answer in the field of "probable" or "highly probable"; because it is impossible to reach a positive individual identification by performing these tests and we can only be informed about the consistency of genetic markers in stains with those of

the suspects or victims.

It is appropriate, in supporting this assertion, to underline that only a small percentage of the human genome will be expressed as proteins more or less easily identifiable.

b)DNA polymorphisms - Personal observations

In forensic laboratories today many techniques are used, peculiar to human genetics which give a great deal of information directed to obtaining a positive indivdual identification of stains by detection of Restriction Fragment Length Polymorphisms (RFLPs).

Nevertheless RFLPs are only minimally informative because of their prevalling dimorphism and it might be necessary to use a great deal of restriction enzymes and as many DNA probes in order to obtain individual identification.

Since Jeffreys et al. (9) described a 33-base pair sequence from an intron of the human myoglobin gene able to detect repetitive and hypervariable regions of the human genome (hypervariable minisatellite regions), the chances of reaching individual identification have been greatly improved. These minisatellites, in fact are highly polymorphic and able to ensure a positive identification by means of peculiar molecular probes.

These probes are short DNA known sequences able to link the fragment with the complementary sequence. Jeffreys' probes are characterized by a sequence of bases called "core region" , which is repeated a variable number of times in every single fragment, so determining the different length of the variable fragments. By means of a restriction endonuclease (Hinf I), which is an enzyme able to cut the double helix in precise sites where there exists a specific known sequence and not inside the "core region", it is possible to separate and detect variable fragments by electrophoresis in agarose gel, hybridization and autoradiography.

In this way it is possible to detect at one time many restriction fragments of variable length.

The two probes (lambda 33.15 and 33.6) can identify hypervariable regions of the genome and ensure, as we remarked before a degree of individual identification which can approach certainty; it has been calculated, in fact that the probability of chance association using probe 33.15 is less than 3×10^{-11}, and if two probes are used the probability is lower than 5×10^{-19}(10).

On the other hand, DNA remains stable in spite of ageing and results can be easily reproduced and checked, even after many times.

These characteristics render the method particularly useful for forensic purposes (11, 12).

Experiments carried out in our laboratory, in collaboration with geneticists of the University of Genoa, first of all allow us to confirm the accuracy and reproducibility of this technique both for the identification of bloodstains and semen stains or fresh semen.

It is important to stress the fact that in our laboratory it has been possible to recover DNA, useful for investigation, from haemolyzed cadaveric blood, dried blood on Petri dish and blood stained cloth; DNA has been recovered too from bloodstain of 40 µl equivalent of fresh blood (12) .

The results can easily be distinguished because we must only confront the patterns of bands with a view to checking their identity, as for fingerprints .

As we said before, the main characteristic of DNA is its extreme stability; and this peculiarity has been experimentally confirmed. Furthermore, no cases of recombination at a somatic level appeared, thus confirming the stability of the hypervariable regions .

In practice this method has been used in cases of rape to identify blood or semen stains on the rapist's or victim's clothes or in cases of murder or attempted murder.

On this view,it may be useful to underline that sometimes we cannot be sure that stains have a human origin. In this case detection of hypervariable repetitive regions of the genome could not be suitable for species identification (Personal observations, data not shown). Therefore, before recovering DNA from the stain in such a case it will be better to elute proteins and match them with antisera for species identification.

CONCLUSIONS

Our experience in the field of individual identification by hypervariable repetitive regions of the human DNA can confirm the experimental data shown by Jeffreys et al. (10) and Gill et al. (11).

It is therefore possible today, by means of investigations of DNA polymorphisms to reach positive solutions to many of the daily problems in forensic laboratory work concerned with individual identification of blood or semen stains. And new polymorphisms are today detectable by means of other molecular DNA probes complementary to other hypervariable regions of the human genome (13-16).

On the other hand, as previously mentioned with the investigations of proteins many difficulties arise which may reduce the accuracy of tests. And here we can remember that some of the aglutination tests may be distorted by subjective interpretation of the results.

Furthermore, many proteic groups are not detectable in stains because of ageing or action of proteolytic agents.

Investigations on DNA polymorphisms may overcome all these difficulties due to ageing or subjectivity because of genome stability and direct detection of bands pattern.

We conclude by saying that these methods will allow us to reach "individuality of blood" pursued from the first discoveries of blood groups.

REFERENCES

1) **Landsteiner K.:** Uber Agglutinationserscheinungen normales menschlichen Blutes. Wien. Klin. Wschr. 14, 1132, 1901.

2) **Landsteiner K., Levine P.:** A new agglutinable factor differentiating individual human bloods. Proc. Soc. exp. Biol. (N.Y.) 24, 600, 1927.

3) **Landsteiner K., Levine P.:** Further observations on individual differences of human blood. Proc. Soc. exp. Biol. (N.Y.) 24, 941, 1927.

4) **Canepa G.:** Double Exclusion of Paternity by the ABO and MN Systems. J. Forens. Sci. 7, 520, 1962.

5) **Denault G.C., Takimoto H.H., Kwan Q.Y., Pallos A.:** Detectability of Selected Genetic Markers in Dried Blood on Aging. J. Forens. Sci. 25, 479, 1980.

6) **Davies A., Lincoln P.J., Martin P.:** Aberrent group B reactions detected in mixtures of semen and vaginal secretions possibly due to acquired B. Forens. Sci. Int. 25, 201, 1984.

7) **Blake E.T., Sensabaugh G.F.:** Gentic Markers in Human Semen: A Review. J. Forens. Sci. 21, 784, 1976.

8) **Sensabaugh G.F., Blake E.T., Northey D.H.:** Genrtic Markers in Semen. III: Alteration of Phosphoglucomutase Isozyme Patterns in Semen Contaminated with Saliva. J. Forens. Sci. 25, 470, 1980.

9) **Jeffreys A.J., Wilson V., Thein S.L.:** Hypervariable "minisatellite" regions in human DNA. Nature 314, 67, 1985.

10) **Jeffreys A.J., Wilson V., Thein S.L.:** Individual-specific "fingerprints" of human DNA. Nature 316, 76, 1985.

11) **Gill P., Jeffreys A.J., Werrett D.J.:** Forensic application of DNA "fingerprints". Nature 318, 577, 1985.

12) **Coviello D.A., De Stefano F., Origone P., Politi M.:** Applicazioni medico-legali di recenti metodologie di indagine sul patrimonio genetico umano. Min. Med. Leg., in press, 1986

13) **Knowlton R.G., Brown V.A., Braman J.C., Barcher D., Schumm J.W., Murray C., Takvorian T., Ritz J., Donis-Keller H.:** Use of Highly Polymorphic DNA Probes for Genetypic Analysis Following Bone Marrow Transplantation. Blood 68, 378, 1986.

14) **Ali S., Mueller C.R., Epplen J.T.:** DNA finger printing by oligonucleotide probes specific for simple repeats. Hum. Genet. 74, 239, 1986.

15) **Vassart G., Georges M., Monsieur R., Brocas H., Lequarre A.S., Christophe D.:** A Sequences in M13 Phage Detects Hypervariable Minisatellites in Human and Animal DNA. Science 235, 683, 1987.

16) **Nakamura Y., Leppert M., O'Connel P., Wolff R., Holm T., Culver M., Martin C., Fujimoto E., Hoff M., Kumlin E., White R.:** Variable Number of Tandem Repeat (VNTR) Markers for Human Gene Mapping. Science 235, 1616, 1987.

QUATRIEME PARTIE

PART IV

TRAITEMENT DE L'INFORMATIQUE SUR LES CRIMES ET LES CRIMINELS

CRIME ANALYSIS SOFTWARES AND MODUS OPERANDI SEARCH

Session 3.1 Crime Analysis Software and M.O. Search
GRASS (Geographic Resource Allocation Software System).

Introduction

by: M.J.G. ARNOLD, Public Security Program

The application of computers in the Canadian Police Community had its' beginnings in the sixties with the implementation of the C.P.I.C. (Canadian Police Information Centre) network. This introduction to the world of computers for the law enforcement community was followed by a gap of about ten years, to the middle seventies where municipal police agencies started to implement their own in-house computer systems. These computer systems were best described as CADRE(computer-aided dispatch and record entry systems.)

By the year 1990 most major municipal police forces will have in place their own versions of CADRE. Interestingly enough the traditional order of these implementations was first the paper records system computerization followed by the CAD component for the dispatching function with the final stage being the implementation of MDTs (mobile data terminals) in the patrol cars. Throughout this implementation process the local police force learned much in the way of computers and how they apply to their day to day activities. Senior police management on their part began to appreciate the impact of such systems on their department and as a result re-structured areas within their departments to handle this impact.

This paper addresses a small but significant area in the interpretation of the vast amount of data in the terms of crime analysis and more significantly resource allocation. Although these two functions can be administered separately from an organizational perspective they both rely on the same computer database.

Background

Around 1970, a small group of NRC researchers (Arnold and Lipsett) discovered that, from the Canadian perspective, there was a void in applied fundamental police research. As a starting point they looked at the use of computers in police work. They implemented a patrol car simulation obtained from Larson, from MIT on the NRC central computer facility. This simulation model was used to perform operational research analysis for the Gloucester Police Force, in Ontario, the RCMP in Burnaby, B.C. and the RCMP Red Deer rural detachment in Alberta. This research contained the following key elements:

- A methodology of dividing a city's geography into reporting areas ("atoms") for the use of classifying where the call for service (CFS) were originating.

- A method of analyzing CFS information in order to redefine patrol car zones to meet present workloads.

About the same time that the simulation work was going on there was model building activity going on in the United States. It was during this time that Chaiken's "Patrol Car Allocation Model" and the Chelst/Larson "Hypercube Model" were being tested and evaluated. About the same time Heller from St. Louis was developing computer scheduling algorithms for the patrol division of a police department.

The NRC research team developed their own approach to data preparation for the computer simulation. It was soon apparent that from he police point of view the most interesting aspect of the simulations was the analysis of calls for service information. The interest was so high that the researchers developed a workshop on patrol car allocation which was presented to the Executive Development course at the Canadian Police College in Ottawa.

Laboratory Development

The focus now shifted from simulation to analysis of calls for service. As the team developed analysis techniques it became clear that the number crunching which generated the basic data for the analysis produced paper output which was lengthy, cumbersome and confusing. It was also during this period that the police were starting to install record systems which generated vast amount of reports which were also very confusing.

A technique which was developed from the simulations was the refinement of mapping techniques which started from a rough line printer generated maps and progressed through to a computer plotted maps. It was soon discovered that when the Chief of Police looked at a colored atom map of his municipality in red, yellow and green that it did not take to much explaination on what the map was indicating. Finally a name change of the NRC section from Data Systems to Computer Graphics reinforced the teams approach to police data.

About 1976 the whole project focus changed. Models and simulations were out (only the researchers understood them anyway) and a computer mapping and analysis were in. The Ottawa Police department furnished the research team a magnetic tape with over 10,000 calls for service. The concept of utilization time was used to denote how much actual time a police car spent servicing citizen's calls for assistance as opposed to displaying only number of calls for service.

Charts

An important aspect of depicting the analysis results was in the form of bar charts, line graphs and pie charts. All of these combinations were developed to draw pictures with the police data.

Another important feature that developed was a series of codes (about 100) describing what the call for service actually was. The proto-type worked on an atom map which was digitized into readible computer records. The raw data had an atom number which was attached to every record. The addition of this seemingly small item took the researchers a lot of preparation time. By 1977 the second version of the proto-type system was working in the laboratories on a DEC 11/55 computer.

The team also addressed another major issue - where to obtain the electronic map. Does one make their own map and maintain and update it? Or is there another simple process of getting a computer map for the local police department.

They looked at simple street maps, maps from Energy Mines and Resources, postal code maps, municipal maps and Statistics Canada maps. Out of all of them it appeared that Statistics Canada's area master files or AMF which are used for the compilation of census data was, at the time, the way to go. Statistics Canada have mapped every city in Canada of a population greater than 55,000 and have inherent in their AMF a street address to block face conversion. One of the most important reasons to use the Statistics Canada AMF was their willingness to regularly update the map and provide copies to the police at a reasonable cost. This assists them as well in having the most up to date geographical information. Although the AMF maps were not the ideal they were a good compromise.

Technology Transfer

The transfer to industry of a real application for an identified client may seem like an easy task. In this instance it wasn't. In 1978 negotiations with a small company collapsed when several key people left the company. **-strike one.**

A second company was contacted about a year and a half later. They were funded to show police how a mapping system might function on their behalf. This was a very positive experience as it exposed the techniques to the police and, as well, established in the minds of the research/technology transfer team that there indeed was a marketable product. Unfortunately after the contract the company did not wish to carry the product to the market.
-strike two

In the summer of 1985 by accident both NRC and company 3 - ACDS Graphics Ltd. found one another. After some lengthy negotiations the GRASS project was initiated between the three parties, the Ottawa Police - who paid for the equipment, NRC who paid half the development costs and the company ACDS who contributed the other half of the development costs. The 12 month contract was put in place in July 1986.

Implementation - Ottawa Police

On July 7, 1987 a news release announced the GRASS development to the media and the police community. The system consists of a work station which includes a super micro, a high resolution display, an alphanumeric display, keyboard, digitizing tablet, plotter and line printer. (see figure 1 and 2).

The system essentially puts housebreakers, car thieves and armed robbers on the map. Crime analysts at police headquarters can call up city or neighborhood maps on the computer screen displaying whatever information they want - burglaries over the past 24 hours, cars stolen at a cetain time of day or sexual assaults in the past month. (see figure 3). Using the map and police records accessible through the terminal they can compare details right down to how and where the burglar broke in to what the armed robber was wearing.

Those details help analysts draw comparisons, spot trends and assist police in trying to catch offenders. The map can also act as a warning by highlighting certain crime areas.

As an operational tool it will help the officer coming on duty. He will be handed a map of his jurisdiction indicating where all crimes occured during the preceding 24 hours. The analysis of crimes such as burglary, armed robbery, auto theft and sexual assault often happen in a series and can be linked. The GRASS system will assist the police in deploying specialty teams very quickly. It's like putting a window on the police information contained in their record systems.

GRASS has the capacity to add tremendous detail including building layouts which could help in the event of a hostage situation.

The detailed application of this high tech tool are limited only by the users imagination. The original intent is only to down load the last 30 days of records for analysis, however it is possible to look at more data for planning and forecast purposes.

Future

The development and use of GRASS has only just begun. With release 2.0 where charts and graphs will be on line there will be continuing work to develope the system. The RCMP have a similar system called VICARS. The researchers are suggesting that there will be work on the merging of VICARS and GRASS to assist in major crime analysis.

From the research side both NRC and the police community hope to develope the system in line with advanced technologies such as artificial intelligence or expert systems where computers can be programmed to use the human's logic and problem solving skills.

It's the start of a major tool that police forces will use on a daily basis to solve both minor and major crime.

Bibliography

1. Arnold, J.G. and Lipsett, F.R. Computer simulation of patrol operations of a semi-rural police force. J. Police Sci., Admin. 2: pp. 190-207; 1974. NRC 14171.

2. Arnold, J.G. and Lipsett F.R. Simulation and analysis of the patrol operations of a semi-rural police force. Gloucester Township, near Ottawa. NRC/ERB-882, July 1974. 171 pages.

3. Arnold, J.G., Dalley, A.F. and Lipsett, F.R. Patrol operations of Burnaby RCMP detachment analysis and simulation. Complete Report. NRC/ERB-887, August 1975. 51 pages.

4. Arnold, J.G., Dalley, A.F. and Lipsett, F.R. Patrol operations of Red Deer rural RCMP detachment. NRC/ERB-892, November 1975. 13 pages.

5. Arnold, J.G. and Lipsett, F.R. Use of a computer for interactive mapping of crime. Third International Conference on Equipment for the Police, Ottawa. October 4-6, 1977.

6. Arnold, J.G., Lipsett, F.R. and Lyon, D.G. Workshop on patrol car allocation. Canadian Police College Executive Development Course 18, Ottawa. April 6, 1978. Also presented as part of CPC Executive Development Courses 19, 20 and 21, and at the Annual Meeting, Canadian Association of Chiefs of Police, Ottawa. August 28, 1978.

7. Arnold, J.G. Computer graphics and the police? Operational Research Society of America, Los Angeles, Calif. November 13, 1978.

8. Arnold, J.G. Making the most of your resources. A look at patrol car activity in a regional police department. NRC/ERB-917. July 1979. 100 pages.

9. Barrs, S. Science Against Crime Helping the Good Guys., Science Dimension - NRC, Volume 17, No. 3, 1985.

10. Chaiken, Jan M. Patrol Allocation Methodology for Police Departments, The New York Rand Institute, September, 1975.

11. Chelst, Kenneth R. "Hypercube Model - The Equity System: A Computer Aided Sector Design System with the enphasis on Equity", Wayne State University-College of Engineering, November 1978, Detroit, Michigan.

12. Dalley, A.F. Geographic Based Reference Files - A Utility for Police; RCMP, Ottawa, Ontario, June 1985.

13. Larson, R.C. Models for the Allocation of Urban Police Patrol Forces - Technical Report No. 44, Operations Research Center - Massachussetts Institute of Technology, November 1969.

14. MacKay, Sgt. D. Crime Analysis - The First Ten Years, Calgary Police Services R.C.M.P., Gazette, Volume 47, No. 11, 1985.

15. Watkin, J.E. and Lipsett, F.R., Editors. Proceedings of the Workshop on Mapping and Related Applications of Computer to Canadian Police Work, April 1977, National Research Council, Ottawa, Canada.

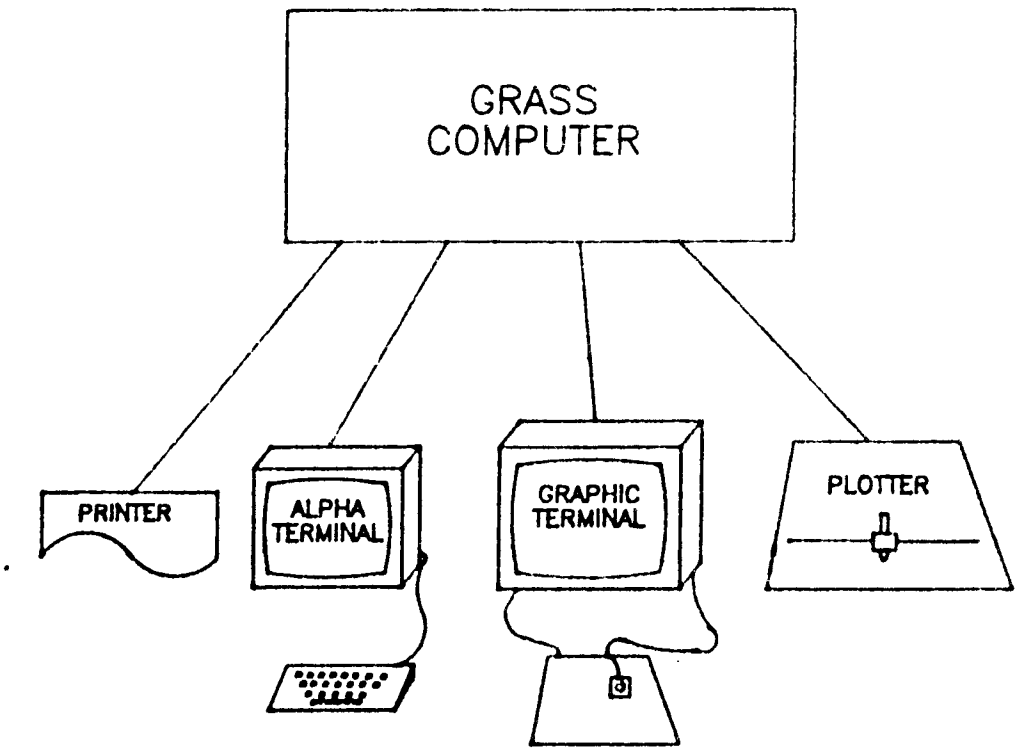


FIGURE 1 - GRASS BLOCK DIAGRAM
CONFIGURATION

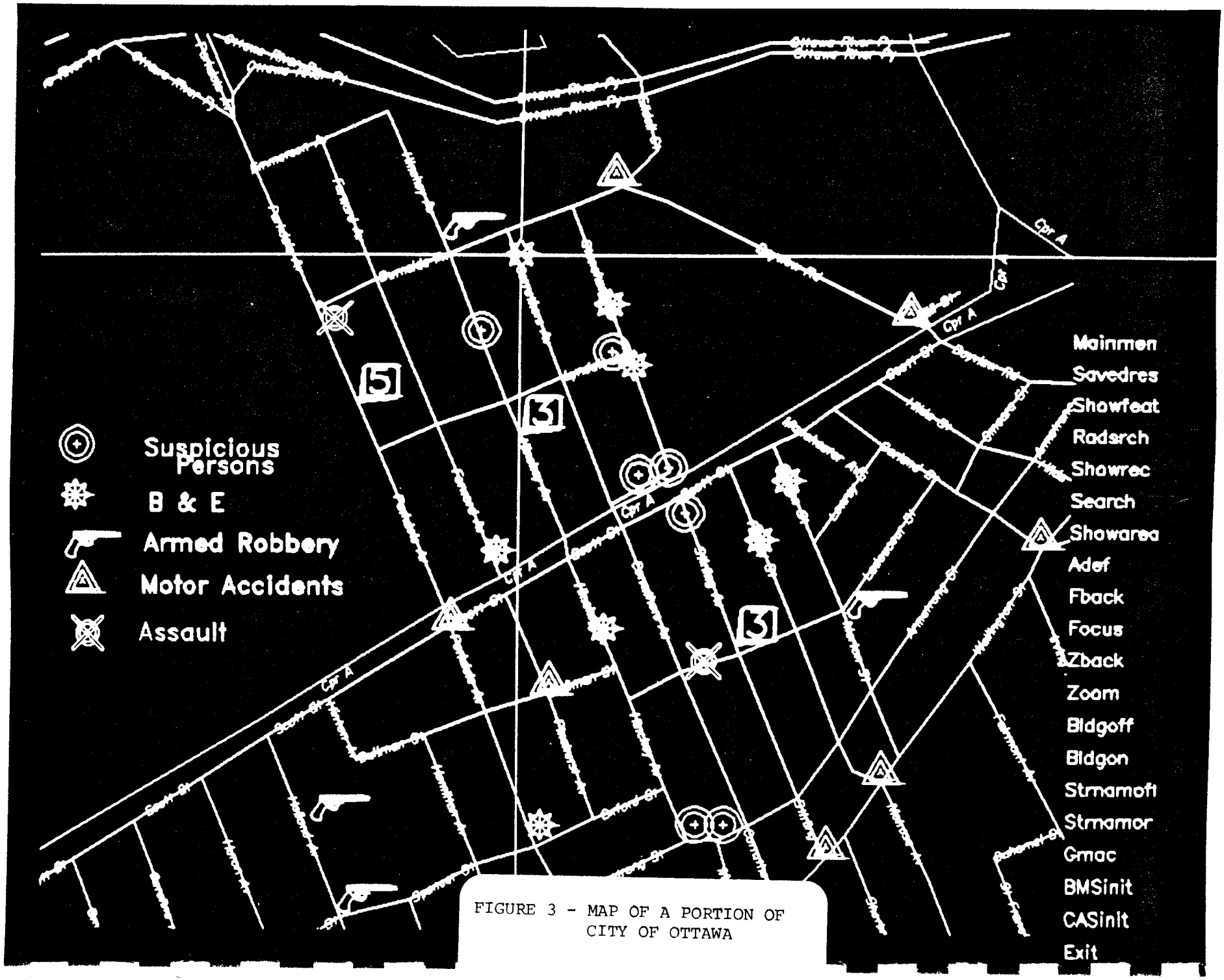


FIGURE 3 - MAP OF A PORTION OF CITY OF OTTAWA

FIGURE 2 - GRASS WORKSTATION AS IT SITS IN THE CITY OF OTTAWA POLICE FORCE

OPERATION OF VINSLEUTH
(C) 1985
VERSION 1.85

Charles A. POPLINGER
by: Former FBI Agent

BACKGROUND:

On March 15, 1979, the National Highway Traffic Safety Administration, with approval of the U.S. Congress, issued Standard 571.115 of the Consolidated Federal Regulations, Chapter 49. This standard requires all passenger vehicles, trucks, and trailers manufactured for sale in the United States, beginning with the 1981 model year, to be identified by a 17 digit Vehicle Identification Number (VIN). The standard requires that the 9th digit of the 17 digit number be a check digit, mathematically determined from the other 16 digits.

During early 1983, Vinsleuth, a computer program, was developed to compute the check digit, given any 17 digit VIN. Computation of the check digit by the program is done using the same method established by Chapter 49, Standard 571.115 of the Consolidated Federal Regulations. Since 1983, Vinsleuth has been modified to compute a few True VINs (TVIN), given that an Altered VIN (AVIN) was entered. The program will audit for accuracy the first 11 digits of a VIN, and it will also build a 17 digit TVIN, starting with entry of the last six digits or the Confidential VIN (CVIN), which is also known as the police VIN.

Vinsleuth was originally developed to assist car theft investigators in determining the car's TVIN when the only information available to the investigator was an AVIN contained on a counterfeit vehicle certificate of title, certificate of registration, or insurance certificate. By knowing the TVIN, the car theft investigator may obtain the car theft report. Vinsleuth has also been used to determine whether or not vehicles shown on bank records as assets for loans are legitimate and identifying a car stolen in one state, transported to and titled in a second state with a counterfeit title from a third state.

By knowing the TVIN, the investigator has access to the car theft report. From that report, the investigator gains considerable information, which includes date of theft, place of theft, victim, insurance company, color of the car, and police report number. Other information, such ad description of suspects, may be available from the car theft report. Separately or combined, the above bits of information from a car theft report provide additional probable cause to seize a suspected stolen car or at least identify a car theft ring operating in a particular locale. Uses of Vinsleuth are limited only by the imagination of the investigator.

Vinsleuth was written by Charles A. Poplinger, a former FBI agent, and it is being distributed by the National Automobile Theft Bureau.

OPERATION OF VINSLEUTH
(C) 1985
VERSION 1.85

Vinsleuth was copyrighted to remove it from public domain and, thus, prevent access to it, under the freedom of information laws, by persons who would use the program for other than legitimate purposes. The copyright is not intended to restrict its use by duly appointed law enforcement agencies. The program and this document may be copied as frequently as is necessary for use within a specific law enformement agency.

This document assumes you are sitting in front of a computer, and you have loaded Vinsleuth. If you have not yet installed Vinsleuth, please refer to the Notes at the end of this document. Please note that whenever you see a question mark, you must enter something from the keyboard and key ENTER, RETURN, or whatever you call the key normally located just to the right of home row on the keyboard. Assume that the True VIN (TVIN) 1G6AS69N7EE823456 represents a stolen car, and this VIN has been entered into NCIC or some other stolen car data base. You will be working with alterations of this VIN, attempting to reconstruct it. You may alternately assume that an alteration of this VIN has appeared as collateral for a bank loan. Also, assume you cannot see or have not seen the stolen car, and you do not have access to the public VIN plate or the Confidential VIN (CVIN).

After the program is started, you will see the Main Menu shown below:

```
                    VINSLEUTH

                    MAIN MENU

          1  COMPUTE CHECK DIGIT (COMPUVIN)
          2  AUDIT VIN USING CAR DATA
          3  CALCULATE SEQUENCE CHANGING ONE DIGIT AT A TIME
          4  CALCULATE SEQUENCE CHANGING TWO DIGITS AT A TIME
          5  BUILD VIN STARTING WITH LAST SIX OR CVIN (VINSTEM)
          6  LOAD CAR DATA PROGRAM (CARENT)
          7  PRINT DATA ON ENTERED CAR
          8  ADMINISTRATIVE
          E  END

SELECT?
```

Vinsleuth is divided into two main programs, which are Compuvin and Vinstem. Compuvin computes the VIN for accuracy, audits the VIN for alterations in the first eleven digits which identify the car, calculates the sequence by changing one or two digits at a time, prints the data on the entered car, and handles the administrative portion. Vinstem allows you to build one or more TVINs if alterations were found in the first eleven digits.

CHECK DIGIT COMPUTATION (OPTION 1):

From the Main Menu, shown above, the operator may select one of the options by keying its number. Press your CAPS LOCK key, select Option 1, key ENTER, and you will see the following:

```
KEY R TO RETURN TO MAIN MENU OR

                !.................!
KEY IN YOUR VIN?
```

You may key R to return to the Main Menu but, for this demonstration, key in the VIN 1G6AS69N7EE8234567 under the line which has 17 dots, and key Enter. This VIN has 18 digits. If you make an error and key in other than 17 digits, you will see the following:

```
KEY IN YOUR VIN? 1G6AS69N7EE8234567
ENTER 17 DIGITS?
```

The program asks you to re-enter the VIN. Enter the VIN 1G6AS69N7EE823456 and key ENTER. The following will be displayed on the screen:

```
1G6AS69N7EE823456

DIGIT SUM IS 403

ENTERED VIN CHECK DIGIT IS 7

CALCULATED CHECK DIGIT IS  7
```

The program displays the VIN, calculates and displays the digit sum, displays the check digit in the entered VIN, and calculates and shows the calculated check digit. The check digit is based upon digits 1 through 8 and 10 through 17. If the calculated check digit does not match the entered VIN check digit, the program will display an "ALTERED" message. Through this option, you may determine if any 17 digit VIN is valid. Though not shown above, the program asks if you want to print the above screen. For the purpose of this demonstration, turn on your printer and key Y and ENTER. You will obtain a hard copy of the above. Vinsleuth will allow you to obtain a hard copy of the result of any of the Main Menu options. If you did not turn on your printer before you keyed Y and ENTER, your computer will set a timer. If the timer runs out before you turn on your printer, your computer will return to the command level, and you will have to type VINP at the A prompt or at the C prompt, if you are using a hard disk drive, to re-enter Vinsleuth.

The program has returned to the Main Menu. Select Option 1, and key ENTER. You will see the following screen:

```
Key Return to retain your previous VIN, or key in a new VIN or

Use the Space Bar to place the cursor under the digits to be
changed.  Use the Back Space key to erase incorrect entries.

YOUR PREVIOUS VIN WAS:1G6AS69N7EE823456
>_
```

The program will perform the selected option function on the VIN currently in its memory. The top line in the above screen tells you to key in a new VIN or key ENTER if the VIN is to remain

unchanged. Alternatly, you may use the Space Bar to place the cursor under the digit you want to change. Key in your changes and continue using the Space Bar to place the cursor under the next digit to be changed. When you have made your last change, key ENTER. If you make a mistake, use the Back Space key to erase the error. Nothing will happen until you key ENTER.

Main Menu Option 1 is used to compute the check digit whether or not you have a VIN with a check digit. For example, if you have built up the VIN 1G6AS69N EE823456 from a Confidential VIN (CVIN), you could substitute a zero for digit nine, the check digit; then the VIN would read 1G6AS69N0EE823456. Make the substitution and key Enter; you will see the following:

```
1G6AS69N0EE823456

DIGIT SUM IS  403

ENTERED VIN CHECK DIGIT IS 0

CALCULATED CHECK DIGIT IS  7

* * * * ALTERED * * * *
```

The screen above tells us that the VIN is altered, and the True VIN check digit should be 7 rather than 0. You may use Option 1 to determine if a VIN is true or to calculate a check digit to make an Altered VIN true.

Key ENTER to return to the Main Menu. Select Option 2 and key ENTER again. You will see the screen which asks for your VIN. Key in the VIN 1G6AS69N7EE823456, and key ENTER.

AUDIT OF THE VIN WITH DATA (OPTION 2):

Main Menu Option 2 causes the program to perform audits on each character of the VIN except the digit 10, the year. The only audit performed on digit 10 is to determine if the year is possible. A partial audit is performed on the last six digits and, all audits are performed using car manufacturers' data. After selecting Option 2, be sure your entered VIN is 1G6AS69N7EE823456, and key ENTER. You will see the following:

```
                VINSLEUTH

            1G6AS69N7EE823456

 1    1   ORIGIN          USA
 2    G   MANUFACTURER    GENERAL MOTORS
 3    6   MAKE            CADILLAC
 4    A   RESTRAINT       MANUAL BELTS
 5    S   MODEL           SEVILLE
 6    6   BODY TYPE       4
 7    9   BODY TYPE         DOORS
 8    N   ENGINE          5.7 LITER, V8, DIESEL
 9    7   CHECK DIGIT     7
10    E   YEAR            1984
11    E   PLANT           LINDEN
12-17     SEQ. PROD. NR.  823456

   THE DIGIT SUM IS  403
   THE CHECK DIGIT IS 7
   THE CALCULATED DIGIT IS  7
```

The program, through Option 2, defines the meaning of each of the VIN digits, indicates the Digit Sum, displays the

check digit, and calculates a check digit based on the entered VIN. The meaning of the digit sum will be explained later. Again, though not displayed, the program asks if you want to print the above. Turn on your printer and key Y for yes and key ENTER.

If any one or more of the VIN digits were altered, the calculated check digit would not match the check digit in the entered VIN and an "ALTERED" message would appear.

Key Y to have the program type the above and key Enter. After the above screen has been typed, the program will proceed to the Administrative section shown below:

```
EXAMPLE DE 26A-56865 OR 15-005576
  FILE?

EXAMPLE OH ST POL SGT WILLIAMSON, CLEVELAND
REQUESTER?
```

Your answers to each of the questions shown above, along with the entered VIN, will be stored in memory for later retrieval. After you have entered the name of the Requester, key ENTER, and the program will return to the Main Menu. The program will proceed to the Administrative section following display of VIN results when requested by Main Menu Option 2. If you do not want to retain a record of the VIN, key ENTER when the program requests entry of the File. The program will skip the administrative and return to the Main Menu.

When you see the Main Menu, key 2, and key ENTER, and space over to the N and key a 6. Space over to the second E and key an 8. The VIN will read 1G6AS6967E8823456. After you key ENTER again, the following screen will appear:

```
                    VINSLEUTH

                1G6AS6967E8823456

 1   1  ORIGIN           UNKNOWN
 2   G  MANUFACTURER     GENERAL MOTORS
 3   6  MAKE             CADILLAC
 4   A  RESTRAINT        MANUAL BELTS
 5   S  MODEL            SEVILLE
 6   6  BODY TYPE        4
 7   9  BODY TYPE          DOORS
 8   6  ENGINE           ERROR DIGIT
 9   7  CHECK DIGIT      8
10   E  YEAR             1984
11   8  PLANT            ERROR DIGIT
12-17   SEQ. PROD. NR.   823456
                         * RUN VINSTEM *

   THE DIGIT SUM IS  437
   THE CHECK DIGIT IS 7
   THE CALCULATED DIGIT IS  8

    * * * * ALTERED * * * *
```

In the above VIN, digit 8 was changed from an N to a 6, and digit 11 was changed from an E to an 8. Notice that, since the calculated check digit did not match the entered VIN digit 9, the "ALTERED" flag appeared. Also notice that, since General Motors did not put a number 6 engine in its Cadillac Sevilles, nor did they make Sevilles at plant 8, the words "ERROR DIGIT" appear in the data section after digits numbered 8 and 11. Also notice

that the word "UNKNOWN" appears in the data section for the Origin. Since the location of the assembly plant is in error, the lace where the car was built is not known. Finally, notice the flag "RUN VINSTEM" at the end of the data section. Vinstem is the program you will use to correct the errors found by the VIN audit in Main Menu Option 2. Vinstem will be covered later.

As previously mentioned, Main Menu Option 2 performs partial audits on the last six digits of the entered VIN. This audit determines if the sequential production number of the entered VIN is within the range of numbers assigned to cars by the manufacturer at the assembly plant during the model year of the car's manufacture. The program again asks if you want the above screen typed. Key ENTER or key N, then key ENTER, and, at the request for the date in the administrative section, key ENTER again. The program will return to the Main Menu. Select Option 2, and key ENTER.

Your VIN was 1G6AS6967E8823456. You will change it to read 1G6AS69N7EE893456. You will reinsert an N for digit 8, an E for digit 11, and you will change the 13th digit from a 2 to a 9. Key ENTER you will see the following screen:

```
                          VINSLEUTH

                     1G6AS69N7EE893456

 1    1   ORIGIN            USA
 2    G   MANUFACTURER      GENERAL MOTORS
 3    6   MAKE              CADILLAC
 4    A   RESTRAINT         MANUAL BELTS
 5    S   MODEL             SEVILLE
 6    6   BODY TYPE         4
 7    9   BODY TYPE           DOORS
 8    N   ENGINE            5.7 LITER, V8, DIESEL
 9    7   CHECK DIGIT       5
10    E   YEAR              1984
11    8   PLANT             LINDEN
12-17     SEQ. PROD. NR.    893456

      THE DIGIT SUM IS  445
      THE CHECK DIGIT IS 7
      THE CALCULATED DIGIT IS  5

SEQUENCE GREATER THAN THE UPPER LIMIT OF 839997

          * * * * ALTERED * * * *
```

The program has determined that General Motors did not produce any Sevilles numbered greater than 839997. The message concerning the sequence will also appear if the VIN is altered to a number less than the number with which the manufacturer began numbering. Return to the Main Menu, select Option 2, and key ENTER. Space over to the 9 and change it to a 7. Your Altered VIN has become 1G6AS69N7EE723456. When you key ENTER, you will see a screen similar to the one above, except the message will read "SEQUENCE LESS THAN THE LOWER LIMIT OF 800001". You will also see the "ALTERED" message. General Motors numbered its Cadillac Sevilles at Linden New Jersey, beginning with 800001. The last car produced was numbered 839997. The beginning and ending sequential production numbers for each car model at each assembly plant from 1981 to date are part of the data on which Vinsleuth relies.

Some car thieves are smart enough to figure out the formula for the check digit. They may alter one of the first 11 digits, so the check digit is correct. For example, the letter J has the same value as does the letter A when computing the VIN's check digit. If this were done in the TVIN 1G6AS69N7EE823456, the AVIN would be 1G6JS69N7EE823456. The fourth digit has been changed from an A to a J. Return to the Main Menu and select Option 1. Enter the above AVIN, key ENTER, and you will see the following:

```
1G6JS69N7EE823456

DIGIT SUM IS  403

ENTERED VIN CHECK DIGIT IS 7

CALCULATED CHECK DIGIT IS 7
```

Since Option 1 only calculates the check digit, nothing seems to be wrong. Key ENTER twice to return to the Main Menu and select Option 2. Key ENTER once more, and the following will be displayed:

```
                    VINSLEUTH

                1G6JS69N7EE823456

 1   1  ORIGIN            USA
 2   G  MANUFACTURER      GENERAL MOTORS
 3   6  MAKE              CADILLAC
 4   J  RESTRAINT         ERROR DIGIT
 5   S  MODEL             SEVILLE
 6   6  BODY TYPE         4
 7   9  BODY TYPE           DOORS
 8   N  ENGINE            5.7 LITER, V8, DIESEL
 9   7  CHECK DIGIT       7
10   E  YEAR              1984
11   E  PLANT             LINDEN
12-17   SEQ. PROD. NR.    823456
                          * RUN VINSTEM *

   THE DIGIT SUM IS  403
   THE CHECK DIGIT IS 7
   THE CALCULATED DIGIT IS  7
```

Notice the words "ERROR DIGIT" in the data section for digit 4. Also notice the flag "RUN VINSTEM" at the end of the data section. Option 2 has determined that GM did not use a J type restraint in the Cadillac Seville. You may also note that the calculated check digit is the same as the check digit in the entered VIN.

PRINT DATA ON ENTERED CAR (OPTION 7):

Another part of Compuvin is Main Menu Option 7, which prints the data on the car you entered through Options 1, 2, 3, or 4. Per Chapter 49 Standard 571.115 of the Consolidated Federal Regulations, each of the VIN digits is given a value. For example, A=1, B=2, C=3, etc. There are no O's or I's. Pursuant to the law, each of the VIN digit values is multiplied by a weight assigned to each digit position. The first digit is assigned a weight of 8, the second a 7, the third a 6, and so on. The VIN

digit values are multiplied by the weights, and the products are summed. The sum of the products is the "digit sum". This sum, when divided by 11 in long hand, will yield a remainder, which is the check digit. Return to the Main Menu and select Option 7 and key ENTER. The following will be printed:

1G6JS69N7EE823456

VIN	VAL	WT	PRD	CUMUL
1	1	8	8	8
G	7	7	49	57
6	6	6	36	93
J	1	5	5	98
S	2	4	8	106
6	6	3	18	124
9	9	2	18	142
N	5	10	50	192
7	7	0	0	192
E	5	9	45	237
E	5	8	40	277
8	8	7	56	333
2	2	6	12	345
3	3	5	15	360
4	4	4	16	376
5	5	3	15	391
6	6	2	12	403

403 / 11 = 36 R 7

As shown above, the VIN is listed down the left side, under VIN. The value of each VIN digit is listed in the column labeled VAL. These values will be different if the VIN digits are different. The numbers in the column labeled WT do not change. The numbers in the column labeled PRD are the products of the VAL times the WT. The numbers in the column labeled CUMUL are the cumulative sums of the products. For example, in the first three rows, 8 + 49 = 57, 57 + 36 = 93, etc. The number 403 is the cumulative product, or the sum of the column labeled PRD. Dividing 403 by 11 in long hand yields 36, with 7 remaining. This 7 is the calculated check digit. Please note that the calculated check digit is the same as digit 9 in the entered VIN. Also, please note that digit 4 is J, and that Vinsleuth has determined digit 4 to be in error.

Since most car thieves prefer to alter one of the last six VIN digits rather than change the identity of the car, Vinsleuth attempts to decipher their alterations. The primary objective of Vinsleuth is to obtain a reasonably small number of True VINs which may be entered into a stolen car data base, such as NCIC, in search of a car theft report.

CALCULATION OF THE SEQUENCE CHANGING ONE DIGIT (OPTION 3):

If you think that the person who disguised the car by altering the VIN changed only one of the last six digits, you may select Option 3 from the Main Menu shown on the next page. This option causes the program to sequence through each of the last six digits, one at a time, and calculate all possible True VINs in the range of numbers of the first car made at the production plant to the last car made at that plant, that year. Each time one of the last six digits is changed, the program calculates a check digit. The program then compares the calculated check digit with VIN digit number nine. If they are the same, the new VIN is retained for display on the screen. Return to the Main Menu shown below:

```
                    VINSLEUTH

                    MAIN MENU

          1  COMPUTE CHECK DIGIT (COMPUVIN)
          2  AUDIT VIN USING CAR DATA
          3  CALCULATE SEQUENCE CHANGING ONE DIGIT AT A TIME
          4  CALCULATE SEQUENCE CHANGING TWO DIGITS AT A TIME
          5  BUILD VIN STARTING WITH LAST SIX OR CVIN (VINSTEM)
          6  LOAD CAR DATA PROGRAM (CARENT)
          7  PRINT DATA ON ENTERED CAR
          8  ADMINISTRATIVE
          E  END

SELECT?
```

Select Option 3, and key ENTER. Key in the AVIN 1G6AS69N7EE823956. In this AVIN, the 15th digit was changed from a 4 to a 9. Key ENTER, and you will see the following:

```
                    VINSLEUTH

                1G6AS69N7EE823956

        THE FOLLOWING ARE THE ONLY POSSIBLE TRUE VINs
        IF ONE OF THE LAST SIX DIGITS WAS ALTERED.

                1G6AS69N7EE823456
                1G6AS69N7EE823926
                1G6AS69N7EE823957

          ENTERED VIN DIGIT SUM IS: 423
          ENTERED VIN CHECK DIGIT IS: 7
          ENTERED VIN CALCULATED CHECK DIGIT IS: 5
```

Please note that we are considering the TVIN 1G6AS69N7EE823456 to have been stolen and entered into NCIC, and the AVIN 1G6AS69N7EE823956 has appeared on a counterfeit title or some other paper which represents the disguised car. As shown above, the program has calculated all possible TVINs. You will receive a theft report when you enter the first of the above TVINs in NCIC. The program will ask if you want to print the above screen. Be sure your printer is on before you key Y for yes, then key ENTER.

When you have returned to the Main Menu, select Option 3 again, and, this time, key S. Now key in the digits 893456, and key ENTER. Please note that the last six digits have been altered to a umber outside the range of numbers assigned by General Motors to its 1984 Seville. The AVIN is 1G6AS69N7EE893456.

```
VINSLEUTH

1G6AS69N7EE893456

THE SEQUENCE HAS BEEN ALTERED TO A NUMBER FOR
WHICH NO CAR WAS BUILT.  THE FOLLOWING ARE THE ONLY
TRUE VINs FOR THIS CAR:

1G6AS69N7EE823456

ENTERED VIN DIGIT SUM IS: 445
ENTERED VIN CHECK DIGIT IS: 7
ENTERED VIN CALCULATED CHECK DIGIT IS: 5
```

The program sequenced through each of the last six digits, calculated all possible True VINS and, it found only one possible TVIN, the one entered in NCIC.

Main Menu Option 3 has the advantage of providing no more than ten possible TVINs; however, some car thieves alter more than one of the last six digits on a Public VIN plate and on related paperwork.

CALCULATION OF THE SEQUENCE CHANGING TWO DIGITS (OPTION 4):

Main Menu Option 4 calculates all possible True VINs changing two of the last six digits at a time in the same manner as Option 3 did for one digit. Unfortunately, when more sequence digits are altered, more TVINs are possible. Return to the Main Menu, and select Option 4. Key S, ENTER, and enter the digits 828459 and, key ENTER again. In this AVIN, the 14th digit was changed from a 3 to an 8, and the 17th digit was changed from a 6 to a 9. Key ENTER, and the following will be displayed:

```
VINSLEUTH

1G6AS69N7EE828459

THE TRUE VIN IS 1G6AS69N7EE PLUS ONE OF THE FOLLOWING.

857459  853959  853489  853458  846459  843559  84345D
835459  833453  833419  833159  829659  829452  829449
828429  827457  827409  827359  826759  826499  826454
825479  825451  825059  824459  823957  823909  823859
823750  823652  823649  823599  823554  823490  823487
823473  823456  823442  823439  823425  823411  823408
823389  823358  823229  823179  823151  823053  823019
822453  822419  822159  821559  821450  820959  820489
820458  813459  803479  803451  803059  802459  0

THERE ARE A TOTAL OF 62 TRUE VINs.
```

Sixty-two TVINs are a lot to enter into NCIC or into any other stolen car data base in search of a car theft report. But, if you need the car theft report, you have all possible TVINs. If you start with the top left sequence and work across and down, you will receive the theft report on the 37th entry. The TVIN sequence is in the sixth row, second column. It should be noted that if Option 4 had been used when only one of the last six digits was altered, the TVIN would also have been found. When the program sequences through the last six digits, changing two at a time, none of the numbers between zero and nine for a given sequence digit are skipped. Thus, one of the digits being considered by the program will be the correct digit, and the other an altered digit. The advantage of Option 3 is that fewer

possible True VINs are reported and fewer need to be entered into the stolen car VIN data base. Option 3 should always be selected first, and, if the theft report is not found, then Option 4 must be used.

There is a possibility that more than one car with a VIN sequence computed by Vinsleuth will be entered as stolen. When you receive a theft report, be sure that all the first eleven digits match the VIN you are attempting to decipher. Secondly, you must enter all the TVINs reported by the program because you could receive two car theft reports, one on a car which is similar but with a slightly different sequence, and the one of interest in your investigation. Though this is unlikely, you will have to testify that all TVINs reported by the program were entered into the stolen car data base. In the event you do obtain two theft reports, the differences must be resolved by other investigation. No attempt was made to program an option to provide True VINs if more than two digits were altered. To do so would defeat the purpose of Vinsleuth, that of determining a few True VINs for entry into a stolen car VIN data base.

The next portion of Vinsleuth is a separate program named Vinstem. You will use Vinstem to correct VINs which have errors in one or more of the first eleven digits.

BUILD A VIN STARTING WITH LAST SIX DIGITS (VINSTEM):

The second part of Vinsleuth is a program called Vinstem, accessed by selecting Main Menu Option 5. If you are at the command level, you may access Vinstem by typing VINS at the A prompt or at the C prompt. The object of Vinstem is to correct errors in the first eleven VIN digits found through Main Menu Option 2, the VIN audit. Like Main Menu Option 2, Vinstem relies on car manufacturers' data, and, to date, car VIN data for General Motors, Ford, Chrysler, Mercedes Benz, and Jaguar, along with VIN data for some cars not sold in the United States, such as the Sunburst and Firefly, have been entered for use by this program. The program does not contain vehicle data for trucks and trailers.

If you have an AVIN such as 1G6JS6967E8823456, select Main Menu Option 2, and enter it when requested. You will see the figure shown below:

```
                        VINSLEUTH

                  1G6JS6967E8823456

 1    1   ORIGIN            UNKNOWN
 2    G   MANUFACTURER      GENERAL MOTORS
 3    6   MAKE              CADILLAC
 4    A   RESTRAINT         ERROR DIGITS
 5    S   MODEL             SEVILLE
 6    6   BODY TYPE         4
 7    9   BODY TYPE           DOORS
 8    6   ENGINE            ERROR DIGIT
 9    7   CHECK DIGIT       8
10    E   YEAR              1984
11    8   PLANT             ERROR DIGIT
12-17     SEQ. PROD. NR.    823456
                            * RUN VINSTEM *

     THE DIGIT SUM IS  437
     THE CHECK DIGIT IS 7
     THE CALCULATED DIGIT IS  8

      * * * * ALTERED * * * *
```

Tell the program to type the screen, then proceed through the administrative section to the Main Menu and select Option 5, and key ENTER. Vinstem will load into the computer, and you will see the following:

```
BE SURE YOUR CAPS LOCK KEY IS ENGAGED.

KEY 'R' TO RETURN TO MAIN MENU OR 'E' TO END.
ENTER ONE OF THE FOLOWING.  IF YOU HAVE A CVIN KEY ENTER THEN ENTER IT.
ENTER THE LAST SIX DIGITS?
ENTER THE CONFIDENTIAL VIN
```

The top line says to key R if you want to return to the Main Menu from which we just came. You may also key E, to stop program execution. If you are using the compiled version, and you key E, the computer will return to its command level, and you will have to type VINS to return to Vinstem. If you are operating in BASIC, type RUN "VINS.BAS". The same is true for Compuvin except you will type VINP or RUN "VINP.BAS", rather than VINS. Again, you should have the caps or shift lock key engaged, and anytime you are asked to enter something from the key board, nothing will happen until you press ENTER.

The fifth line shown above tells you to enter the Confidential VIN. Please notice that your cursor is located at the end of the fourth line. If you have the car in your possession, and you have obtained the CVIN, key ENTER once to place the curcor at the end of the fifth line. Now you would key in your CVIN. The CVIN derivative for the TVIN 1G6AS69N7EE823456 is 6EE823456. This will be covered later.

The cursor is currently located at the end of the fourh line. You have the AVIN 1G6JS6967E8823456, and the VIN audit, Main Menu Option 2, has determined that there are errors in digit 1, the Origin; digit 4, the Restraint; digit 8, the Engine; and digit 11, the Plant. The program wants you to enter the last six digits which are 823456. Enter them, and, after you key ENTER, you will see the following:

```
ENTER THE TWO DIGIT SYMBOL WHICH REPRESENTS THE CAR:
DIGITS 2 AND 3

        G1  CHEVROLET            81  SUNBURST
        G2  PONTIAC              87  SPECTRUM
        G3  OLDSMOBILE           A3  IMPERIAL
        G4  BUICK                C3  CHRYSLER
        G6  CADILLAC             B3  DODGE
        G7  ACADIAN & FIREFLY    P3  PLYMOUTH
        Y1  NOVA                 DB  MERCEDES BENZ
        FA  FORD                 AJ  JAGUAR
        LN  LINCOLN              N1/N4  NISSAN CAR (N6) PICKUP
        MR  CONTINENTAL
        ME  MERCURY
        F1  MERKUR

SELECT?
```

The screen asks you to enter the letters which represent the car. Look at the print-out. VIN digits 2 and 3 are G6. Since the data section of the print-out does not indicate a problem with these two digits, enter them. If you key ENTER without keying any of the above digits, the program will return to the Vinstem menu. If you enter anything that is not in the above list, the program will flash an error message and ask you to select from the above list.

The next screen requests the model year as follows:

```
ENTER LETTER WHICH REPRESENTS THE YEAR:
DIGIT 10
          B  1981      G  1986
          C  1982      H  1987
          D  1983      J  1988
          E  1984      K  1989
          F  1985      L  1990

     SLEECT?
```

Refer to the audit print-out, and note that digit 10 is an E. Since the audit data does not show an error for VIN digit 10, enter E, and key ENTER.

The next screen asks for the letter which represents the car model, which is digit 5. It should be noted that General Motors started identifying its 1985 car models with two digits, VIN digits 4 and 5. In 1985, General Motors dropped the Restraint designation entirely. Thus, if you were interested in a 1985 or later VIN, you would enter two digits to describe the car to the computer program. If this were a Ford automobile, you would enter two numbers to describe the model for the computer. To date, Ford has always used a constant P for VIN digit 5, and Ford uses digits 6 and 7 to designate its car models. Chrysler uses only VIN digit 5 to differentiate between its car models, while Mercedes Benz uses digits 4 through 7 to differentiate between its car models. You will not have to worry about any of this; the program knows the difference between each of the car companies, and it will tell you which VIN digits to enter, as shown in the example screen below:

```
ENTER LETTER WHICH REPRESENTS THE CAR NAME:
DIGIT 5
        W  FLEETWOOD FWD      B  FLEETWOOD RWD
        M  DEVILLE RWD        D  DEVILLE FWD
        F  LIMOUSINE          G  CIMARRON
        L  ELDORADO           S  SEVILLE

     SELECT?
```

Since the audit does not show a problem in the data section for digit 5, enter an S and key ENTER.

The next screen requests you to enter the number of doors or VIN digits 6 and 7. If you are building up a CVIN, you would know how many doors the car has. But, since the AVIN is from a counterfeit title or another piece of paper, and you do not yet have access to the car, refer to the audit.

```
ENTER THE NUMBER OF DOORS OR VIN DIGITS 6 AND 7;  KEY ENTER IF UNKNOWN:

ENTERING VIN DIGITS WILL REDUCE POSSIBILITIES.

          DOORS    DIGITS    VEHICLE
            4        69      SEVILLE

SELECT?
```

The data section of the audit shows that there are no problems with digits 6 and 7. Enter 69 and key ENTER. General Motors made 1984 Sevilles only with 4 doors in the body style 69. Pontiacs are made in as many as 3 body styles. Cadillac Fleetwoods were made in two body styles, 47 and 69, the 2 and 4 door types. If the Seville were made in more than one body type, the choices would have appeared on the screen. When you have only one choice to make, as above, you may just key ENTER. The program would have entered 69 for you.

To date General Motors has offered a passive type restraint system in only one car, the 1981 Cadillac Fleetwood. The Program does not discount the fact that GM may offer both passive belts and air bags in the future. Unless a particular GM car has two or more types of restraint systems available, you will not see a screen which requests you to select a type of restraint. The program will automatically insert the proper letter in the proper position for this VIN digit.

The next screen lists three types of engines which GM used in its Sevilles. The engine is VIN digit 8.

```
ENTER LETTER REPRESENTING ENGINE; KEY ENTER IF UNKNOWN:
DIGIT 8
              N  5.7 V8 DIESEL
              9  6.0 V8 ELECT FUEL INJ
              8  4.1 V8 DIGITAL FUEL INJ

         SELECT?
```

Refer to the data section of the audit and observe the words "ERROR DIGIT" in the data section for the engine. Since the true engine designation is not known, key ENTER, and let the program figure it out.

United States car manufacturers publish data concerning their cars. This data includes the types of engines they will use during the manufacture of a particular car model. Occasionally, the manufacturer will, to improve sales, change the type of engine it puts in a model during the production year. The fact that the manufacturer used an engine not planned when the original data was published could cause this program to indicate the VIN digit for the engine to be in error. Fortunately, U.S. car manufacturers do not introduce a completely new engine during the model year. If the program does not find the engine in its data base for a particular model, it then searches for other engines produced for that car line. If the engine designated by the entered VIN is found, an asterisk will precede the description for the engine, and no error will be indicated in the data section of the print-out. If the program shows an asterisk in the data section of

digit eight, a description of the engine designated by the entered VIN will follow. If the calculated check digit matches VIN digit 9, and the engine designation, digit 8, in your VIN does not appear on the screen above, then enter digit 8 from your VIN. Yours is porobably the correct digit. If you use Main Menu Option 2 on that VIN, before the data is corrected, you will see an error for the engine digit. As long as the calculated check digit matches VIN digit nine, the VIN is alright.

Once the car model has been found the program checks for the number of assembly plants. If the program finds that the car model was been made at more than one plant, you would see a screen which asks you to select the proper assembly plant, You could also tell the program to give you True VINs for all assembly plants where the car was made. Since this car, the Cadillac Seville, was made only at Linden, New Jersey, you will not see a screen which asks for the assembly plant. The program will insert the proper character in the eleventh VIN position.

Unless the car was made in two or more different countries, the program will automatically insert the proper character for the origin of the assembly plant, VIN digit one. If the car was made in more than one country you will see a screen which asks you to select the proper origin or give you VINs which reflect all origins of the car model in question.

After you select the car model and body style, the program will display the true VINs as shown below:

VINSLEUTH

THE FOLLOWING ARE TRUE VINS BASED ON ENTRIES:

1G6AS69N7EE823456
1G6AS6993EE823456
1G6AS6984EE823456

Examination of the above resulting VINs reveals that VIN digits 1 has been verified. Digit 11 has been corrected, and VIN digit 8 is an N, 9, or 8. Vinstem has inserted the correct check digit, depending on the variation of digit 8. When you use Vinsleuth, you assume that VIN digit 9, the Check Digit, has not been altered. You may now enter the above three True VINs into a stolen car VIN data base in search of the theft report.

Most car thieves alter one of the last six digits to disguise a stolen car, and you need only to use Main Menu Option 3, which sequences through the last six digits changing one at a time form zero to nine, with replacement, to find the possible TVINs. You may find a VIN which contains alterations in both the last six digits and in the first eleven. Assume you have the Altered VIN 1G6AS68N7EE823486, in which the seventh digit was altered from a 9 to an 8, and the 16th digit was altered from a 5 to an 8. Also assume that the car with TVIN 1G6AS6967EE823456 has been reported stolen. Select Main Menu Option 2, and enter the altered VIN. You will see the result shown on the next page:

```
                    VINSLEUTH

                1G6AS68N7EE823486

 1   1   ORIGIN            UNKNOWN
 2   G   MANUFACTURER      GENERAL MOTORS
 3   6   MAKE              CADILLAC
 4   A   RESTRAINT
 5   S   MODEL             SEVILLE
 6   6   BODY TYPE         ERROR DIGITS 6 & 7 AND MAYBE 5
 7   8   BODY TYPE
 8   N   ENGINE
 9   7   CHECK DIGIT
10   E   YEAR              1984
11   E   PLANT
12-17    SEQ. PROD. NR.    823486
                           * RUN VINSTEM *

    THE DIGIT SUM IS  410
    THE CHECK DIGIT IS  7
    THE CALCULATED DIGIT IS  3

     * * * * ALTERED * * * *
```

Key Y to print the above screen, and proceed through the administrative section. When you return to the Main Menu, select Option 5. Enter the last six digits, 823486. The next screen will ask for the type of car, so enter G6 because the audit data section of the VIN print-out does not indicate a problem with these two digits. The next screen will ask for the year. Enter an E, representing 1984. The note in the data section of the audit indicated a problem with digits 6 and 7. There may also be a problem with digit 5. If digit 5 was altered, you would have to repeat the Vinstem routine for each letter shown in the screen below:

```
ENTER LETTER WHICH REPRESENTS THE CAR NAME:
DIGIT 5
        W  FLEETWOOD FWD        B  FLEETWOOD RWD
        M  DEVILLE RWD          D  DEVILLE FWD
        F  LIMOUSINE            G  CIMARRON
        L  ELDORADO             S  SEVILLE

 SELECT?
```

If you key ENTER without making a selection the program will ask for some entry. If you enter something that does not appear on the screen, the program will ask that you make a selction from the car models presented.

Assume that digit 5 was not altered, and key S; then key ENTER. The audit revealed an error in digits 6 and 7, but only one choice is displayed on the screen which asks you to enter the body style of the car. You may type 69 and key ENTER or just key ENTER and let the program enter the 69 for you. The next screen asks you to select the type of engine. The VIN audit reveals that this digit is in error, so key ENTER. The program will give you three VINs, each with a different engine designation.

General Motors made the Seville at only one plant, with only one type of restraint, and they did not make the Seville in more than one country. You will not be asked to select VIN digits which represent the origin, restraint, and plant. The program will insert the proper digits for you.

The program will display the following True VINs. These are the only ones possible.

THE FOLLOWING ARE TRUE VINS BASED ON ENTRIES:

1G6AS69N5EE823486
1G6AS6991EE823486
1G6AS6982EE823486

Notice that Vinstem has verified digit 1, corrected digit 7 from an 8 to a 9, and the variations in digit 8, the engine symbol, have caused the variations in the Check Digit. As previously mentioned, when you use Vinsleuth, you must assume that the Check Digit in your VIN has not been altered. Key Y to obtain a typed copy of the screen above, then change digit nine to read 7 in each of the above VINs. You will now have the following three VINs.

1G6AS69N7EE823486
1G6AS6997EE823486
1G6AS6987EE823486

If Vinstem produced a set of VINs, and one of them contained the proper Check Digit, but you did not find the theft report in NCIC, you would have to change the Check Digit in the other VINs to match the one in your AVIN.

When you return to the Vinstem Menu, key R and key ENTER where the program asks for the last six digits. Compuvin will load into your computer, and the Main Menu will be displayed. Select Option 3. When the program asks for your VIN, key in 1G6AS69N7EE823486, which is the first of the three VINs listed above, then key ENTER. The program will display the following:

VINSLEUTH

1G6AS69N7EE823486

THE FOLLOWING ARE THE ONLY POSSIBLE TRUE VINs
IF ONE OF THE LAST SIX DIGITS WAS ALTERED:

1G6AS69N7EE823456
1G6AS59N7EE823487

ENTERED VIN DIGIT SUM IS: 412
ENTERED VIN CHECK DIGIT IS: 7
ENTERED VIN CALCULATED CHECK DIGIT IS: 5

Key Y to obtain a print-out, and when you see the Main Menu again, select Option 3, and enter the second of the above three VINs, which is 1G6AS6997EE823486. Key Y to obtain the print-out of the screen, then repeat this procedure for the third VIN, which is 1G6AS6987EE823486. In addition to the above, the print-out will contain the following:

```
                    VINSLEUTH

              1G6AS6997EE823486

THE FOLLOWING ARE THE ONLY POSSIBLE TRUE VINs
IF ONE OF THE LAST SIX DIGITS WAS ALTERED:

              1G6AS6997EE833486
              1G6AS6997EE822486
              1G6AS6997EE823086
              1G6AS6997EE823489

  ENTERED VIN DIGIT SUM IS: 452
  ENTERED VIN CHECK DIGIT IS: 7
  ENTERED VIN CALCULATED CHECK DIGIT IS: 1


                    VINSLEUTH

              1G6AS6987EE823486

THE FOLLOWING ARE THE ONLY POSSIBLE TRUE VINs
IF ONE OF THE LAST SIX DIGITS WAS ALTERED:

              1G6AS6987EE813486
              1G6AS6987EE824486
              1G6AS6987EE823886
              1G6AS6987EE823466
              1G6AS6987EE823483

  ENTERED VIN DIGIT SUM IS: 442
  ENTERED VIN CHECK DIGIT IS: 7
  ENTERED VIN CALCULATED CHECK DIGIT IS: 2
```

You have eleven True VINs to enter into NCIC for the car theft report. Actually, you will obtain the theft report on the first entry.

If you had an AVIN, such as 1GGAS69N7EE823456, in which the third digit is a G, and you selected Main Menu Option 2, the VIN audit, you would see numerous error flags. They will exist because the car's manufacturer was not found. If you are sure that the car is within the data base of this program, you may proceed to Vinstem through Main Menu Option 5. Enter the last six digits. The screen will display the true designation for digits two and three. Often, on paper such as car titles, a six is written as a G, a 5 is interpreted as an S, a zero is written as the letter O, and an I is written for the number 1. If you have a VIN in which nothing seems to work, try substituting for some of these more obvious copying errors. Then use Main Menu Option 1 to determine if the VIN is true.

You may use Vinstem in another way. Suppose you have a VIN which is not complete. For example, you may have the last six digits and possibly the first few. Go ahead and select Vinstem, then proceed through the menu screens. Enter the digits you know or have, and key ENTER after the word Select, in those screens for the digits you do not know or do not have. You may be rewarded with only a few True VINs or you may have many. At least, one of the computed VINs will be the correct one.

General Motors, Ford and Chrysler identify their cars with a non-public number known as the Police or Confidential VIN.

These numbers are a derivative of the 17 digit True Number. To date, General Motors has used a 9 digit number while Ford and Chrysler use an 8 digit number. The General Motors number consists of the division, year, plant, and sequence while Ford and Chrysler numbers consist of the year, plant, and sequence.

CALCULATION OF A VIN USING CVIN (VINSTEM):

Calculation of the True 17 digit VIN from the Confidential VIN is the second option available in Vinstem. You would use this option when you have either the nine or the eight digit derivative. One assumption must be made. You are able to see or you have seen the car. You must, therefore, know which company produced the vehicle, what the car line is, and how many doors the car has.

The CVIN derivative for 1G6AS69N7EE823456 is 6EE823456. This derivative means that the car was produced by General Motors because there are nine digits. The car is a Cadillac because the first digit is a six. The car was made in 1984 at Linden, New Jersey, and it was the 23456th car made. In the Vinstem Menu, shown below, your cursor will be located after the line which asks for the last six digits. Key ENTER, and the cursor will appear after the line which asks for the CVIN. Enter the digits 6EE823456, and key ENTER. If you do not enter anything after either of the two requests, a message will tell you to make some entry in this screen. The cursor will reappear after the line requesting the last six digits.

```
BE SURE YOUR CAPS LOCK KEY IS ENGAGED.

KEY 'R' TO RETURN TO MAIN MENU OR 'E' TO END.

ENTER ONE OF THE FOLOWING.  IF YOU HAVE A CVIN KEY ENTER THEN ENTER IT.

ENTER THE LAST SIX DIGITS

ENTER THE CONFIDENTIAL VIN?
```

Again, to enter the CVIN, key ENTER once, and key in your nine digits. The following will be displayed:

```
ENTER THE TWO DIGIT SYMBOL WHICH REPRESENTS THE CAR:
DIGITS 2 AND 3

     G1  CHEVROLET            81  SUNBURST
     G2  PONTIAC              87  SPECTRUM
     G3  OLDSMOBILE           A3  IMPERIAL
     G4  BUICK                C3  CHRYSLER
     G6  CADILLAC             B3  DODGE
     G7  ACADIAN & FIREFLY    P3  PLYMOUTH
     Y1  NOVA                 DB  MERCEDES BENZ
     FA  FORD                 AJ  JAGUAR
     LN  LINCOLN              N1/N4  NISSAN CAR (N6) PICKUP
     MR  CONTINENTAL
     ME  MERCURY
     F1  MERKUR

SELECT?
```

The next screen will ask for the letter which represents the car name. Please ignore the words "Digits 2 and 3" in line two, since they refer to the full VIN you would be correcting if you had first used Main Menu Option 2, the VIN audit, and the audit had found errors.

```
ENTER LETTER WHICH REPRESENTS THE CAR NAME:
DIGIT 5
        W  FLEETWOOD FWD        B  FLEETWOOD RWD
        M  DEVILLE RWD          D  DEVILLE FWD
        F  LIMOUSINE            G  CIMARRON
        L  ELDORADO             S  SEVILLE

 SELECT?
```

Starting with this screen, you may build the True VIN for any of the cars shown above. But, since you have seen the car and it is a Seville, enter an S and key ENTER. The next screen will tell you to enter the number of doors or VIN digits 6 and 7. Again, VIN digits 6 and 7 refer to the full 17 digit number. This screen is as follows:

```
ENTER THE NUMBER OF DOORS OR VIN DIGITS 6 AND 7; KEY ENTER IF UNKNOWN:

ENTERING VIN DIGITS WILL REDUCE POSSIBILITIES.

          DOORS   DIGITS   VEHICLE
            4       69     SEVILLE

SELECT?
```

The program does not expect you to know that General Motors uses 47 for digits 6 and 7 for a 2 door car and 69 for for a 4 door car, so the the provision of simply entering the number of doors was provided. In the above screen, enter 4 because your Seville has 4 doors. The next screen asks for the letter which represents the type of engine.

```
ENTER LETTER REPRESENTING ENGINE; KEY ENTEP IF UNKNOWN:
DIGIT 8
            N  5.7 V8 DIESEL
            9  6.0 V8 ELECT FUEL INJ
            8  4.1 V8 DIGITAL FUEL INJ

      SELECT?
```

You would probably know whether the engine is a diesel or not, but few people would know if the engine has an electronic or digital fuel injection. In this screen, key ENTER without making a selection.

The program will display the following True VINS:

```
                        VINSLEUTH

      THE FOLLOWING ARE TRUE VINs BASED ON ENTRIES:

                    1G1AS69N7EE823456
                    1G6AS6993EE823456
                    1G5AS6984EE823456
```

FORD CVIN:

Ford Motor Company uses digits 6 and 7 to designate its car lines. Thus, the procedure for describing the proper car to the program requires a little more knowledge about the car. Suppose you have the CVIN FF123456. This number has only 8

digits, so it is from a Ford or Chrysler. Suppose it is from a Mustang LX Hatchback. The first F means that the car was made in 1985, and the second F means that the car was made at Dearborn, Michigan. In the Vinstem screen, key ENTER once to place the cursor at the line which requests the CVIN and key in the number FF123456. The next screen will ask for the name of the car company. Since the Mustang was made by Ford, key FA. The next screen, shown below, will list the car lines made by Ford during 1985.

```
SELECT THE TWO NUMBERS WHICH REPRESENT THE CAR:
DIGITS 6 & 7
DIGITS DOORS CAR                    DIGITS DOORS CAR
  04     2    ESCORT L                 13     4    ESCORT L
  09     4    ESCORT L STA WGN         05     2    ESCORT GL
  14     4    ESCORT GL                10     4    ESCORT GL STA WGN
  07     2    ESCORT GT/TURBO          15     4    ESCORT LX
  11     4    ESCORT LX STA WGN        26     2    MUSTANG LX
  28     3    MUSTANG LX               27     2    MUSTANG CONVERT
  28     2    MUSTANG GT/SVO           01     3    EXP
  18     2    TEMPO                    21     4    TEMPO L
  19     2    TEMPO GL                 22     4    TEMPO GL
  20     2    TEMPO GLX                23     4    TEMPO GLX
  46     2    THUNDERBIRD              39     4    LTD & LTD BROUGHAM
  40     4    LTD STATION WAGON        43     4    LTD CRWN VICT S
  44     4    LTD CRWN VICT S          42     2    LTD CROWN VICTORIA

SELECT?
```

Ignore the words "Digits 6 & 7" in line two of the above screen because they refer to the full 17 digit VIN. Look down the third and sixth columns for the car you have. The car is a Mustang, and you must know which kind of Mustang. The car will usually have some letter or letters on the side or rear which designate a trim package. The number of doors for each car line is listed in columns two and five. Since the car is a Hatchback, it must have three doors, and the proper entry is 28 as listed under "Digits", in column 1, rather than 26 as listed under "Digits" in column 4. Enter 28 and key ENTER.

The next screen will ask for the letter representing the engine as shown below:

```
ENTER LETTER REPRESENTING ENGINE; KEY ENTER IF UNKNOWN:
DIGIT 8

        A  2.3 LITER, L4 1BBL OHC
        F  5.0 LITER, V8 2BBL/CFI
        M  5.0 LITER, V8 2BBL OHC
        3  3.8 LITER, V6 2BBL/EFI

    SELECT?
```

We will assume that the car is stripped, and both the engine and transmission were removed. Key ENTER without making a selection. The program will display the four possible true VINs as shown below:

```
                        VINSLEUTH

THE FOLLOWING ARE TRUE VINs BASED ON CVIN FF123456

                    1FABP28A8FF123456
                    1FABP28F3FF123456
                    1FABP28M5FF123456
                    1FABP2836FF123456
```

CHRYSLER CVIN:

Suppose you have recovered a stripped Chrysler Le Baron Convertible, and you have obtained the CVIN ER123456 from the frame. Again, since this is an 8 digit number, it is a Ford or Chrysler CVIN. In the main Vinstem screen, key ENTER once, then enter the digits ER123456 in the line which requests the CVIN. Since the first digit is an E, which represents the year the car was made, you will not see the screen which requests the year. The next screen will ask you to select the three digits which represent the model.

```
SELECT THE THREE DIGITS WHICH REPRESENT THE CAR:
DIGITS 5, 6, & 7

DIGITS DOORS CAR NAME        BODY TYPE
 A44     2   LASER           HATCHBK
 A54     2   LASER XE        HATCHBK
 C51     2   LE BARON        COUPE
 C55     2   LE BARON        CONVERT
 C56     4   LE BARON        SEDAN
 C59     4   TOWN & COUNTRY  STA WGN
 C53     4   EXECUTIVE       SEDAN
 T46     4   E CLASS         SEDAN
 T56     4   NEW YORKER      SEDAN
 F46     4   NEWPORT         SEDAN
 F66     4   FIFTH AVENUE    SEDAN

SELECT?
```

You obtained the CVIN from a Chrysler Le Baron Convertible. Find name Le Baron in column 3, look for the name convertible in column 4, then enter the digits C55 from column 1. If you are not sure whether the car is a convertible or a sedan, due to its stripped condition, column 2, the number of doors, will help you out. The sedan has 4 doors and the convertible has 2 doors. After you key ENTER, the program will display the types of engines which Chrysler made available for the Le Baron. They are as follows:

```
ENTER LETTER REPRESENTING ENGINE; KEY ENTER IF UNKNOWN:
DIGIT 8

        C  2.6 LITER, L4
        D  2.8 LITER, L4 TBI
        E  2.6 LITER, L4 TURBO
        G  2.8 LITER, V6

    SELECT?
```

Again, we will assume that the engine and transmission are missing, so key ENTER without making a selection. The program will then display the True VINs as shown below:

```
                    VINSLEUTH

THE FOLLOWING ARE TRUE VINs BASED ON CVIN ER123456

                2C3BC55D6ER123456
                2C3BC55E5ER123456
                2C3BC55G3ER123456
                2C3BC55C7ER123456
```

ADMINISTRATIVE SECTION (OPTION 8):

When you key Main Menu Option 8, the following will appear on your screen:

```
ADMINISTRATIVE

1  LIST RECORD OF ENTRIES
2  TYPE RECORD OF ENTRIES
3  ELIMINATE ENTRIES
4  RETURN TO MAIN MENU

SELECT?
```

If in this secondary menu, you select Option 1, you will see the list of entries which you made through Main Menu Option 2. An example is shown below:

```
1 1/30/87  DE26A-56832   1G6AS69N7EE823456  CHARLES A. POPLINGER
2 -1
KEY ENTER WHEN READY?
```

There is room in memory for 100 records, but you should, after 50 entries, key Option 2, which will cause the program to type the list. Below is an example of a typewritten list:

```
NR    DATE     FILE           VIN              REQUESTER
1   1/30/87   DE26A-56832   1G6AS69N7EE823456  CHARLES A. POPLINGER
```

The reason for typing 50 at a time is that your paper will hold 66 lines, and you need some room for a top and a bottom margin. After you have typed the list, you may erase entries by keying Option 3. You will see two screens which have been combined as shown below:

```
ENTER LOWEST RECORD TO BE ERASED?

ENTER HIGHEST RECORDTO BE ERASED?
```

If you want to erase just one record, enter the same record number for both the lowest and highest to be erased.

CARENT (OPTION 6):

Option 6 allows alteration of and addition to the data on which this program relies. If you select Main Menu Option 6 and key ENTER you will see the screen shown on the next page. To avoid inadvertent alteration of the data, Carent is not included on the diskette you have received.

```
CHEVROLET                SUNBURST
PONTIAC                  SPECTRUM
OLDSMOBILE               IMPERIAL
BUICK                    CHRYSLER
CADILLAC                 DODGE
ACADIAN & FIREFLY        PLYMOUTH
NOVA                     MERCEDES BENZ
FORD                     JAGUAR
LINCOLN                  NISSAN
CONTINENTAL
MERCURY
MERKUR

FOR ALTERATION OF CATA CONTACT
THE NATIONAL AUTOMOBILE THEFT BUREAU
(312) 430-2430

KEY ENTER WHEN READY?
```

Data on which Vinsleuth acts has been spot checked against VINs of cars actually on the road. Unfortunately, no data is 100 percent accurate, even when supplied by the manufacturer. If you find a True VIN, enter it into the program, and the program declares the VIN to be in error, please contact me for correction of the data. I will correct the data or rewrite the program to eliminate errors. I will return the corrected diskette to you.

DISCUSSION OF VIN FORMAT:

Pursuant to Chapter 49, Standard 571.115 of the Consolidated Federal Regulations, the Vehicle Identification Number for cars sold in the United States after 1980 must contain 17 digits. The 17 digit VIN has four parts which are the world manufacturer identifier, the vehicle description section, the check digit, and the vehicle identification section.

The world manufacturer identifier is the first three digits. The first first is the origin of the car or where it was assembled. Digits two and three identify the assembling company within the nation where the car was built.

The vehicle description section are digits four through eight. The meaning of the digits in this section are left up to the manufacturer and no two manufacturers standardize the meaning of each of these digits. For example General Motors uses digit 5 to help identify their car models where as, digit 5 in the Ford VIN is a constant P, which means passenger car.

The third section of the VIN, the ninth digit, is the check digit and this section is standard.

The last section of the VIN, digits ten through 17 contain the model year, digit 10, the plant where the car was made, digit 11, and the sequential production number, digits 12 through 17. The meaning of these digits are standardized.

To determine what kind of car you are are concerned with, Vinsleuth first determines the car company which made the car by looking at digits two and three. The program then determines the model year by looking at digit ten. The program is unable to audit this digit.

FOREIGN BUILT CARS:

MERCEDES BENZ:

You may have noticed, when looking at screen two after you selected Vinstem, that Mercedes Benz data is included in the data base of this program. Main Menu Option 2 and Vinstem will audit and correct a Mercedes Benz VIN. Vinstem will also correct the European Mercedes Benz VIN. Suppose you have the Altered VIN, WDBD024C4FF050385, in which digit 5 has been altered from an A to a zero. If you are in Vinstem, key R at either of the two requests, the last six digits, or the CVIN. When you key ENTER, the program will return to the Main Menu. Select Main Menu Option 2, and enter the VIN WDB024C4FF050385. After you Key ENTER again, the program will display the following:

```
                        VINSLEUTH

                   WDBD024C4FF050385

 1  W  ORIGIN            WEST GERMANY
 2  D  MANUFACTURER      DAIMLER BENZ A.G.
 3  B  MAKE              MERCEDES BENZ
 4  D  MODEL             ERROR DIGITS 4 THRU 7
 5  0  STYLE
 6  2  DOORS/ENGINE
 7  4  EUROPEAN NR.
 8  C  RESTRAINT
 9  4  CHECK             0
10  F  YEAR
11  F  PLANT
12-17 SEQ. PRODUC. NR.   050385
                         * * RUN VINSTEM * *

    THE DIGIT SUM IS  330
    THE CHECK DIGIT IS 4
    THE CALCULATED DIGIT IS  0

     * * * * ALTERED * * * *
```

Key Y or key YES to obtain a hard copy of the above screen. The note at the end of the data section wants you to return to the Main Menu and select Option 5. When you do, Vinstem will load, and you will be asked for the last six digits. Enter 050385, and key enter. The next screen will ask for the type of car, so enter DB, which are digits 2 and 3, and key ENTER. The next screen will ask for the model year, digit 10. Refer to the audit print-out, and notice that, since the error is in the first part of the VIN, the year may be correct. Key F for 1985, and key ENTER.

The next screen asks if you want to build the European VIN as shown below:

```
DO YOU WISH TO ASSEMBLE THE EUROPEAN VIN (Y/N)?
```

For the moment we will stay with the U.S. VIN. Key N for no and key ENTER, or you may just key ENTER.

The next screen will display the car lines which Mercedes Benz makes available in the United States.

```
ENTER THE LETTERS AND DIGITS WHICH REPRESENT THE CAR:
DIGITS 4, 5, 6, AND 7
IF UNKNOWN, YOU MAY ENTER THE CARS NAME.

    DIGITS     NAME     EUROPEAN NR.      STYLE
     DB22      190D       201122          SEDAN
     DA24      190E       201024          SEDAN
     AB33      300DT      123133          SEDAN
     AB53      300CDT     123153          COUPE
     AB93      300TDT     123193          STATION WAGON
     CB20      300SD      126120          SEDAN SUPER
     CA32      380SE      126032          SEDAN SUPER
     CA37      500SEL     126037          SEDAN SUPER-LONG
     CA44      500SEC     126044          SEDAN
     BA45      380SL      107045          ROADSTER SUPER-LIGHT

SELECT?
```

The audit indicates an error in digits 4 through 7. Compare the digits D024 with the numbers in the left column as shown above. The closest is DA24. Try entering DA24. If you are not successful in obtaining the theft report after you have built the True VIN, you will have to return to this screen and select the next one closest to your VIN. I would try DB22, next.

The next screen asks for the restraint as shown below:

```
ENTER THE RESTRAINT SYSTEM; KEY ENTER IF UNKNOWN:
DIGIT 8
                C  MANUAL
                D  AIR BAG

          SELECT?
```

The correct value for digit 8 is not known. You may assume that C is correct or you may let the program give you VINs with both C and D in that VIN digit position. Key ENTER and let the program insert both. The next screen asks for the digit which represents the plant.

```
ENTER THE DIGIT WHICH REPRESENTS THE PLANT; KEY ENTER IF UNKNOWN:
DIGIT 11
                F  BREMAN
                G  BREMAN
                H  BREMAN

          SELECT?
```

Mercedes Benz uses several letters to designate the same plant. You may select F or make no entry and just key ENTER. If you do not make a selection, the program will give you VINs with F, G, and H, in the VINs eleventh digit position.

Vinstem will provide the following list of True VINs:

```
                    VINSLEUTH

THE FOLLOWING ARE TRUE VINs BASED ON ENTRIES:

                WDBDA24C4FF050385
                WDBDA24C1FG050385
                WDBDA24C9FH050385
                WDBDA24D3FF050385
                WDBDA24DOFG050385
                WDBDA24D8FH050385
```

If the VIN WDBDA24C4FF050385 had been entered as stolen, you would have found the theft report.

You may have noticed that you can also build the European VIN. The European Mercedes Benz VIN does not have a digit which represents the model year. Therefore if you are one or two years off the true model year you will still see the proper screen which will ask for the six digit European number, digits 4 through 9, as shown below.

```
ENTER THE EUROPEAN NUMBER OF CAR:
DIGITS 4 THRU 9

   DIGITS     NAME     EUROPEAN NR.      STYLE
    DB22      190D       201122         SEDAN
    DA24      190E       201024         SEDAN
    AB33      300DT      123133         SEDAN
    AB53      300CDT     123153         COUPE
    AB93      300TDT     123193         STATION WAGON
    CB20      300SD      126120         SEDAN SUPER
    CA32      380SE      126032         SEDAN SUPER
    CA37      500SEL     126037         SEDAN SUPER-LONG
    CA44      500SEC     126044         SEDAN
    BA45      380SL      107045         ROADSTER SUPER-LIGHT

IF THE EUROPEAN NUMBER DOES NOT APPEAR ABOVE THEN KEY 'E' AND SLELECT
ANOTHER YEAR.

SELECT?
```

In this case we are interested in building the VIN for the 190D. Enter the digits 201122. The next screen will ask whether the car is a left or right hand drive and, the following one will ask whether the transmission is standard or automatic. Assume that you are looking at a gray market German title or you are investigating a shop which makes repairs to foreign cars so they conform to United States VIN standards. Key ENTER at the question mark in both these screens without making entries. The program will display the following four VINs.

```
VINSLEUTH

THE FOLLOWING ARE THE EUROPEAN VINs:

WDB20102410050385
WDB20102411050385
WDB20102420050385
WDB20102421050385
```

Before 1981, the Mercedes Benz VIN contained 14 digits. After the United States passed Chapter 49, Section 571.115 of the Consolidated Federal Regulations, cars made in West Germany contained a W in VIN digit position one. The Daimler Benz Company elected to use DB for VIN positions 2 and 3. The letters WDB are now used by Mercedes Benz in the first three VIN digit positions to designate all the cars they produce, including the cars they sell in the United States. The European VIN now has 17 digits and it is easy to confuse the European VIN which does not have a check digit with the Unites States Mercedes Benz VIN which does have a check digit. The best way to tell is to look at the rest of the VIN. The European VIN will contain only numbers in positions 4 through 17, and the United States VIN, which contains the check digit, will contain letters and numbers.

JAGUAR:

Assume that the True VIN SAJAV1349FC399123, has been stolen and entered into NCIC and that you have the altered VIN SAJAV1349FD399123 on paper. If you are in the Vinstem Menu key R and ENTER to return to the Main Menu. Select Option 2 and key ENTER. When requested, enter the VIN SAJAV1349FD399123. You will see the following:

```
                              VINSLEUTH

                        SAJAV1349FD399123

 1   S  ORIGIN           ENGLAND
 2   A  MANUFACTURER     BRITISH LELAND MOTORS
 3   J  MAKE             JAGUAR
 4   A  MODEL            XJ6 III
 5   V  SPECIFICATION    NORTH AMERICAN
 6   1  BODY TYPE        4 DOORS
 7   3  ENGINE           2.4L  6 CY
 8   4  TRANSMISSION     AUTOMATIC LHD
 9   9  CHECK            6
10   F  YEAR             1985
11   D  PLANT            ERROR DIGIT
12-17   SEQ. PROD. NR.   399123
                         * RUN VINSTEM *

    THE DIGIT SUM IS  325
    THE CHECK DIGIT IS 9
    THE CALCULATED DIGIT IS  6

     * * * * ALTERED * * * *
```

There is an error flag in the data section of VIN digit, position 11. The flag at the end of the data section wants you to go to Vinstem. Key Y to obtain a print-out of the above screen and when you return to the Main Menu, key Option 5. When Vinstem loads, enter the digits 399123 where the program asks for the last six digits. The next screen asks for the model year. Key an F and key ENTER. The next screen shown below asks for the five letters which represent the car.

```
ENTER THE FIVE LETTERS WHICH REPRESENT THE CAR NAME, SPECIFICATION,
BODY TYPE, ENGINE, AND TRANSMISSION; KEY ENTER IF UNKNOWN:
DIGITS 4 THRU 8

THESE ARE ALL THE POSSIBILITIES; KEY IN THE ONES CLOSEST
TO THE AUDITED VIN.

          AV134    XJ6          4 DOORS
          AY134    VANDEN PLAS  4 DOORS
          NV584    XJS          2 DOORS

SELECT?
```

If the VIN audit had indicated errors in VIN positions 4 through 8, you would select the five letters and numbers which are the closest to your Altered VIN. In this case, the audited VIN does not contain error flags in these positions. Key in AV134 and key ENTER.

You will be given the only possible True Vin as shown:

```
                              VINSLEUTH

          THE FOLLOWING ARE TRUE VINs BASED ON ENTRIES:

                        SAJAV1349FC399123
```

Most foreign car manufacturers fit engines to the car. Thus, like Mercedes Benz, Jaguar does not provide optional engines for the various car models they produce. In addition, Jaguar only makes cars at one plant. This is the reason you did not see a screen asking for selection of various engines and plants.

NISSAN (DATSUN):

Suppose you have the altered VIN JN1CZ1483GX100022, from a 1986 Datsun 300ZX, in which the eighth letter was altered from an S to an 8. The True VIN JN1CZ14S3GX100022 has been entered into NCIC as stolen. If you are in Vinstem, key R to return to the Main Menu. Select Option 2, the VIN audit, and enter the altered VIN shown above. The following will be displayed:

```
                        VINSLEUTH

                    JN1CZ1483GX100022

 1   J   ORIGIN
 2   N   MANUFACTURER      NISSAN MOTOR CORP.
 3   1   MAKE              PASSENGER CAR
 4   C   ENGINE
 5   Z   MODEL             DATSUN
 6   1   MODEL             ERROR IN DIGITS 4-8
 7   4   BODY STYLE
 8   S   RESTRAINT
 9   3   CHECK             3
10   G   YEAR              1986
11   X   PLANT
12-17    SEQ. PROD. NR.
                           * RUN VINSTEM *

          DIGIT SUM IS 327
          CHECK DIGIT IS 3
          CALCULATED CHECK DIGIT IS 8

           * * * * ALTERED * * * *
```

When the program asks if you want the above screen typed, key Y, for yes, and key Enter. When the Main Menu appears, select Option 5, key Enter, and Vinstem will load into the computer. Since you have the full VIN, you will rebuild it starting with the last six digits. Enter the digits 100022 and key Enter. The next screen shown below, will ask you to enter digits two and three:

```
ENTER THE TWO DIGIT SYMBOL WHICH REPRESENTS THE CAR:
DIGITS 2 AND 3

        G1  CHEVROLET           81  SUNBURST
        G2  PONTIAC             87  SPECTRUM
        G3  OLDSMOBILE          A3  IMPERIAL
        G4  BUICK               C3  CHRYSLER
        G6  CADILLAC            B3  DODGE
        G7  ACADIAN & FIREFLY   P3  PLYMOUTH
        Y1  NOVA                DB  MERCEDES BENZ
        FA  FORD                AJ  JAGUAR
        LN  LINCOLN             N1/N4  NISSAN CAR (N6) PICKUP
        MR  CONTINENTAL
        ME  MERCURY

  SELECT?
```

The Nissan Motor Corp. which makes Datsun motor vehicles, also makes Pickup trucks. Digits two and three for the car are N1 or N4, and these digits for the pickup are N6. If digits two and three in your altered VIN were N1, you would have a car made in Japan. If they were N4, the car was made at Smyrna, Tennessee. If digits two and three in your altered VIN were N6,

you would be interested in a pickup truck. In any case you would enter the digits N1, N4, or N6. It should be noted here that the only trucks in the program to date are the Datsuns. It is hoped that General Motors, Ford, and Chrysler trucks will be included along with Toyota cars and trucks. In the above screen, key N1 and key Enter.

The next screen will ask for the year the car was made, digit 10. Refer to the VIN audit and note that digit 10 is a G. Key G and key Enter.

The next screen shown below, will list the several models made by Nissan:

```
ENTER LETTER WHICH REPRESENTS THE MODEL:
DIGIT 5
YOU MUST MAKE A SELECTION FROM THIS SCREEN.

          B  SENTRA
          N  PULSAR
          T  STANZA
          M  ST.WGN
          U  MAXIMA
          S  200SX
          Z  300ZX
          D  TRUCK

     SELECT?
```

Refer to the VIN audit and notice that digit 5 is a Z. Key Z and key Enter. If the second and third digits of your VIN were N6, then the fifth digit will be a D which Nissan uses to designate their pickup truck. In this were the case you would enter a D rather than a Z. The next screen, shown below, will ask you to enter 5 digits which will describe the correct car to the program:

```
ENTER THE FIVE DIGITS, IN THE LEFT COLUMN, WHICH REPRESENT
THE ENGINE, MODEL, MODEL TYPE, BODY TYPE, AND RESTRAINT:
DIGITS 4, 5, 6, 7, & 8

     DIGITS    DOORS       CAR NAME
     HZ14S       2       300ZX
     CZ14S       2       300ZX TURBO
     HZ16S       2       300ZX 2+2

SELECT?
```

Refer to the VIN audit and note that these digits are CZ148. The closest is CZ14S. If you build up your VIN with these, enter the VIN in NCIC, and do not get a "hit", then return to this screen and try HZ14S. Key CZ14S and key Enter.

The final screen will display your true VIN as follows:

```
VINSLEUTH

THE FOLLOWING IS THE TRUE VIN:

JN1CZ14S3GX100022
```

INSTALLING VINSLEUTH ON A HARD DISK:

This diskette contains the DOS operating system version 2.1. You may use a hard disk operating system version 2.1 or higher but, you will have to erase the operating system and AUTOEXEC.BAT from this diskette before you try to load the contents of the diskette into your system. The diskette contains BASERUN20.EXE, VINP.EXE, and VINS.EXE, TYPE.DAT, VIN.DAT, ADM.DAT, YEAR.DAT, and all the data on which Vinsleuth relies. BASERUN20 is the catalyst for execution of VINP and VINS. Do not erase it. The compiled program, VINP will cause VINS to load through Main Menu Option 5, and VINS will cause VINP to load by keying an R in the VINS menu.

To load the contents of the diskette onto you hard disk I suggest you make a directory via the DOS command MKDIR\VINPRG\. Then type CD\VINPRG\. Now you may use the DOS command, COPY A:*.* C:\VINPRG*.* at the C prompt. Now store the diskette in a safe place.

To start the program, path to the proper directory and type VINP at the C>. You may go directly to Vinstem by typing VINS at the C> while in the sub-directory.

INSTALLING VINSLEUTH IN A SINGLE FLOPPY DRIVE:

Put the diskette in your default disk drive. Type VINP at the A> to start Vinsleuth. To start Vinstem, type VINS at the A>. The diskette contains the DOS Operating System and AUTOEXEC.BAT. Vinsleuth will self boot if you press CTRL, ALT and DEL at the same time.

DATA:

To date, the program contains car data for General Motors, Ford, Mercedes Benz Jaguar, and Nissan from 1981 through 1986. The program contains car data for Chrysler from 1983 through 1986.

REVISIONS:

This is version 1.85 which is a revision from 1.8. Some users suggested that when selecting cars in the Vinstem program, after entering the CVIN, the screen should show only those cars made at the plant as depicted in the CVIN. That suggestion has been implemented and, both the Vinprogram and Vinstem include Nissan programming.

CINQUIEME PARTIE

PART V

SURVEILLANCE ELECTRONIQUE DES CONDAMNES

ELECTRONIC MONITORING OF OFFENDERS

ELECTRONIC MONITORS

Annesley K. Schmidt[1]

Within the last two and a half years, electronic monitors have burst onto the correctional scene, gaining acceptance from a number of correctional agencies, and attention from the public and the press. A literature about monitors has begun to develop.[2] Discussion of all kinds has been generated but very little scientifically sound research has yet been completed.

In this article, I will focus only on specific aspects of monitors. First, I will define and describe the monitoring technology currently available commercially. Then, I will present the results of a survey of monitors in use on February 15, 1987. Finally, I will briefly discuss some of the issues and questions that still remain to be resolved.

ELECTRONIC MONITORING EQUIPMENT

---

[1]. Annesley K. Schmidt is a Research Analyst at the National Institute of Justice, U.S. Department of Justice, Washington,D.C. The points of view and opinions are those of the author and do not necessarily represent the official position of the U.S.Department of Justice or the National Institute of Justice.

[2] For a review of the literature see: Schmidt, Annesley K.and Curtis, Christine E. "Electronic Monitors"In Belinda R.McCarthy ed. Intermediate Punishments: Intensive Supervision,Home Confinement and Electronic Surveillance Monsey, New York,Criminal Justice Press, 1987: 137-152.

Electronic monitors are devices which use telemetry technology to monitor the offender's presence in a particular place where he or she is required to remain. Usually, the monitors are used to assure that the offender complies with a house arrest or home confinement condition of his release.

Two types of electronic monitoring equipment are presently available. "Continuously signalling devices," constantly monitor the presence of an offender at a particular location. "Programmed contact devices" contact the offender periodically to verify his presence. [3]

Most "continuously signalling devices" have three major components: A **transmitter** is attached to the offender that sends out a continuous signal. A **receiver-dialer** located in the offender's home is attached to his telephone and detects signals from the transmitter. It reports to the central computer when it stops receiving the signal and when it starts receiving it again. The **central computer** or **receiver** accepts reports from the receiver-dialer over the telephone lines, compares them with the offender's curfew schedule, and alerts correctional officials about any unauthorized absences. The computer also stores information about routine entries and exits of each offender so

---

[3]. A list of manufacturers, entitled "Electronic Monitoring Equipment", is available at no change from the National Institute of Justice, National Criminal Justice Reference Service, Box 6000, Rockville, Md, 20850 or 800-851-3420.

that reports can be generated.

There are a number of variations on a "continuously signalling device" available from the six presently known manufacturers of that type of equipment. Transmitters produced by some manufacturers send an altered signal to alert officials if they are tampered with and others do not. The transmitter of one manufacturer sends out a constant signal. However, instead of being relayed over telephone lines, the signal is "heard" by a portable receiver, in the car of the officer who is monitoring the offender. This receiver is tuned to the signal from a specific transmitter when the officer drives within one block. Some use the cellular telephone system to maintain contact between the offender's transmitter and the base, and may include a tracking capacity. Another system communicates with the base station over telephone lines or by using a long-range wireless repeater system.

"Programmed contact devices" provide an alternative approach. They contact the offender at intervals to verify that he is at the location where he is required to be. These devices all use a computer programmed to contact the offender during the monitored hours, usually by telephone, either randomly or at specifically selected times. The computer is also programmed to prepare reports on the results of the call. However, each uses a different method to assure that the response is from the offender

being monitored. One system uses voice verification technology to assure that the telephone is being answered by the offender. Another system requires that the offender wear a device which looks like a wrist watch and is programmed to provide a number unique to that offender at that time. This number appears when a special button on the watch device is pressed and is entered into a touch tone telephone in response to the call. The third system requires a wristlet, a black plastic module, which is strapped to the offender's arm. When the computer calls, the wristlet is inserted into a verifier box connected to the telephone to verify that the telephone is answered by the monitored offender. A fourth system uses visual verification. The final programmed contact requires the offender to carry a digital read-out pager which displays a number to be called to verify the presence of the offender.

Both the continuously signalling and programmed contact devices described above electronically verify the presence of the offender in a specific location. However, offenders are also monitored without electronic verification. The automatic telephoning equipment monitors an offender where the response to the call is recorded but there is no electronic verification that the person responding is in fact the monitored offender.

WHEN WERE THEY FIRST USED?

On December 14, 1984, the Sheriff's Stockade in Palm Beach,

Florida released an offender beginning an innovative community corrections program. This offender was not going into the community unsupervised. He was under home confinement and his presence in his home was being verified by an electronic monitoring device attached to his ankle. That release marked the beginning of programs that electronically monitor offenders. Prior to that and since then, monitoring has been was discussed in the literature [4] and tested on a short-term, experimental basis. However, the Palm Beach initiative has developed into the oldest on-going program of electronically verified supervision in the country.

Since that Palm Beach release, manufacturers have entered the commercial market with significantly different technological approaches to electronic monitoring[5] and programs have been implemented in all parts of the United States. In an effort to assist criminal justice agencies considering the use of this equipment and to provide information to those interested in tracking these developments, the National Institute of Justice undertook a voluntary survey. This paper reports the responses to that survey.

---

[4] For a discussion of the literature about monitors, see Schmidt and Curtis, 1987

[5] A description of the types of monitoring equipment is provided in appendix I.

THE STUDY

As part of tracking of the development of electronic monitors, the National Institute of Justice has maintained a list of manufacturers of electronic monitoring equipment. These manufacturers voluntarily identified the programs using their equipment.

Each program director was contacted and asked for information on each offender who was being monitored on February 15, 1987, the program history and any other information about the program that were easily available. The responses to those letters provided the basis of this report.

RESPONSES

The manufacturers' lists provided contacts with fifty-four (54) monitoring programs in 21 states. Fifty-three (53)programs responded. The programs contacted are in large metropolitan areas, medium-sized cities, small towns and rural areas in all sections of the country. The states in which they are located and the number of programs or monitoring locations is shown in Table I.

TABLE I

STATES BY THE NUMBER OF MONITORING PROGRAMS AND/OR LOCATIONS

States with one (1) program: Arizona, Delaware, Maryland, Massachusetts, North Carolina, Pennsylvania, Texas

States with two (2) programs: Kentucky, Michigan, New Jersey, New York, Utah, Virginia

States with three (3) programs: Colorado, Illinois,Indiana, Missouri

States with four (4) programs: California, Oregon, Tennessee

State with ten (10) programs: Florida

The responses, shown in Table II, indicated that on February 15, 1987, most offenders were monitored in a manner that could be verified. 369 offenders were monitored by continuously signalling devices, that constantly sends out a signal the presence or absence of which is conveyed to and interpreted by a computer to determine if the offender is present when he is supposed to be. 316 offenders were monitored by verified programmed contact devices, where a computer calls the offenders to verify that he is home when required (see Appendix for a description of the equipment and the verification technology). An additional 141 offenders were monitored by programmed contact devices which were not providing verification on those cases.

Thus, continuously signalling devices are used by more programs and on more offenders than were the verified programmed contact devices. However, the sum of the verified programmed contact devices and those without verification indicates more use of programmed contact devices than continuously signalling devices.[6]

TABLE II

NUMBER OF PROGRAM PARTICIPANTS BY TYPE OF MONITORING EQUIPMENT
February 15, 1987

	Monitored with Electronic Verification		Monitored Without Electronic Verification	TOTAL
	Continuously Signalling	Programmed Contact		
TOTAL PARTICIPANTS	369	316	141	826
Percent	44.7	38.3	17.1	100.0
NUMBER OF PROGRAMS WITH				
1 - 5 participants	15	9	1	25
6 - 10 participants	5	2	0	7
11 - 20 participants	9	7	0	16
More than 20 participants	5	4	2	11

---

[6] One location reported an interesting program variation. They use a polygraph in conjunction with the monitor if the offender has a drug or alcohol history. The polygraph may replace the electronic device when the offender's occupation is felt by the staff to preclude the use of a monitor. This was true, for example, for a telephone lineman, a dynamiter and a waitress whose uniform had a very short skirt.

The columns of Table II total to more than the 53 programs included in the survey, because some programs use continuously signalling equipment in combination with a programmed contact device. Two programs include verification by the programmed contact device and two do not. In addition, there is one program that uses all three types of equipment.

The February figures reflect increases in electronic verification and a decrease in the cases using monitors without verification from the findings in December, 1986. (Department of Justice, 1987).[7]

OFFENDER/PARTICIPANT CHARACTERISTICS

The programs provided descriptive characteristics of the 826 offenders who were being monitored. These included age, sex, offense and legal status of the offender as well as the date that the monitoring began. 53.6% of the offenders had been monitored for 6 weeks or less, their monitoring having begun in 1987. At the other extreme, 55 offenders had been monitored longer than 6 months. Almost all of those being monitored were male. There was no difference between the males and the females in terms of the type of equipment being used.

---

7. Since participation in both surveys was voluntary it is not known whether respondents felt that the survey referred only to those being monitored and verified so that those not verified would be irrelevant and therefore not reported or whether the number has in fact decreased.

There were no major difference between the sexes in the age of the offenders being monitored. Males averaged 30.2 years while females averaged 31.2 years. The participants ranged in age from 14 to 78, with 56.2% under 30.

TABLE III

AGE GROUP BY SEX

Age group	Male	Female	TOTAL	Percent
Under 20	57	9	66	8.0
20 to 24	188	12	200	24.2
25 to 29	174	19	193	23.3
30 to 34	136	11	147	17 8
35 to 39	76	18	94	11.5
40 to 49	61	8	69	8.3
50 and over	42	4	46	5.6
Missing	8	3	11	1.3
TOTAL	742	84	826	
Percent	89.8	10.2	100.0	

(T=-.82, P=.415)

The sexes were also similar in terms of offense or sentence status. Most participants (93.5%) were convicted and sentenced.

TABLE IV

SENTENCE STATUS
COMPARED TO OFFENSE

Sentenced	Pretrial	Other and Unknown	Total	Percent

Offense					
Major traffic	268	7	0	275	33.3
Drugs	109	10	0	119	14.4
Crimes vs persons	40	6	1	47	5.7
Property offenses	133	18	0	150	18.2
Sex offenses	21	3	0	24	2.9
Frauds	28	0	0	28	3.4
Non-support	13	0	0	13	1.6
Probation violation	39	1	0	40	4.8
Multiple charges	73	3	0	76	9.2
Other	38	3	0	41	4.9
Unknown	8	0	5	13	1.6
TOTAL	769	51	6	826	100.0

The distribution of offenses is shown on table IV. They cover the full range of more serious criminal charges with major traffic (33.2% of the total), property offenses (18.2%) and drugs (14.4%) predominating. Looking at the categories in more detail, almost four-fifths (78.9%) of those shown in the category major traffic were charged with drunk driving -- driving under the influence, driving while intoxicated, etc. -- and an additional 8.7% were charged with driving while suspended or revoked, an offense often related to drunk driving. However, the drug charges were more evenly distributed over the range of drug offenses: cocaine possession (21.8%) and distribution (10.9%), or controlled substance possession (26.9%) and distribution (24.4%).

Property offenses were dominated by burglary (35.3%), and by theft and larceny (38.0%).

The relative infrequent use of monitors on non-support cases was noteworthy, because monitoring allows the offender to continue to earn income. The data does not indicate whether this reflects a reaction about nonsupport cases in the jurisdictions with monitoring programs, or a prioritization among offenders to be assigned to monitors. It is also possible that the use of monitors on these offenders has never been suggested.

Several of the offense categories (e.g. sex offenses) were more serious than might have been expected to be monitored. Most of these offenders were monitored by programs directed at prison releasees. Having been required to release the offender, the program is doing what it can to continue to protect the community. The three pretrial sex offense cases reflect the problem of categorization schemes which may combine within one category the full range of offense severity.

Probation violators are placed on monitors in some jurisdictions to avoid sending these offenders to crowded prisons. The offender is sanctioned for his violation while the community receives greater protection. There is little information on the effectiveness of this approach.

PROGRAM CHARACTERISTICS

Most of the electronic monitoring programs were recently established. More than half of them had been in operation for less than a year and 21 had been in operation for six months or less.

TABLE V

PROGRAM START DATE COMPARED TO NUMBER OF PARTICIPANTS

Number of Participants	When Program Started: Sept 86 or more recently	Earlier in 1986	Prior to 1986
1 - 10	15	9	3
11 - 20	6	6	2
More than 20	3	4	5
TOTAL	24	19	10

$X^2 = 6.254$ $p \not< .10$

However, surprisingly, as can be seen on Table V, there is no significant relationship between the number of participants in a program and the length of time that the program has been operating. This is surprising in that one might expect programs to start slowly, gradually increasing the number of participants but many programs that have been operating for 6 months or longer

still have few participants, whereas others with a large number of participants have been operating for a short time.

These monitoring programs are run by a wide variety of types of organizations. About half (50.9%) are correctional agencies, either at the state or local level, including departments of corrections, parole boards and probation agencies. Almost a quarter (22.6%) are private monitoring service providers. The remainder are public agencies, including police departments, sheriffs and courts.

TABLE VI

TYPE OF AGENCY PROVIDING MONITORING PROGRAM

COMPARED WITH FEES CHARGED TO THE PARTICIPANT/OFFENDERS

Type of Agency	Do Not Charge for Monitoring	Charge for Monitoring	TOTAL
State or local corrections	13	14	27 (50.9%)
Other public agency	8	6	14 (26.4%)
Private contract provider	11	1	12 (22.6%)
TOTAL	32 (60.4%)	21 (39.6%)	53 (100.0%)

Almost all private agencies and about than half of all the responding programs charge fees to offenders in the monitoring program, as shown on Table VI. Most fees are established based on the ability to pay and on a sliding scale. When a private company provides the monitoring equipment and supervision of the offenders, the fees for the service are usually paid by the offender. Public agencies, who contract directly with the manufacturers and use their own staff to manage the program, meet the costs from the agency's budget or are reimbursed, in whole or in part, by fees charged of offenders who are able to pay.

Besides differences in program sponsorship of the program and fees, the programs also differ in intent. Among the programs were:

- A pre-trial program that monitors the release of those defendants held in jail for 2 weeks or more pending trial and who would have previously remained in jail;

- A town's police department that monitors those charged with or convicted of violations of city ordinances who would otherwise have been held in a county jail that charges the town per diem costs of custody;

- A work release program at a county jail from which offenders can "graduate" to living at home with an electronic

monitor;

- A program for those at risk of a probation or parole failure;

- A local jail with a court-ordered ceiling on its population that uses monitors for less serious offenders in order to make jail space available for more serious offenders; and

- An intensive probation supervision program that uses electronic monitors to augment the efforts of the staff to assure compliance with the house arrest requirement of the program.

Electronic monitoring devices have also helped correctional agencies solve the difficulties of handling unusual cases. For example, placement in a monitoring program enabled one 70 year old repeat drunk driving offender whose health was very poor to remain out of jail. In another jurisdiction, a device was used to monitor a victim of AIDS who was charged with a criminal violation. Monitoring him in the community avoided the problems inherent in his confinement in the close conditions of the jail and allowed him to continue to receive treatment from medical personnel familiar with the disease and with his care.

PROGRAM EXPERIENCES

As of February 15, 1987 at least 3000 offenders have participated in monitoring programs. About 10% of these participants have failed to complete the program satisfactorily. Some programs had not experienced a failure while others had a third or more of the participants fail. The most frequent causes of failure were absconding and failure to abide by curfew. Some offenders failed when tests for alcohol or drugs revealed use of those substances.

While there is no clear explanation of why failure rates vary, selection of participants for the program is clearly important. Some programs have a "right to refuse" anyone recommended for the program if they feel the person is unsuitable or will be unsuccessful. Other programs feel that they must accept anyone recommended by the judge regardless of their determinations about the suitability or appropriateness of the client. In addition, some programs purposely focus on problem cases and so anticipate higher failure rates.

In-program failure generally leads to removal from the program, but some programs have lesser sanctions that they can apply if appropriate. This approach is exemplified by the Tennessee intensive parole supervision program which has 3 phases, each with a minimum 30 days duration. Progress through the phases involves a gradual reduction in controls. Offenders who successfully complete all phases are placed on regular

supervision. If an offender's behavior deteriorates, a variety of options are available, including lengthening the time in the current phase of the program, moving the offender back to the previous phase, making specific program requirements more stringent, lengthening the curfew, or increasing the hours of required community service. (Tennessee Board of Paroles, 1987)

Some programs had assessed their use of monitors and attached their findings to their responses to the survey. Their findings are summarized in Appendix II. Most of these reported that there was insufficient data to form conclusions. Several authors reported on the successful tests of the functioning of equipment.

CONCLUSIONS

This report is based on a one-day snap-shot of offenders monitored on February 15, 1987. It provides one picture of offenders being monitored on that day and of the programs of which they were a part. It can not indicate how long these offender were monitored, whether they successfully completed the program, or if they recidivated after completing the program. A further caveat in interpreting the data is that "snap-shot" counts tend to overstate the proportion of long duration

participants. The conclusions below are reached within those limitations.

Electronic monitors are devices to monitor the house arrest or home incarceration of the offender. They indicate only whether the offender is present or not. They do not indicate his specific location nor do they eavesdrop on conversation. Many of the criticisms of monitors that have been made are based on the assumption that they do or could do more than they actually do. It is difficult to dispute future possibilities since crystal balls differ. However, it will continue to be important to educate all who are interested about what the equipment actually does, how it functions and what it is not capable of doing.

Should monitors be limited only to those who have committed a certain limited list of offenses? At present, some programs concentrate on one offender group, such as drunk drivers. Others define their focus differently and included offenders who have committed a variety of offenses. In the future, this issue will not easily be resolved, since the answer is a function of philosophical and pragmatic considerations. The answer may depend on factors as diverse as what kind of equipment the program has and how tolerant the community is. Thus,in the future, the answer may be yes in some programs or no in others.

At present, many monitoring programs require that participants be

employed. Those who favor this requirement point out that seeking employment is an unstructured activity during which the location of the offender may be difficult to determine. They feel that monitoring of unemployed, able-bodied offenders does not provide adequate protection to the community. On the other hand, those who feel that programs should not be limited to those who are employed point to the potential for discrimination since the unemployed are disproportional poor and members of minority groups. Since the discussion of this question mixes practical issues with philosophical ones, it seems unlikely that it will be resolved and, if it is, there does not seem to be a possible resolution that would please both sides.

Fees for program participation raise questions issues similar to those raised about the requirement that offenders be employed. Many programs feel that the fee question can be handled through a sliding scale that charges offender on the basis of ability to pay. In some cases, these scales charge those most able to pay more than the cost of their program so that they subsidize the program for those less able to pay.

EPILOGUE: SOME THOUGHT ON THE FUTURE OF ELECTRONIC MONITORING

There is an inherent tension as monitoring programs are established. Monitors are an alternative or sentencing option but an alternative to what and option for whom? Some feel that

monitors should only be used as an alternative to incarceration and only for those who would be imprisoned if the monitoring program did not exist. On the other hand, there are those who feel that some offenders are being sentenced to probation, because of the pressure created by prison crowding make prison space unavailable to them. These people feel that the use of a monitor would increase an inappropriately mild sanction to a more appropriate level. Since this debate is part of the ongoing discussion of the purpose of and application of sanctioning, it is doubtful that an easy resolution of this is possible.

In the short period of time since electronic monitors have been available commercially, there has been a growth in their use from one offender monitored in December, 1984 to about 800 in February, 1987. Discussions with the manufacturers indicate that this pattern of growth is continuing. Many have outstanding orders for equipment to be used in new programs or to augment existing programs. In addition they report receiving quite a few inquiries from those considering the establishment of a program. Thus, it seems reasonable to expect that, in the future, at least some of the existing programs will expand and that there will be more monitoring programs in more states and localities.

As information about monitors appears in the press, it is read by marketing and product development officials. They explore the market potential of monitors, try to predict the potential future

market for the devices and determine if their company should enter this market. While it is impossible to determine if any of these companies will enter this field, that seems entirely possible. If new companies enter the field, what kinds of devices will they produce? Will there be a device that is able to track the offender as he moves from place to place? Conversely, some of the manufacturers presently in the field may leave it.

Research presently supported by the National Institute of Justice is examining electronic monitoring equipment. One project will examine the reliability of the different devices by comparing the computer output with activity logs maintained by paid program subjects. Other projects are using the monitors in experiments designed to determine the extent to which community protection is being enhanced by their use.

As the research findings become available, more experience is gained with monitors, and more time passes so that recidivism rates can be determined, it seems likely that clearer indications will develop of the most appropriate use of monitors. A number of future scenarios seem plausible related to different aspects of the question "who should be monitored?"

The debate on whether electronic monitoring should only be used as an alternative to incarceration has the potential for obscuring a more basic question. To what extent and in what way

is electronic monitoring a meaningful form of punishment? Is sentencing someone to electronic monitoring a meaningful sentence or are electronic monitors only to insure compliance with program requirements? Pragmatic experience and philosophical debate will have to combine with legal policy in order to begin to resolve these questions.

No matter how the questions about the use of monitors are dealt with, it is likely that as more and more offenders are monitored the worst case is going to occur. Some monitored offender is going to commit a heinous crime. That occurrence can be expect to stimulate a whole series of questions. These will start with particular questions about the perpetrator -- should he have been released? could this have been predicted? -- and then develop into more general questions -- should offenders be released? should there be a monitoring program? It is hard to predict how this will eventually be resolved in the community where it occurs and even harder to predict its impact nationally. At the same time, it seems likely that it will cause some programs to tighten their requirements, at least temporarily, and a rethinking of such questions as how to respond to offender infractions. It may also cause a temporary slowdown in new program development.

While that worst case situation will be unpleasant and difficult to live through, it seems likely that it will happen, and monitoring programs will survive. The programs that have

established a base of community support will call on their supporters and receive the assistance they need. The programs will find their successes and introduce them to the press so that the other side of the story is told. Then, perhaps changed somewhat in character, monitoring programs will continue and continue to develop. This seems probable since the pressures and concerns that lead to their development in the first place seem unlikely to change.

REFERENCES

Jolin, Annette, Electronic Surveillance Program, Clackamus County Community Corrections, Oregon, Evaluation, Clackamus County Community Corrections, undated.

McGowan, Jeanne, Letter to The Honorable Harrison D. Griffin, February 11, 1987.

Schmidt, Annesley K. & Curtis, Christine E., Electronic Monitoring, In McCarthy, Belinda R. Intermediate Punishments, Criminal Justice Press, New York, 1987._

Whittington, Marie "Adult Detention as an Alternative to Incarceration" Orange County Probation Department, xeroxed, June, 1986.

APPENDIX I

SOME PRELIMINARY FINDINGS ABOUT THE USE OF MONITORS

Pride, Inc., Daytona Beach, Florida, (McGowan, 1987) asked 64 clients to complete a confidential exit interview form and a provided a summary of their responses. Not surprisingly, most offenders rated house arrest far more positively than jail. Almost two-thirds of the participants reported that being on house arrest had altered their life style. The program staff reported that those with short monitoring sentences, 30 days or so, responded that their social life was restricted but they were not really affected. On the other hand, those with sentences of 90 days or more were far more likely to respond that life style changes had occurred. When asked the reason that they responded as they had, the explanations included such comments as "I learned to budget my time." "I no longer have the urge to constantly be going out somewhere and I will probably stay home more often now" and "It made me more happy about my home environment and now I find myself staying home more and enjoying it." Another offender described himself before monitoring as leaving work, going to a bar with the boys and then sometime in the evening going home drunk. While being monitored, he had to omit the bar so he went home and got to know his wife and son. He felt that his habit of the bar had been interrupted so that after the monitoring ended he would continue to go home.

Orange County, California, sent a report (Whittington, 1986) describing the first six months of their program. They screened 127 inmates from the jail which resulted in 51 participants, 11 of whom were people with handicaps or serious medical problems who would have been held in the jail's medical ward if not for the program. Those placed in the program were 93% male, 67% non-minority white, 26% hispanic, 93% had no prior felonies, were regularly employed, 85% were charged with driving under the influence, 88% were classified as having an occasional or frequent problem with alcohol abuse, and 98% were rated as "motivated to change". The Orange County program uses programmed contact monitoring device which telephones the offender who verifies his presence by responding to questions and then inserting a wristlet in a verifier box. Initially, the instructions to the offenders were given only in English, but Spanish and Vietnamese have been added. One technical violation, possession of beer and a small amount of marijuana, occurred, but there were no new law violations.

Dr. Annette Jolin (undated) has recently completed an evaluation of the electronic surveillance program in Clackamus County,

Oregon which has been operating for a longer time. The report provides statistical information on the first 96 offenders to complete the program, 52% of the whom had been charged with drunk driving and 11% with driving while suspended. These offenders spent an average of 33 days under house arrest, with 53% being monitored by a program contact device, 40% by a continuously signalling device and 8% switched from one system to the other. The report also discussed the problems experienced with the functioning of each type of equipment.

The Clackamus County report discussed the program outcomes for these offenders, which did not involve the loss or destruction of any equipments. 90% of these offenders successfully completed the program. Of the 10 offenders who failed, only one was charged with a new crime. Post-program recidivism was examined when the time since program termination ranged from 6 to 18 months. 27% (25 of 95) had been rearrested in Oregon, most within six months of ESP termination.

SURVEILLER ET PREVENIR:
L'ASSIGNATION A DOMICILE SOUS SURVEILLANCE ELECTRONIQUE

par:

Pierre LANDREVILLE
Directeur
Ecole de criminologie
Université de Montréal

La technologie est en train de transformer de façon radicale, comme le souligne entre autres G.T. Marx[1], notre conception de la vie privée et de la liberté individuelle, dans la mesure où elle permet de nouvelles formes de surveillance plus extensives et intensives que tout ce que nous connaissions jusqu'à présent. L'accumulation de données personnelles dans des fichiers informatisés, le couplage de ces fichiers, l'utilisation de caméras vidéo dans les endroits publics, les magasins, à l'usine, la généralisation des tests d'urine ou de sang dans la sélection et la gestion du personnel, la mise en place de systèmes de surveillance électronique pour contrôler et "suivre à la trace" des personnes, ne sont que quelques-uns des éléments de cette nouvelle technologie.

Cette surveillance peut avoir une portée générale, lorsqu'on accumule des informations sur la plupart des individus et que l'on tente de prévenir les comportements indésirables et induire la conformité de tous, mais elle peut être plus spécifique, lorsqu'elle vise un contrôle intensif d'une population donnée, telle celle gérée par le droit pénal.

Il sera ici question de cette surveillance spécifique des criminalisés "grâce" au progès de l'électronique. Nous verrons tout spécialement l'assignation à domicile sous surveillance électronique, qui se développe comme un champignon aux Etats-Unis, ainsi que l'impact de ce développement sur la transformation du contrôle social.

L'assignation à domicile, ou l'obligation pour un contrevenant de ne pas quitter son domicile durant certaines heures, ordinairement entre ses heures de travail, est imposée par le tribunal comme une des conditions dans quelques ordonnances de probation ou lors de la remise en liberté avant procès. Une telle obligation figure aussi, occasionnellement, comme une des conditions de la libération conditionnelle. En 1976, la Commission de réforme du droit du Canada proposait d'inclure parmi les mesures sentencielles à la disposition du tribunal "l'assignation de résidence" qui consisterait en un "engagement d'habiter une résidence donnée, pendant une période déterminée en sus ou au lieu de toute autre

mesure". Cette résidence peut être le lieu de résidence habituel du contrevenant[2]. Dans plusieurs pays, c'est aussi une mesure administrative prise contre des opposants ou des dissidents politiques.
Ces dernières années, la surpopulation des prisons américaines a suscité un grand intérêt pour ce que l'on appelle Home confinement ou Home incarceration. Pour plusieurs, cette mesure est d'autant plus attrayante qu'elle peut être assistée par la surveillance électronique. En fait, même si l'assignation à domicile peut se réaliser sans surveillance électronique, c'est cette dernière qui a moussé l'intérêt pour la première et c'est cette nouvelle technologie que l'on tente de promouvoir à grand renfort de publicité et par un "lobbying" important auprès des administrateurs de la justice et des législateurs. C'est elle qui retient pour l'instant notre attention.

I- La surveillance électronique, aujourd'hui et demain.

Il y a déjà plus de vingt ans, un américain le Dr. Ralph K. Schwitzgeber et son équipe[3] proposèrent la surveillance électronique (Electronic monitoring) des contrevenants. Les premiers projets pilotes dans le système pénal ont eu lieu en 1983 et 1984, entre autres au Nouveau-Mexique et en Floride[4], mais se sont répandus très rapidement, de sorte qu'à la fin de 1986 il y avait quarante cinq (45) programmes du genre dans vingt (20) États américains.[5] Les articles à ce sujet se sont aussi multipliés ces dernières années [6] et le Comité d'étude sur les solutions de rechange à l'incarcération, mis sur pied par le Solliciteur général du Québec, a dû se pencher sur cette question.[7]

La surveillance électronique est actuellement réalisée au moyen de systèmes passifs et actifs.[8] La technologie dite "active", celle qui est la plus souvent utilisée, est généralement réalisée au moyen d'un système qui comprend trois éléments: 1) un transmetteur miniature, fixé de façon inamovible à la cheville du contrevenant, qui transmet un signal

dans un rayon de 60 à 70 mètres; 2) un récepteur-transmetteur situé dans la résidence du contrevenant, près d'un téléphone, qui capte et relaie le signal à un ordinateur central par la ligne téléphonique; 3) un ordinateur central qui reçoit le signal et produit un rapport lorsqu'un des surveillés n'émet plus pendant les heures prescrites. Un autre appareil n'utilise pas le téléphone. Il s'agit aussi d'un petit émetteur, fixé de façon continu. Un récepteur portatif, installé dans la voiture du surveillant, capte le signal de cet émetteur, lorsque le véhicule est situé dans un certain rayon de la résidence du contrevenant.

La technologie dite "passive" utilise le téléphone pour vérifier périodiquement si le contrevenant est à l'endroit désigné. Ce dispositif, qui peut fonctionner selon plusieurs modalités, utilise toujours un ordinateur central programmé pour téléphoner, de façon aléatoire ou selon un horaire pré-établi, au contrevenant durant les heures d'assignation à résidence. Selon une première modalité, l'information est enregistrée sur une cassette et sur l'imprimante de l'ordinateur. Celui-ci enregistre le numéro composé, la réponse, le moment de l'appel, si la ligne était occupée, si l'appel n'a pas pu être acheminé, si on a raccroché ou s'il n'y a pas eu de réponse. La personne responsable de la surveillance, l'agent de libération conditionnelle, par exemple, peut lire périodiquement le rapport produit par l'ordinateur et écouter l'enregistrement. Il peut ainsi vérifier si c'est bien le contrevenant qui a répondu. On peut aussi munir le contrevenant d'un bracelet inamovible retenant un petit module de plastique. Le contrevenant doit insérer le module dans un appareil relié à son téléphone, de façon à s'assurer que c'est bien lui qui répond à l'appel de l'ordinateur. Dans un autre cas, c'est un identificateur de voix qui identifie le contrevenant. Enfin, on peut remettre au contrevenant une montre bracelet inamovible programmée pour produire un chiffre spécifique lors de chaque appel. Le contrevenant doit composer ce nombre sur son téléphone, en réponse à l'appel de l'ordinateur.

La technologie favorisant la surveillance à domicile, bien qu'elle en soit à ses premiers balbutiements, s'est développée en progression géométrique ces dernières années. Une technologie semblable, réalisée dans d'autres domaines, ou sur le point de l'être, permettra un contrôle et une surveillance encore bien plus "efficace". La transmission de signaux et d'informations rend actuellement possible de localiser et de suivre le déplacement d'un objet, d'un animal ou d'une personne et de transmettre des informations physiologiques à leurs sujets. Dans le domaine spatial, on transmet régulièrement des informations sur la respiration, la température du corps, la pression artérielle, le rythme cardiaque, et d'autres données physiologiques d'êtres vivants circulant dans l'espace. On utilise une technologie semblable pour étudier le déplacement et les habitudes de vie de certains oiseaux, animaux terrestres ou poissons. Enfin on peut aussi localiser de façon très précise des signaux de détresseémis par des personnes égarées. Au Québec, par exemple, on étudie la mise au point d'une montre émettrice qui pourrait permettre de localiser facilement les chasseurs perdus en forêt. Des satellites captent déjà les signaux de détresse et permettent de localiser des avions ou des bateaux en perdition.

Les émetteurs, utilisés dans toutes ces occasions, peuvent être externes: des montres, des bracelets, des colliers, des bagues, portées par l'animal ou la personne à retracer. Ils peuvent aussi être internes, constitués par exemple d'appareils miniaturisés qui peuvent être avalés par la personne ou l'animal, ou que l'on peut implanter sous la peau ou ailleurs dans l'organisme.

Les progrès de la technologie n'ont pas manqué de susciter des hypothèses d'application dans le domaine pénal. Par exemple, dès 1971, J. Meyer[9] envisagea un système de surveillance qui s'étendrait à la majorité des grandes villes américaines et impliquerait des millions de personnes accusées ou déjà condamnées. Ces personnes seraient munies d'émetteurs, et des récepteurs, placés ici et là, capteraient leurs signaux pour les relier par lignes téléphoniques à un ordinateur central. On pourrait

ainsi localiser toutes les personnes surveillées et détecter celles qui violent certaines conditions de leur remise en liberté, telle la restriction de circuler hors d'un certain territoire. Selon Meyer:

> "Parce qu'il nous fournit la quasi-certitude que l'infracteur sera arrêté et condamné, le système peut prévenir les crimes sans isoler irrévocablement le contrevenant de la société. Ainsi une surveillance intensive et des peines légères se substitueraient à une surveillance légère et de fortes peines..." (10) (11)

De leur côté Ingraham et Smith(12) ont eux aussi imaginé des utilisations peu rassurantes. Ainsi écrivent-ils, en 1972:

> "A la lumière de l'état des recherches, il semble tout à fait possible et réalisable d'utiliser la télémétrie, comme méthode de contrôle, pour surveiller des êtres humains, pour obtenir des données physiologiques ainsi que sur leur système nerveux, et pour stimuler leur cerveau, à distance, par des ondes électriques... Certaines données physiologiques, telles la respiration, la tension musculaire, la présence d'adrénaline dans le sang, associée à la connaissance de l'endroit où se trouve le sujet, peuvent être particulièrement révélatrice. Ainsi, si un libéré conditionnel, qui a déjà commis des cambriolages, est dépisté dans un quartier commercial (précisément près de boutiques fermées pour la nuit) et que ses données physiologiques révèlent une accélération de son rythme respiratoire, une tension musculaire inhabituelle et une augmentation de son taux d'adrénaline, on peut facilement deviner qu'il y a quelque chose de louche. L'ordinateur pourrait alors, après avoir soupesé les probabilités, en venir à la conclusion d'avertir les policiers ou l'agent de libération conditionnelle pour qu'ils puissent intervenir. Si on avait déjà implanté un transmetteur dans le sujet, ils pourraient transmettre un signal électrique qui lui ferait abondonner ou oublier son projet." (13)

Récemment, M. G. Ruygrok proposait, dans le bulletin d'information de l'Association canadienne de la justice pénale (auparavant de l'Association canadienne de criminologie),

> "une mise en liberté avant terme en utilisant la surveillance électronique. Cette méthode alternative de pister et de surveiller devrait procurer une protection efficace au public. Les détenus éligibles à la libération conditionnelle et soumis à

> un tel système de surveillance auraient le choix de demeurer incarcérés ou: 1) de porter un anneau, un collier ou un bracelet jusqu'à l'expiration de leur sentence; 2) de consentir à l'implantation de l'appareil (pour les condamnés à perpétuité); 5) d'encourir les frais de cette surveillance électronique... Des mécanismes sophistiqués de pistage dévoileraient les allées et venues des détenus au moyen d'un réseau informatisé. Ce système national de pistage dévoilerait, sur le champ, les irrégularités aux forces policières et au surveillant des cas... La technologie canadienne des télécommunications pourrait inventer un système avancé qui puisse détecter un condamné à perpétuité portant un transpondeur implanté sous la peau. Sachant qu'il peut être repéré en tous lieux, ce système devient un moyen de dissuasion à toute nouvelle activité criminelle..."(14)

Même si cette proposition "ne reflète pas nécessairement les vues de l'Association canadienne de justice pénale", elle donne une idée des hypothèses qui sont actuellement en voie d'être considérées.

Enfin, il est possible d'imaginer plusieurs autres hypothèses d'application de cette technologie qui, à notre connaissance, n'ont pas encore été mentionnées dans les écrits à ce sujet. On pourrait par exemple concevoir que certains groupes (les policiers par exemple) ou certaines institutions, (les banques par exemple) pourraient posséder des récepteurs capables de détecter les personnes en libération conditionnelle, qui rôdent à proximité, et prendre alors les mesures jugées appropriées.

L'utilisation de cette technologie à l'intérieur du système pénal soulève de nombreux problèmes et on peut d'ores et déjà s'interroger sur le sens de ces transformations par rapport au contrôle social. En premier lieu, l'utilisation de la surveillance électronique constitue une menace pour les libertés individuelles et un risque sérieux d'escalade du contrôle pénal.

II- Une menace pour les libertés individuelles

La surveillance électronique amènera la personne surveillée à devoir se défendre, à prouver son innocence. La mise en place d'un tel système repose sur le postulat qu'il est efficace et assure une surveillance continue du contrevenant. S'il n'émet plus, c'est qu'il est sorti du périmètre autorisé. Aussi, à chaque fois que son nom ou son numéro apparaîtra sur le moniteur, on supposera que le contrevenant est fautif. A chaque fois qu'il n'émet pas, il devra être en mesure de s'expliquer. Il devra rendre compte de ses allées et venues et éventuellement apporter des preuves à l'agent de surveillance qu'il n'est pas fautif. Il devra démontrer qu'il avait une raison majeure de s'absenter ou que c'est le système qui a fait défaut, qui n'a pas transmis le signal adéquatement. A ce stade, devant l'agent de surveillance ou l'agent de la paix, dans son contact quotidien avec l'administration de la justice, la personne doit faire face à une sorte de renversement du fardeau de la preuve. Même si un tribunal n'accepterait pas comme preuve de la culpabilité le fait que l'émetteur n'ait pas transmis, il faut réaliser que les tribunaux n'interviendraient qu'exceptionnellement dans la gestion quotidienne de la surveillance: les contrôles à domicile lorsqu'on n'émet pas, les demandes de justification, les soupçons, la suspension du privilège de purger sa peine à domicile et même le retour en institution. L'utilisation de cette technologie soulève donc un danger considérable pour les libertés fondamentales.

III- L'escalade du contrôle pénal.

Il y a, d'autre part, un risque d'escalade du contrôle pénal. Le contrôle électronique pourrait s'appliquer à des contrevenants qui n'auraient été soumis à aucun contrôle, à d'autres qui en auraient subi un beaucoup moins intensif et, règle générale, il ne serait probablement pas une mesure de

substitution à l'emprisonnement. Selon la métaphore de plus en plus répandue,(15) le filet du contrôle pénal s'élargit, il se diversifie et ses mailles deviennent plus serrées.

Il y a, tout d'abord, lieu de croire que l'assignation à domicile sous surveillance électronique deviendrait très populaire auprès des administrateurs de la justice et des juges, dès qu'elle serait réellement fiable et peu coûteuse. On l'imposerait sans doute à des contrevenants qui ne sont actuellement soumis à aucun contrôle, qui sont remis en liberté avant procès, qui ont une amende, un sursis, une probation ou une sentence suspendue. Actuellement, dans plusieurs cas, le tribunal évalue que le prévenu n'a probablement pas besoin de surveillance ou il n'impose pas de surveillance, parce qu'il considère que les conditions ne seront souvent pas respectées ou parce qu'on a pas vraiment les moyens de faire une surveillance adéquate. Une surveillance "douce", efficace et peu coûteuse aurait facilement raison de ces hésitations ou ces réticences. Déjà, l'utilisation que l'on fait de la surveillance électronique pour les conducteurs en état d'ébriété, à qui on imposait une amende auparavant, illustre bien ce risque.(16)

En second lieu, il apparaîtrait encore plus normal d'imposer la surveillance électronique à des délinquants en probation, qui ont un sursis avec mise à l'épreuve ou une libération conditionnelle, qui doivent actuellement respecter un couvre-feu, lorsqu'ils ne sont pas au travail. La surveillance électronique ne serait perçue que comme un moyen de faire respecter l'ordonnance du tribunal ou de la Commission des libérations conditionnelles. On conviendra, cependant, que cette surveillance continue est plus intensive qu'une surveillance sporadique par des policiers ou des agents de probation ou de libération conditionnelle. La mesure serait encore plus punitive si, comme c'est ordinairement le cas aux Etats-Unis, on obligeait le contrevenant à payer, du moins en partie, les coûts de la surveillance électronique. On peut aussi concevoir, que les tribunaux ou les commissions de libération conditionnelle imposeraient plus souvent un couvre-feu, s'ils avaient des moyens efficaces et peu

coûteux de le faire respecter. Dans ce cas, la surveillance électronique serait une restriction supplémentaire de liberté, plus coûteuse et moins humaine que la mesure qui aurait été imposée autrement.

Mais ce ad-on effect n'existerait pas, dira-t-on, si, comme le prétend le discours actuel, l'incarcération à domicile remplaçait vraiment des peines d'emprisonnement. On peut douter qu'il en serait généralement ainsi. Deux finalités de la peine, la dénonciation et la neutralisation, sont généralement invoquées pour justifier le recours à l'assignation à domicile avec surveillance électronique comme solution de rechange à l'incarcération. Si ces deux finalités ou sous-finalités, ne sont que des dimensions d'une finalité principale, réduire les comportements prohibés, la première est d'ordre plutôt symbolique et s'adresse aux citoyens en général, alors que la seconde vise celui qui vient de commettre une infraction.

Notre analyse et le résultat de consultations menées par un comité québécois(17) nous portent à croire que, dans la logique du système pénal, l'assignation à domicile sous surveillance électronique n'est pas perçue comme une mesure adéquate pour remplacer l'emprisonnement lorsque le tribunal vise la dénonciation d'un comportement hautement répréhensible. Il semble que nous soyons ici devant une alternative: a) si le comportement est hautement répréhensible, l'assignation à domicile n'est pas une mesure assez sévère pour le dénoncer; b) si l'assignation à domicile semble adéquate pour dénoncer le comportement, il y a tout lieu de croire que l'amende ou les travaux communautaires (ou d'intérêt général) pourraient être avantageusement utilisés.

Il semble bien en effet que plusieurs perçoivent l'assignation à domicile sous surveillance électronique comme une peine mineure, peu crédible pour dénoncer un comportement hautement répréhensible. Il n'est pas certain que, pour les juges, les procureurs et une partie du public, cette peine exprime une grande réprobation sociale. Plusieurs citoyens, des personnes âgées ou certains malades, sont forcés de rester à domicile pour de

longues périodes et cette restriction s'apparente, d'une certaine façon, à celle qu'on imposerait aux contrevenants assignés à domicile. Il est donc concevable que pour plusieurs, le fait d'être confinés chez soi, tout en continuant à bien boire et bien manger, à recevoir des amis et à bien s'amuser, n'a rien d'une peine bien sévère. Cette analyse est confirmée par le fait que souvent, aux Etats-Unis, on établit une table d'équivalence entre la détention et la surveillance électronique. Un jour de détention équivaut à 3 ou 4 jours de surveillance électronique.(18) Pour atteindre une dénonciation adéquate, il semble qu'il faudrait multiplier par 3 ou par 4 la durée de la peine.

Par ailleurs, l'assignation à domicile avec surveillance électronique ne serait probablement pas jugée plus adéquate, comme solution de rechange à l'emprisonnement, pour punir ou intimider un contrevenant ou comme mesure de dissuasion générale. Ici aussi, soit que la mesure n'est pas perçue comme assez sévère pour être une solution de rechange à l'emprisonnement, soit qu'elle est jugée adéquate pour punir, intimider ou dissuader, auquel cas d'autres mesures telles la probation, l'amende ou les travaux communautaires pourraient s'y substituer avantageusement.

Cette perception de l'emprisonnement à domicile sous surveillance électronique comme une peine "banale" "peu crédible" est certes favorisée par ce que d'aucuns, tel Pires (1986), ont appelé la dévalorisation anormale du temps par la justice pénale. La présence de peines maximales disproportionnellement élevées pour un grand nombre d'infractions et l'escalade des peines imposées, ou réellement purgées, depuis quelques années, ont contribué à établir ce "tarif inflationniste"(19). Que peut représenter l'emprisonnement chez soi, si la peine minimale pour importation de drogues est de sept ans, et si on peut être condamné à une peine ferme d'un minimum de 25 ans? Les coûts sociaux et l'effet stigmatisant de cette nouvelle forme d'incarcération, tant pour le contrevenant que pour sa famille, le fait qu'elle créé une main d'oeuvre captive très vulnérable à l'exploitation, ne sont jamais mentionnés et semblent tout à fait ignorés.

Le tribunal peut aussi imposer une peine pour neutraliser le contrevenant, pendant un certain temps, au moyen de l'incarcération. Dans la logique même du pénal, l'emprisonnement peut se justifier dans ce cas s'il s'agit d'un comportement violent et qu'il y a lieu de croire que le contrevenant constitue un danger réel et imminent pour autrui, ou qu'il s'agit d'un comportement répétitif très répréhensible. Mais il semble bien que les législateurs, et les tribunaux, soient tout à fait réticents à utiliser l'assignation à domicile avec surveillance électronique pour des personnes qui ont commis des infractions comportant de la violence. Les programmes américains en cours refusent généralement les personnes qui ont commis des crimes contre la personne, des infractions sexuelles, ou celles qui ont des problèmes d'alcool ou de drogue.(20)

Il est donc possible de prétendre, que l'assignation à domicile sous surveillance électronique ne serait généralement pas perçue et utilisée comme une solution de rechange à l'incarcération, mais serait plutôt une mesure qui viendrait s'ajouter à d'autes peines ou a une libération conditionnelle, "pour assurer une surveillance plus adéquate".

IV- La transformation du contrôle social

Toutes les possibilités de surveillance, qu'offre la technologie, n'auront pas seulement des effets quantitatifs sur le contrôle pénal, mais probablement un effet qualitatif sur le contrôle social en général. Cette technologie participera à la transformation du contrôle social.

Le contrôle social des marginaux a connu une profonde transformation dans les sociétés occidentales industrialisées à la fin du XVIIIe et au début du XIXe siècle. Cohen (1985, p. 13) met l'accent sur quatre changements majeurs: 1) L'intervention accrue de l'Etat dans le contrôle de la déviance; 2) la différentiation et la classification des déviants en des catégories de plus en plus fines; 3) l'enfermement des déviants et en

particulier l'émergence de la prison comme lieu et instrument de transformation et de punition des criminels; 4) le déclin des châtiments corporels, le remplacement du corps par l'esprit comme objet de discipline.

Depuis quelques années, des études sur le contrôle social ont soulevé l'hypothèse que nous sommes peut-être entrés dans une nouvelle phase de transformation. On se demande que deviennent le rôle et la place de la prison comme moyen de contrôle social et, par extension, quelle est la place du système pénal dans l'élaboration et l'application des normes sociales.

Plusieurs auteurs, plus ou moins influencés par Foucault (1975), formulent à ce sujet des hypothèses convergentes. Dans nos sociétés, le pouvoir doit s'exercer aux moindres coûts (économiques et politiques) possibles et ses effets doivent être intensifs et extensifs et pénétrer tout le corps social. Pour Garland (1985), par exemple, "Dans les "démocraties avancées" où toutes les classes doivent bénéficier de la citoyenneté et de la sécurité, on ne peut plus imposer la discipline par la répression et l'exclusion. On doit désormais utiliser des modalités, plus raffinées et discrètes, qui seront cependant plus systématiques, intensives et extensives." (p. 247) (21)

D'une façon un peu plus concrète, et ce, malgré les discours divergents sur la "décarcération", (22) la déjudiciarisation, la décriminalisation et le désinvestissement de l'Etat, il est possible de synthétiser certaines des grandes transformations actuelles dans l'économie des peines, dans le recours au système pénal et dans l'application du contrôle social, autour des quatre tendances suivantes: 1) une augmentation du contrôle étatique, tant pénal que non pénal; 2) une stabilité, ou même parfois une augmentation des taux d'incarcération; 3) une diminution de l'utilisation relative de l'emprisonnement dans l'arsenal pénal; 4) un passage de la moralisation des esprits vers une surveillance accrue et un contrôle des comportements.

1- Augmentation du contrôle pénal et non-pénal

Une des constatations les plus fréquentes est que l'appareil pénal étatique n'a cessé de croître et d'avoir un impact de plus en plus considérable, tout particulièrement durant les dernières décennies. Cette croissance s'observe à tous les stades du processus pénal.

On assiste tout d'abord à une inflation législative et, de façon encore plus marquée, à une prolifération de la réglementation étatique: les comportements des individus et les activités des institutions qui sont régies par l'Etat vont en augmentant. La majorité de ces infractions ont vraisemblablement été créées depuis la Seconde guerre mondiale. Une recherche effectuée sur le droit pénal provincial du Québec a constaté "qu'au cours de cette dernière décennie (1965-1975), on a créé presque autant d'infractions ou de peines nouvelles qu'on ne l'avait fait au cours du siècle précédent" (Brissette, 1977).(23)

Un autre élément important de l'appareil pénal étatique est l'appareil policier. Même si les activités des corps policiers ne sont pas toutes reliées au fonctionnement du processus pénal ou du contrôle social, elles représentent un des axes privilégiés du contrôle social pénal étatique. L'appareil policier a, lui aussi, subi une expansion considérable depuis un siècle. Par exemple, le taux de policiers par 100 000 habitants au Canada est passé de 45 en 1901 à 143 en 1961 et à 221 en 1980. depuis la Seconde guerre mondiale, le taux de policiers a doublé au Canada(24); ces taux ont suivi un mouvement semblable aux Etats-Unis.

Par ailleurs, Anthony Bottoms (1983) rapporte qu'il y a eu, dans la plupart des pays occidentaux, une augmentation dramatique du nombre de personnes condamnées depuis la guerre. Ce phénomène, qui témoigne lui aussi de l'augmentation du contrôle social pénal étatique, se constate aussi au Canada. Le taux de condamnation pour des actes criminels, par 100 000 personnes de 16 ans et plus, est passé d'environ 300 en 1950, à 500 en 1973 et, en 1973, il était 5 fois plus élevé qu'au début du

siècle. Celui des condamnations pour des infractions sommaires est presque 15 fois plus élevé qu'en 1900. (25) Ces quelques éléments illustratifs ne laissent aucun doute sur l'augmentation du contrôle social pénal étatique.

Même si nous avons parlé d'une inflation des lois à caractère pénal au cours des dernières décennies, il faut reconnaître que les peines prévues par ces lois sont rarement appliquées et, qu'en fait, elles n'ont pas souvent pour but la punition mais la réparation, le rétablissement d'un équilibre rompu, ou sont avant tout à caractère "restitutif", comme les lois fiscales par exemple. Dans d'autres cas, des législations pénales ont surtout des visées régulatrices en mettant l'accent sur la conciliation et la négociation des conflits. Ponsears et Cuper (1981) ont souligné le caractère régulateur des législations belges dans le domaine de l'inspection du travail. Aussi, y a-t-il une application différentielle de ces diverses lois qui répondent à des logiques et des finalités différentes. Il nous a semblé préférable de les citer en parlant du contrôle social non pénal même si elles prévoient toute l'application des peines.

Ces lois sont souvent appliquées par des inspecteurs qui perçoivent leur rôle surtout comme étant préventif (Bottoms, 1983) et qui ont souvent des pouvoirs beaucoup plus polyvalents que les simples agents de la paix. Ils peuvent, et dans certains cas, ils doivent, donner des avertissements, réprimander, donner des conseils sur les façons de remédier à une situation, favoriser la conciliation entre des parties, faire en sorte que quelqu'un se conforme à une norme, améliore sa compétence, dédommage une partie, etc. Tout cela avant de recourir à la voie pénale.

Parfois, ces inspecteurs oeuvrent au sein d'organismes qui ont des pouvoirs de contrôle encore plus étendus. Ces organismes (commission, régie, office, bureau de révision, tribunaux), souvent appelés tribunaux administratifs, se sont aussi multipliés au cours des deux dernières décennies. Leur mission est très vaste. Certains ont une activité de

surveillance et de contrôle d'un secteur quelconque de l'activité économique et social. Ils ont pour mission d'appliquer une politique gouvernementale en prenant des décisions suivant un pouvoir discrétionnaire quelquefois très étendu. D'autres sont chargés d'appliquer une loi particulière, en tranchant des litiges ou en prenant des décisions à portée individuelle.

Ces organismes sont souvent habilités à saisir les tribunaux civils et pénaux pour obtenir l'exécution des décisions qu'ils prennent à titre de sanction, mais ces pratiques sont peu fréquentes par rapport à l'ensemble des activités de contrôle de ces organismes. Ils ont plus souvent recours à d'autres styles de contrôle social que le style punitif, (26) et on peut ici parler d'extension du contrôle social étatique non-pénal.

2- Stabilité (ou même augmentation) des taux d'incarcération

Une des façons les plus adéquates de mesurer l'évolution d'une population pénitentiaire, ou de comparer plusieurs populations pénitentiaires est d'utiliser le taux d'incarcération à un moment donné, ou le rapport du nombre de personnes incarcérées à un moment donné par 100 000 habitants(27).

En 1977, Scull a analysé les taux d'institutionnalisation dans les prisons et les hôpitaux psychiatriques aux Etats-Unis et en Grande-Bretagne de 1960 à 1975 environ. Il est arrivé à conclure de l'existence d'un mouvement de "décarcération" qu'il expliquait, entre autres, par la crise fiscale à laquelle doivent faire face ces deux pays, et par l'existence de mesures d'aide sociale qui peuvent être des solutions de rechange à l'institutionnalisation.

Mais, ayant pris une période relativement courte, Scull a été induit en erreur par une baisse des taux d'incarcération qui s'est produite dans plusieurs pays, dont les Etats-Unis et le Canada, au début des années '70. Aux Etats-Unis, le taux d'incarcération est passé de 192 à 175 de

1960 à 1970, tandis qu'au Canada, il s'est maintenu au-dessous de 85 de 1971 à 1974 alors qu'il avait été de 100 et plus de 1961 à 1965. Si l'on regarde ces chiffres sur des séquences plus longues, l'on constate qu'au Canada, le taux d'incarcération par 100 000 habitants est étonnamment stable depuis 50 ans,(28) se maintenant presque toujours entre 90 et 100 et atteignant son plus bas niveau en 1974 (82) pour remonter à 100 en 1980. Aux États-Unis par contre, où il est actuellement plus du double de celui du Canada, il était près de 100 au début du siècle(29).

Récemment on a définitivement rejeté cette hypothèse de la "décarcération"(30). Il y a au moins une stabilisation (ou même parfois une augmentation) des taux d'incarcération dans la plupart des pays occidentaux industrialisés.

3- Une diminution de l'utilisation relative de l'emprisonnement

Bottoms (1983) a attiré notre attention sur le fait que, malgré l'augmentation considérable du nombre de personnes en prison et de celles placées en probation, l'amende était la sanction pénale qui avait subi l'accroissement le plus spectaculaire. Il signalait, qu'en Angleterre et au pays de Galles, l'amende était maintenant la peine la plus fréquemment utilisée, même pour les actes criminels. En 1980, 53% des personnes condamnées pour un acte criminel avaient eu une amende, alors que le pourcentage des gens condamnés à l'amende était de 45% en 1959 et de 27% en 1938. Par ailleurs, les pourcentages de personnes condamnées à l'emprisonnement avaient décru constamment passant de 33% en 1938 à 29% en 1959 et enfin à 15% en 1980. Au Canada, la tendance est similaire: en 1978, 61% des personnes condamnées par les tribunaux au Québec s'étaient méritées une amende alors que 24% avaient été condamnées à l'emprisonnement. Par ailleurs, il semble(31) qu'au Canada, en 1900, les proportions aient été inversées: environ 55 à 60% des condamnés étaient incarcérés et environ 30% d'entre eux avaient une amende.

Un nombre et un pourcentage de plus en plus élevés de citoyens tombent sous la coupe du droit pénal, mais une proportion relativement constante d'entre eux sont incarcérés. Les autres mesures pénales, que l'on propose souvent comme des solutions de rechange à l'incarcération, sont généralement en fait imposées aux personnes reconnues coupables de nouvelles infractions (comme celles relatives à la circulation routière), à des personnes qui ne subissaient souvent pas de mesures pénales, ou elles viennent s'ajouter à une peine d'incarcération, comme c'est parfois le cas pour l'amende ou la probation.

4- Passage de la moralisation des esprits vers un contrôle des comportements...

A la fin du XVIIIe et au début du XIXe siècle, on l'a déjà mentionné, l'économie de la peine subit un profond changement. De l'intervention sporadique mais exemplaire, on passe graduellement à une peine plus certaine. L'auteur de l'acte devient de plus en plus le centre des préoccupations. La prison du début du XIXe tentait de transformer les esprits et la nouvelle pénologie de la fin de ce siècle, ainsi que les théories des positivistes, viendront accentuer et améliorer ce modèle.

Mais, récemment, des critiques du "modèle thérapeutique", soit d'une part du point de vue de l'équité des peines et de l'efficacité des interventions pour diminuer la récidive, ou d'autre part du point de vue de l'efficacité du modèle par rapport à la prévention générale ou de son manque de sévérité, semblent mener à des changements importants des politiques pénales et des stratégies de luttes contre la criminalité.

Le rejet du "modèle thérapeutique" a favorisé une revalorisation de la punition soit en fonction de la rétribution ou comme moyen de modifier les comportements. Par ailleurs, il y a aussi un retour de la prévention générale et une redécouverte de la neutralisation (incapacitation) générale ou sélective.

Un certain courant criminonogique récent s'intéresse aussi moins à l'homme criminel, du moins à ses motivations, à la dynamique profonde de son comportement, qu'aux situations criminelles, aux opportunités, aux stratégies et aux tactiques des délinquants. L'accent est mis sur la prévention. Mais par prévention, on entend plus l'action des travailleurs de rue ou des clubs de prévention, ou encore les réformes sociales d'envergures, telles la lutte contre la pauvreté ou l'accessibilité à l'éducation et à la formation professionnelle. La "nouvelle" prévention vise non pas à transformer les quartiers, mais à surveiller les quartiers; non pas à augmenter les occasions d'amélioration des plus démunis, mais à diminuer les occasions de délits.(32) L'accent est mis sur la réduction du nombre, de l'accessibilité et de la vulnérabilité des cibles. La technologie et les stratégies de surveillance prennent la vedette.

Quant à l'intervention pénale "l'important n'est pas tant de réhabiliter les délinquants que de minimiser leurs gains, maximiser leurs coûts et, si nécessaire, neutraliser ceux dont l'activité criminelle est trop virulente"(33). Il ne s'agit plus de transformer ceux qui contreviennent aux lois, mais de les punir, les intimider, les surveiller et les neutraliser. S'il reste une place pour l'intervention "thérapeutique", on favorisera celles qui tentent de modeler les comportements, d'obtenir un respect des règles ou qui ont pour effet de faire cesser le comportement violent. D'où la popularité des thérapies behaviorales, et l'intérêt de plus en plus grand pour la chimiothérapie et la neurochirurgie. Par ailleurs, on développe aussi, en Amérique du Nord de nouvelles mesures de surveillance telles la surveillance intensive (I.S.P.) en probation ou en libération conditionnelle(34) et la surveillance électronique.

5- ...par la surveillance électronique

Jusqu'à présent, les analyses de la transformation de l'économie des peines et du contrôle social ont accordé peu d'importance à la surveillance électronique. On la concevait comme un élément marginal,

lointain, qui relevait plus de la science fiction ou de la pensée futuriste, que comme une des composantes importantes du contrôle social de l'an 2000[35].

Compte tenu de la transformation du contrôle pénal et du contrôle social de la fin du XXe siècle, compte tenu des progrès technologiques importants dans le domaine de l'électronique, de la télécommunication et de la biotechnologie ces dernières années, et de l'intérêt fulgurant pour la surveillance électronique depuis le début des années 80, cette dernière n'est-elle pas un moyen de surveillance "idéal" qui cadre parfaitement et qui peut donner un élan au mouvement actuel? Ne sommes-nous pas devant une technologie qui permettra la réalisation du panoptique, qui assurera, à des coûts économiques relativement acceptables, une surveillance et une neutralisation intensive, extensive, sans affecter la capacité de production des surveillés et qui est tout à fait adaptable aux besoins de main-d'oeuvre?

La surveillance électronique, telle quelle est présentement expérimentée, est très intensive. Elle permet une intrusion considérable et continue dans la vie sociale et personnelle de l'individu. Mais la technologie permet d'aller beaucoup plus loin. On pourrait par exemple suivre toutes les allées et venues d'une personne, suivre ses déplacements sur un territoire donné. On pourrait aussi relier l'émetteur à un implant qui permettrait de détecter la présence d'alcool ou d'autres drogues dans le sang, un taux anormalement élevé d'adrénaline, une excitation sexuelle, etc. De tels implants soulèveraient un tollé de protestations au sujet des libertés fondamentales, mais notre société tolère déjà des tests d'urine réguliers et aléatoires sur les personnes incarcérées et sur certains travailleurs, ainsi que des prises de sang, sans le consentement du sujet, pour déterminer s'il conduisait en état d'ivresse. Beaucoup de principes d'éthique ou légaux tombent quand on décrète que le "jeu en vaut la chandelle", quand des entrepreneurs moraux des "spécialistes" de la sécurité et de la protection, des politiciens clament que "la situation est urgente", la "menace est grave", le "danger est terrible". Les libertés individuelles tiennent peu de place en temps de guerre, même dans une guerre contre "l'ennemi de l'intérieur", "les criminels".

D'autre part, elle permet aussi une surveillance individuelle et sociale beaucoup plus extensive. Comme la prison, elle permet une surveillance continuelle de l'individu. Mais elle permet, à plus ou moins courte échéance, de surveiller beaucoup plus d'individus que la prison. La surveillance étatique peut s'étendre, vingt-quatre heures par jour, sur un nombre considérable d'individus.

Si la neutralisation et surtout la surveillance s'adressent à un nombre de plus en plus grand de personnes, il est impératif, si on veut limiter les coûts du contrôle social, que ces personnes demeurent ou deviennent productrices, ou qu'elles le soient lorsqu'on aura besoin d'elles. Comme le soulignait Marlène Lehtinen, "Les méthodes de neutralisation technologique qui peuvent prévenir effectivement la commission d'infractions, ne doivent pas empêcher les activités productrices."(36) Cette technique de surveillance est d'autant plus adéquate économiquement, qu'en plus de ne pas limiter les capacités de production, elle permet aux surveillés d'avoir les moyens d'assumer les coûts de leur propre surveillance, comme cela se fait très souvent, dans les programmes en cours aux Etats-Unis.

La surveillance électronique a aussi connu une vogue de popularité ces quelques dernières années, et on peut lui prédire un "avenir très prometteur", parce qu'elle s'appuie parfaitement et légitimise le discours sur la "bifurcation" en politique pénale, qu'a décelé le criminologue anglais A. Bottoms, il y a déjà une décennie. Bottoms entendait par "bifurcation" dans la détermination des peines, l'augmentation de la sévérité des mesures pénales pour ceux que l'on qualifie de "délinquants violents", de "vrais délinquants" (really serious offender), et le développement de mesures moins draconniennes, appelées souvent solutions de rechange à l'incarcération, pour les "petits délinquants". Même s'il semble que, jusqu'à présent, une seule branche de la "bifurcation", celle concernant l'augmentation de la sévérité des peines, se soit réellement concrétisée, il ne fait pas de doute que le discours est généralement bien reçu et qu'il contribue à la multiplication de mesures pénales, qui ne

sont généralement pas des solutions de rechange à l'incarcération. La surveillance électronique, que l'on propose comme un moyen (peu coûteux et plus humain que la prison) d'assurer une "vraie" surveillance et de protéger réellement le public, a tous les atouts pour entretenir et faire accepter ce discours. C'est probablement la raison qui la rend aussi populaire auprès des politiciens et des administrateurs pénaux.

Si l'analyse est exacte, et si la surveillance électronique s'inscrit bien dans les transformations actuelles du contrôle social, si elle peut donner un essor encore plus important à l'extension de ce contrôle social et à la surveillance pénale, tout en constituant un danger sérieux pour les libertés individuelles, compte tenu surtout des possibilités à moyen terme de la technologie(37), il est certes temps de s'alarmer, de pousser les réflexions à ce sujet et de voir comment on peut en limiter l'expansion et les conséquences.

Peut-être doit-on se demander comme Gary T. Marx: "Doit-on avoir un tel système tout d'abord?" Une fois que ces nouveaux systèmes de surveillance sont institutionnalisés et sont pris pour acquis dans une société démocratique, on peut les utiliser à de mauvaises fins. Sous un gouvernement plus répressif et une opinion publique moins tolérante (peut-être troublée par de sérieuses difficultés économiques, des vagues importantes d'immigration, une grave désorganisation sociale ou des revers en politique extérieure), ces moyens pourraient facilement être utilisés contre les dissidents politiques, les membres de minorités raciales, ethniques ou religieuses et ceux dont le style de vie offense la majorité" (1985, p. 33).(38)

Pierre Landreville
École de criminologie
Université de Montréal

NOTES

1) Marx, G.T. (1985a, b)

2) C.R.D.C. (1976) p. 22

3) Schwitzgebel, R.K., et al (1964); voir aussi: Schwitzgebel, R.K. (1968)(1969a)(1969b)

4) Ford, D., Schmidt, A.K. (1985) et Flynn (1986a, b)

5) Sherman, L.W. (1987)

6) Ces articles ont presque tous été publiés depuis 1985; voir les références. On a même publié récemment aux U.S.A., un livre sur le droit dans ce domaine: Carr, J.G. (1986)

7) Landreville, P. (1986), appendice V

8) Ford, D., Schmidt, A.K. (1985) et Paparozzi, M.A. (1986)

9) Meyer, J.A. (1971). Crime deterrent transponder system. IEEE Trans aeros electron sys., 7, 2-22. Cité par Gable (1986) pp. 168-169.

10) Les soulignés sont de nous.

11) "By increasing the probability of apprehension and conviction to a near certainty, the transponder system can discourage crime without isolating the offender irrevocably from the society. Thus, heavy surveillance and light penalties substitute for light surveillance and heavy penalties". Cité par Gable (1986) p. 169.

12) Ingraham, B.L., Smith, G.W. (1972). Voir aussi la critique de cet article par Shapiro (1972).

13) Ingraham, B.L., Smith, G.W. (1972). "The use, then, of telemetric systems as a method of monitoring man, of obtaining physiological data from his body and nervous system, and of stimulating his brain electrically from a distance, seems in the light of present research entirely feasible and possible as a method of control... Certain physiological data, such as respiration, muscle tension, the presence of adrenalin in the blood stream, combined with knowledge of the subject's location, may be particularly revealing e.g., a parolee with a past record of burglaries is tracked to a downtown shopping district (in fact, is exactly placed in a store known to be locked up for the night) and the physiological data reveals an increased respiration rate, a tension in the musculature and an increased flow of adrenaline. It would be a safe guess, certainly, that he was up to no good. The computer in this case, weighing the probabilities,

would come to a decision and alert the police or parole officer so that they could hasten to the scene; or, if the subject were equipped with an implanted radiotelemeter, it could transmit an electrical signal which could block further action by the subject by causing him to forget or abandon his project..."

14) Ruygrok, G. (1986) pp. 11-12.

15) Voir entre autres Cohen (1985) Ch. 2.

16) Tuthill, J. (1986)

17) Landreville, P., prés.(1986)

18) Ford, D., Schmidt, A.K. (1985)

19) Pires, A. (1986) p. 164.

20) Ford, D., Schmidt, A.K. (1985) et Sherman, L.W. (1986)

21) "In the new democracy, where citizenship and security extended to all classes, discipline could no longes function through repression and exclusion. Henceforth its modalities would have to be more refined and discreet. Yet at the same time they would require to be more systematic and penetrating, more thorough in their effects.

22) Pour reprendre l'expression popularisée par Schull (1977)

23) Cette inflation législative a cependant eu peu d'impact sur la pratique pénale. Les tribunaux et les prisons continuent à "gérer" des contrevenants provenant des mêmes groupes (ou classes) sociaux.

24) Waller (1982) tableaux 40-42

25) Waller (1982) tableau 9

26) Selon l'expression de Black (1976)

27) Waller et Chan (1974)

28) Waller (1982) tableau 26

29) Cahalan (1979)

30) Entre autres: Cohen (1985) et Chan et Ericson (1985)

31) Selon notre évaluation à partir du tableau 35 de Waller (1982) en faisant l'hypothèse qu'environ 50% des entrées en prison en 1900 l'étaient pour défaut de paiement d'amende.

32) Les récentes politiques de prévention reposent plus sur la réduction des "criminal opportunities" (Cook, 1986) que sur Delinquency and oportunity de Cloward et Ohlin, (1964).

33) Cusson, Maurice. La criminologie a-t-elle un avenir? Document dactylographié, mars 1987, p. 8.

34) Voir entre autres: Crime and delinquency (1985), 31, no 3, special issue: community supervision; et Mc Carthy, Belinda R. (ed.) (1987)

35) Cohen (1985) écrit par exemple: "a reading of correctional stories gives an exaggerated notion of how much innovation there has been: novel alternatives such as traking of house arrest involve only a minority of offenders", p. 84

36) "Methods of technological incapacitation while effectively preventing the commission of crime, should not prohibit productive activity", p. 35

37) La surveillance électronique peut se transformer en technique de neutralisation efficace. Un professeur de sociologie l'envisageait favorablement il y a déjà quelques années: "It would be possible to built... measures that could render the monitored subjects immobile or significantly reduce their mobility by either direct electrical stimulation of the brain or through the release of drugs into their bloodstream by an internal telemetry receiver."... "The urgency of the situation demands radicals solution which attack the problem directly." Lehtinen (1978) pp. 35-36.

38) "...Should the system be there to begin with? Once these new surveillance systems are institutionalized and taken for granted in a democratic society they can be used for harmful ends. With a more regressive goverment and a more intolerant public (perhaps upset over severe economic downturns, large waves of immigration, social dislocations, or foreign policy setbacks) these devices could easily be used against racial, ethnic, or religious minorities, and those with life styles that offend the majority." Marx (1985) p. 33.

RÉFÉRENCES

ACKERMANN, J.R. Applying electronic surveillance systems to probation in New York State. Journal of probation and parole, 1986, 17, fall, 5-8.

BALL, R.A., LILLY, J.R. Home incarceration: an international alternative to institutional incarceration. International journal of comparative and applied criminal justice, 1985, 9, 2, 85-97.

BALL, R.A., LILLY, J.R. A theoretical examination of home incarceration. Federal probation, 1986a, L, 1, 17-24.

BALL, R.A., LILLY, J.R. The potential use of home incarceration for drunken drivers. Crime and delinquency, 1986b, 32, 2, 224-247.

BERRY, B. Electronic jails: a new criminal justice concern. Justice quarterly, 1985, 2, 2-22.

BLACK, D.J. The behavior of law. London, Academic Press, 1976.

BOTTOMS, A.E. Reflexions on the renaissance of dangerousness. The howard journal of penology and crime prevention, 1977, XVI, 2, 70-95.

BOTTOMS, A.E. Neglected features of contemporary penal systems, ch. 8 in Garland, D., Young, P. (eds.) The Power to punish. London, Heinemann educational books, 1983.

BRISSETTE, M. L'infraction dans le droit pénal du Québec, v. II. Montréal, Université de Montréal, Centre international de criminologie comparée, 1977.

CAHALAN, M. Trends in incarceration in the United States since 1880. Crime and delinquency, 1979, 25, 1, 9-41.

CARR, J.G. The law of electronic surveillance. New York, Clark Boardman, 1986.

CHAN, Janet B.L., ERICSON, R.V. Decarceration and economy of penal reform, in Fleming, T. (ed) The new criminologies in Canada. pp. 223-241. Toronto, Oxford University Press, 1985.

CLOWARD, R.A., OHLIN, L.E. Delinquency and opportunity. Free Press, 1964.

COHEN, S. Visions of social control. Cambridge, Polity Press, 1985.

COMMISSION DE RÉFORME DU DROIT DU CANADA. Principes directeurs: sentences et mesures non sentencielles dans le processus pénal. Ottawa, Information Canada, 1976.

COOK, P.J. The demand and supply of criminal opportunities, in: Tonry, M., Morris, M.N. (eds) Crime and Justice, 1986, 7, 1-27.

CORBETT, R.P., FERSH, E.A.L. Home as prison: the use of house arrest. Federal probation, 1985, XLIX, 1, 13-17.

FLYNN, L.E. House arrest: Florida's alternative eases crowding and tight budgets. Corrections today, 1986a, July, 64-68.

FLYNN, L.E. House arrest: staff it right or quit. Journal of probation and parole, 1986b, 17, Fall, 1-4.

FORD, D., Schmidt, A.K. Electronically monitored home confinement. National Institute of Justice reports, 1985, November, 2-6.

FOUCAULT, M. Surveiller et punir. Paris, Gallimard, 1975.

FRIEL, C.M., VAUGHN, J.B. A consumer's guide to the electronic monitoring of probationers. Federal probation, 1986, L, 3, 3-14.

GABLE, R.K. Application of personal telemonitoring to current problems in corrections. Journal of criminal justice, 1986, 14, 167-176.

GARLAND, D. Punishment and welfare. England, Gower Pub. Co, 1985.

INGRAHAM, B.L., SMITH, G.W. The use of electronics in the observation and control of human behavior and its possible use in rehabilitation and parole. Issues in criminology, 1972, 7, 2, 35-53.

KORPIVAARA, A. Electronic anklets: the potential for abuse. Journal of probation and parole, 1986, 17, Fall, 14.

LANDREVILLE, P. Prison, système pénal et contrôle social. Le contrôle social en pièces détachées. Actes du Colloque de l'A.C.S.A.L.F., Université Laval, mai 1984, pp. 21-32, 1985.

LANDREVILLE, P. (prés.). Rapport du Comité d'étude sur les solutions de rechange à l'incarcération. Québec, Ministère du Solliciteur général, 1986.

LEHTINEN, M.W. Technological incapacitation a neglected alternative. Quarterly journal of corrections, 1978, 2, 31-38.

MARX, G.T. I'll be watching you. Dissent, 1985a, 32, 1, 26-34.

MARX, G.T. The new surveillance. Technology review, 1985b, 88, 4, 43-48.

McCARTHY, Belinda R. (ed.). Intermediate punishments: intensive supervision, home confinement and electronic surveillance. Monses, N.Y., Willow Press Inc, 1987.

PAPAROZZI, M. Electronic monitoring in parole supervision "passive vs. active systems". Journal of probation and parole, 1986, 17, Fall, 9-10.

PIRES, A. Critiques à la prison et principe de modération: inventaire d'extraits dans les documents canadiens. Document à l'intention de la Commission canadienne sur la détermination de la peine. 1986.

PONSEARS, P., CUPER, R. L'inspection du travail: mission de l'autorité ou affaire privée? Déviance et société, 1981, 4, 347-367.

RUYGROK, G. Une alternative à l'incarcération. Actualités-justice, 1986, 3, 2, 10-12.

SCHWITZGEBEL, R.K. Electronic alternatives to imprisonment. Lex et Scientia, 1968, 5, 99-104.

SCHWITZGEBEL, R.K. Development of an electronic rehabilitation system for parolees. Law and computer technology, 1969a, 2, 9-12.

SCHWITZGEBEL, R.K. Issues in the use of an electronic rehabilitation system with chronic recidivists. Law and society review, 1969b, 3, 597-611.

SCHWITZGEBEL, R.K., SCHWITZGEBEL, R.L., PAHNKE, W.N., HURD, W.S. A program of research in behavioral electronics. Behavioral science, 1964, 9, 233-238.

SCULL, A. Decarceration. Englewood Cliffs, N.J., Prentice-Hall, 1977.

SHAPIRO, M.H. The use of behavior control technologies: a response. Issues in criminology, 1972, 7, 2, 55-93.

SHERMAN, L.W. What's new in prison jewelry. Wall Street Journal, January 16, 1987.

TUTHILL, J. An evaluation of electronic home detention as a deterrent for offenders convicted of driving under the influence of alcohol. Journal of probation and parole, 1986, 17, Fall, 11-13.

WALLER, I. Canadian crime and justice in comparative perspective: selected indicators for selected countries 1900-1980. Ottawa, Département de criminologie, 1982.

WALLER, I., CHAN, Janet. Prison use: a canadian and international comparison. Criminal law quaterly, 1974, 17, 47-71.

A Consumer's Guide to the Electronic Monitoring of Probationers

BY CHARLES M. FRIEL and JOSEPH B. VAUGHN*

Criminal Justice Center, Sam Houston State University

DURING THE 1970's, crime escalated beyond most predictions and seemingly, beyond the ability of anyone to control it. As fear of crime increased, so did the public's demand that something be done. In response, numerous statutes were enacted during this period which reflected the growing demand for crime control. The principal policy objectives of this era seemed to be:

- Increase the probability that those convicted would be incarcerated.
- Increase the duration of their incarceration.
- Reduce the probability of offenders being released before serving the full term of their sentences.

Not surprisingly, these policy changes—coupled with the increasing number of offenders moving through the justice system—resulted in a massive institutional overcrowding problem which has had profound and irrevocable effects on both local jails and state prison systems. The ripple effects of overcrowding precipitated a correctional case law revolution which raised a variety of challenges to the constitutionality of the nation's correctional system. As a result, policy makers have been confronted with a two-headed dragon, neither head of which could be chopped off without increasing the dangerousness of the other. If the public's demand for punishment were to be accommodated, institutions would become more crowded and legal sanctions would ensue. Conversely, building more institutions, a fiscally objectionable alternative, or reducing prison populations by greater use of parole, would likely fly in the face of public sentiment. Neither alternative was attractive, since few policy makers wanted to ask the public to choose between their pocketbook and their demands for safety.

Prompted by legal pressure, alternatives to incarceration, including increased use of probation, were explored. By the end of 1982, for example, 61 percent of all adults under correctional supervision were on probation, with an additional 11 percent on parole, resulting in 7 out of 10 convicted offenders being supervised in the community (Bureau of Justice Statistics 1983).

* Dr. Friel is a professor and Mr. Vaughn is a doctoral fellow at the Criminal Justice Center, Sam Houston State University, Huntsville, Texas.

The demands placed on probation over the past few years have been extraordinary. Not only is the nation's probation system expected to handle an increased number of offenders with relatively fewer resources, but also to supervise a more diversified group of offenders in terms of both risk and need. To accommodate this sudden shift in clientele, administrators have found it imperative to look for new supervisory strategies capable of both meeting the needs of offenders and the demands of the public. This has resulted in the emergence of a variety of new approaches to probation, including intensive supervision probation (ISP), an increasing dependency on contractual services, the promulgation of specialized caseload strategies for use with drug and alcohol dependent offenders and sex offenders, and—most recently—the use of electronic monitoring devices (EMD).

The purpose of this article is to explore some of the administrative and policy implications of the electronic monitoring of probationers. One can find scattered references to the potential use of telemetry in the supervision of offenders in both the futurist and criminal justice literature as far back as the late 1960's and early 1970's (Ingraham and Smith 1974). However, it was not until the prison overcrowding problem created an unprecedented demand for diversion that market conditions were attractive enough to encourage the private sector to make the technology commercially available. Over the past 2 years, several companies have been marketing different versions of EMD which have broad potential applications in corrections. Because the technology is new, there is not yet a body of empirical knowledge assessing its utility and cost-benefit (Berry 1985). Therefore, this article can only speculate on potential applications, abuses, and administrative and policy implications, since time must pass before empirical evaluations can be conducted.

In the absence of such evaluative studies, the method employed in this study involved a series of telephone interviews with probation administrators, users of the technology, and manufacturers. The intent was not to interview a random cross section of the field, but to confer with informed invidivuals on the possible issues raised by the use of the technology. The interviews centered around the following questions:

- What is electronic monitoring technology and how does it work?
- What is the cost-benefit of the technology?
- What functional characteristics of the technology are important to probation?
- What kinds of offenders might be good candidates for the technology?
- Does the technology necessitate any special administrative considerations?
- What are the potential abuses of the technology?
- What philosophic issues does the technology raise for probation administrators?

What is Electronic Monitoring and How Does It Work?

Interviews with probation administrators suggested that the term "electronic monitoring" is a bit ambiguous, since three different meanings attach to the term.

- The use of a conventional telephone to call the probationer during curfew hours to determine whether she or he is at home.
- A computer which automatically dials the probationer's telephone and receives voice and/or electronic identification.
- Systems wherein the probationer wears a transmitting device which sends a radio signal to a receiver attached to the probationer's phone which can communicate with a computer.

Although some of the observations presented in this article can be applied to all three forms of electronic monitoring, most are concerned with the latter two.

The basic idea behind electronic monitoring is twofold: divert offenders from incarceration and confine them in their place of residence during specified curfew hours. Typically, offenders in such a program are required to be in their residence during the evening hours and on weekends. Depending upon the particular system employed, some form of telephone communication is used to verify that the offender is at home during specified hours. For example, some intensive supervision programs simply use conventional telephone communications to achieve this objective. More recently, however, several companies have introduced automated telecommunications systems which can achieve the same objective, thereby eliminating the actual involvement of probation officers in making calls.

One form of the technology which is offered by several companies requires the probationer to wear a small transmitter.[1] The transmitter emits a radio signal which is picked up by a receiver attached to the probationer's telephone. During curfew hours, the receiver automatically dials the monitoring computer to advise whether it is receiving a signal from the transmitter. If so, the computer assumes that the probationer is at home. If not, the computer registers a potential curfew violation and notifies the person monitoring the system.

Another version of the technology uses a wrist band instead of a transmitter.[2] In this case, a computer dials the probationer's home during curfew hours, the probationer is asked to identify himself, insert an identification bracelet worn on the wrist into a receiver attached to the phone, and the receiver sends a signal back to the computer. If the telephone is not answered, or the bracelet is not inserted into the receiver, the computer notes a potential violation.

It is not the intention of this article to evaluate the hardware systems offered by different manufacturers. Instead, the purpose is to explore the administrative and policy issues raised by the use of such technology. The National Institute of Justice is currently conducting benchmark tests of the equipment offered by several companies, and the results should be available in the near future.[3]

Companies currently offering electronic monitoring systems include Advanced Signal Concepts, Contrac, Control Data Corporation, Computrac, Correctional Services, Inc., Cost Effective Monitoring Systems, Life Sciences Research Group, Inc., Controlec Inc., Digital Services Inc., and Voxtron. As of this writing, there are several agencies either using the technology or conducting feasibility studies. These include correctional agencies and private service corporations in Florida, Idaho, Kentucky, Michigan, New Jersey, Oklahoma, Oregon, Pennsylvania, Texas, and Utah.

Cost-Benefit of Electronic Monitoring

It is premature to attempt to determine the actual cost-benefit of the technology. It has been only recently introduced to the field and only time will tell whether the benefits derived outweigh the costs. In addition, the question of cost-benefit is complex, not simple. The assessment of costs and benefits varies depending upon one's point of view—for instance, the sheriff with an overcrowded jail versus the probation department which may have to pay for the technology. In addition to the direct cost of purchasing equipment, there are the indirect costs of operating the system. One should also consider the lost opportunity costs and benefits. What other programs could have been initiated or expanded with the funds used to purchase the monitoring equipment? Finally, there are

[1]Such systems are offered by Advanced Signal Concepts, Contrac, Control Data Corporation, Computrac, Corrections Services, Inc., and Controlec, Inc.

[2]Digital Products, Inc. offers such a system.

[3]The tests are being conducted by the Law Enforcement Standards Laboratory, National Bureau of Standards. The results will be made available by the National Institute of Justice.

nonmonetary costs and benefits to be considered.

Probably the primary selling point of the technology is the potential cost savings involved in the operation of institutions and new construction. The institutional overcrowding problem has made policy makers keenly aware of the extraordinary costs associated with incarceration. Operating costs vary, but recent studies suggest that they may well range between $15 and $50 per day. Similarly, the cost of new construction varies from $25,000 to $75,000 or more per bed depending upon the level of architectural security desired (Funke 1985).

From this perspective, there is no question that the direct cost of electronically monitoring offenders in the community is cheaper than incarceration. Although costs vary among vendors and also as a function of the number of units purchased, the current direct cost of a system might range up to $15 a day or more for each probationer. This represents an attractive cost tradeoff for policy makers who can see savings not only in institutional operating costs but also in the reduced need for future capital construction.

From the legislator's point of view, the technology represents a tempting cost savings if the public's demand for punishment and public safety can be set aside for the moment. However, from the probation administrators' point of view, the technology may not be cost beneficial. Relatively speaking, public expenditures for the administration of justice are a zero sum game. Funds expended for one purpose are no longer available for another. When a probation department considers the use of electronic monitoring, it should carefully consider the lost opportunity costs in terms of the benefits that might be derived from other programs. If a department is successful in securing funds to buy a monitoring system, will this frustrate efforts to secure needed funds to expand other programs or initiate new ones? Careful consideration should be given to how the technology will be used in the overall supervisory strategy of the department. Probation administrators need to properly assess the priority to be attached to electronic monitoring relative to other departmental needs. If the need for additional officers or higher salaries is more important, then care should be exercised to ensure that purchase of the technology will not inadvertently frustrate these ends.

Most of the administrators surveyed agreed that the technology should only be used to divert offenders who would be otherwise incarcerated. If the technology is simply used with individuals who would be granted probation anyway, there is no cost savings relative to institutional costs. Unless it is demonstrated that the use of the technology with typical probationers reduces recidivism more than conventional supervisory strategies, there would be no savings from a public safety perspective. Along this same line, it is likely that if the technology is only used to enhance surveillance of people who should be granted probation in the first instance, the result may be just a widening of the correctional net, increasing costs with no noticeable benefit.

An empirical question yet to be answered is whether the technology has a greater effect on recidivism than do conventional modes of supervision. If the technology is only used to divert offenders who would otherwise be incarcerated, one might reasonably expect under the best of circumstances a higher recidivism rate than is typical with those who would normally be granted probation. However, the potential cost savings from the technology declines rapidly as the recidivism rate of this higher risk group increases. If recidivism is high, then the costs associated with incarceration have simply been forestalled, not eliminated. In fact, one could argue, depending upon the rate of recidivism and the effects of inflation on the future costs of incarceration, that the use of the technology to divert and forestall incarceration will result in higher net future costs than would the initial incarceration of these offenders.

There are a variety of potential monetary benefits which could flow from the use of the technology. Obviously money saved by diverting offenders can be used in other ways. However, the nonmonetary benefits that might flow from the technology are equally attractive. One cannot deny the humanistic benefits which might be achieved. The decisionmaking criteria used in the administration of justice are generally conservative for understandable reasons. When the risks associated with diversion seem high, the system is more likely to incarcerate the individual than provide supervision in the community. In such instances, the secondary effects of incarceration are neither few nor trivial. Pretrial detainees, for instance, who are unable to make bond or be released on their own recognizance, may lose their jobs, apartments, default on their car payments, and not be in a position to support their families. In this case, policy makers must weigh the secondary effects of incarceration against the magnitude of the risk to public safety and failure to appear rate. Although the actual calculation of such tradeoffs is complex, the cost-benefit issue is simple: It is neither humanistically nor economically beneficial to hold people in prison or jail who do not need to be there (Nagel, Wice, and Neef 1977).

There may be a public image benefit to be derived from the use of the technology. Many citizens believe that being granted probation is simply "getting off," merely a slap on the wrist. For the most part this attitude emanates from the public's misconception of the role played by probation in the criminal justice system. Nevertheless, the attitude may be pervasive in a particular community, and the use of electronic monitoring may help to enhance the

public safety image of the department. Such a benefit is worth considering, since community acceptance of the legitimacy of probation is likely to increase its efficacy.

Advocates of electronic monitoring argue that the technology has the potential to reduce jail and prison populations. If successful, depending upon local conditions, this could have one of three effects. First, it could reduce the rate of capital expansion in the future. Secondly, it could obviate the need for new construction. Thirdly, it could actually reduce the population in existing facilities. Critics of the technology express skepticism about the third alleged benefit. They suggest that even if offenders were diverted from existing institutions, thereby making bed space available, the beds would be filled anyway. The result would not be a reduction in operating costs; on the contrary, it would simply increase overall public expenditures by the cost associated with the purchase of the technology. This school of thought reflects the belief that incarceration rates are determined by available bed space. The debate over the causal relationship between available bed space and institutional populations is a complex one which cannot be addressed here. Suffice it to say, however, that it is an issue which ought to be considered by policy makers in evaluating the costs-benefit tradeoffs associated with the use of electronic monitoring (Conrad and Rector 1977).

Regardless of who benefits from the technology, someone will have to pay for it, likely the taxpayer. Some suggest, however, that the probationer defray the cost, since she or he is a principal beneficiary of diversion. Initially this may seem to be an attractive alternative, but it raises a variety of concerns. Will such a policy discriminate against the indigent offender and raise equal protection issues? What portion of the cost can probationers be reasonably expected to pay? Is the option even realistic considering that probationers in many jurisdictions are already paying court costs, fines, restitution, and/or probation fees?

A final thought on cost-benefit concerns the research and development costs associated with the technology. If the proposed benefits are to be realized by the correctional community and the public, then the cost of the technology must be reasonable, the equipment reliable, operation efficient, training requirements minimal, and noticeable enhancements in public safety achieved. Currently, there are several companies offering electronic monitoring technology. In selecting among systems, the cautious consumer should keep in mind the adage "caveat emptor." Certainly the probation department does not want to become a guinea pig, paying for the research and development of an untested system. Prudent public policy requires that the private sector absorb the research and development costs prior to offering the technology to the correctional community. This suggests that the probation administrator should look not only at the comparative cost among the different systems currently in the marketplace, but also assess the extent and quality of the research and development which stands behind these products. Purchase of an unreliable system requiring a high degree of maintenance may prove to be an irrevocable mistake resulting in professional embarrassment and loss of public confidence.

Functional Considerations

In addition to cost, there are a number of functional considerations that the potential consumer should consider.

Several companies offer systems which require the probationer to wear a transmitter. Such devices can be worn around the neck, the waist, the wrist, or the ankle. Where the transmitter is worn may not only affect the reliability of transmission, but it may also raise cosmetic and safety concerns as well.

Transmitters worn on the ankle may not create a cosmetic problem for a man who wears trousers, but it could be a source of embarrassment for a woman who is accustomed to wearing a dress. One might counter that if the woman wants to get on the program, then she can wear pants. However, this doesn't seem to be a sufficient argument. The purpose of the technology is to divert offenders without jeopardizing public safety, not to brand the probationer with an electronic scarlet letter.

Devices worn around the neck or wrist may create problems for probationers involved in specific kinds of work or recreational activities. For instance, probationers working with certain machinery may be required to remove articles from their fingers, wrists, and from around their necks for safety reasons. Such restrictions may emanate from company policy, occupational safety laws, or the requirements of insurance underwriters. Although not a major problem, it may be an issue with some offenders admitted to the program.

If the probationer takes the transmitter off and leaves it next to the telephone while going out for a night on the town, the system is clearly jeopardized. Therefore, in comparing different systems, the consumer may want tamper-proof devices. Specifically, such a system is designed to sense whether the transmitter has been removed or tampered with. While a tamper-proof transmitter is a security benefit, it may also increase cost in two ways. First, the direct cost of such a device may be more than one which is not tamper-proof. Secondly, in making the device tamper-proof, it may not be reusable, depending upon the design of the particular manufacturer. If removal of the device makes it inoperant, then it may not be reusable when the probationer completes his term of surveillance. This may be an im-

portant cost consideration, depending upon how the department proposes to use the technology. If the department only intends to put probationers on the system for a short period of time (e.g., 30 or 60 days), then reusability becomes an important cost consideration. On the other hand, if probationers will be under surveillance for long periods of time, then reusability may not be as important; however, the number of units that will have to be purchased will be larger, driving up cost.

Some consideration should be given to the source of electricity used to energize the system. Typically the transmitter is powered by batteries, while the receiver and the computer use a conventional electrical outlet. Because of the dependency on electricity, power surges may jeopardize the system. A power outage may cause the computer to crash, temporarily eliminating its capacity to monitor probationers. Similarly, a power failure in the probationer's home or neighborhood will shut off the receiver, again jeopardizing the system. Several companies offer a receiver with a battery backup which permits continuing monitoring during a power failure. This is a desirable feature, particularly in areas subject to frequent power failures.

The transmitter worn by the probationer is powered by batteries which have a limited life. If the batteries fail, no signal will be sent to the receiver, and the computer will register a curfew violation. Therefore, consumers should look for some feedback mechanism in the system which can indicate that the batteries are beginning to run down. This will decrease the cost and administrative complications that result from false alarms.

The systems available today use telephone lines to provide the communications link between the receiver and the monitoring computer. The quality of local telephone service and any factors which affect land-line communications will effect the system's reliability. As one user put it, "If your telephone lines are mush, the system's not for you." The wise consumer should confer with the local telephone company to determine the quality of line service, particularly in areas in which probationers are likely to reside. If the manufacturer's minimum requirements and the quality of local telephone service are a poor match, the technology may be a bad investment.

Line seizure capability is another feature to consider in purchasing a system. What happens, for instance, if the probationer is on the telephone at the time the receiver attempts to dial the computer? Systems that cannot directly access the computer while the phone is off the hook can be easily compromised. Security can be circumvented if the probationer simply takes the phone off the hook and goes out for the evening or if the probationer or one of the family inadvertently leave the phone off the hook.

Existing systems have not been on the market long enough to assess their durability. The monitoring computer and the receiver are probably less liable to wear and tear than the transmitter worn by the probationer. It may be, for instance, that transmitters worn on one part of the body may be more subject to wear than those worn elsewhere. Depending upon the nature of the work and/or recreational activity engaged in by the probationer, devices worn around the neck or wrist may be subject to much more wear than those worn around the ankle.

Early experience indicates that large metal objects, such as a furnace or home freezer, which come between the transmitter and receiver, may interrupt the transmission, thereby creating a false alarm. This could be a persistent problem for probationers living in mobile homes, which for the most part are constructed out of metal. In this case, the probationer's residential mobility could be severely curtailed. Along the same line, at least one user suspects that false alarms may occur when the probationer curls up when sleeping and the body is positioned between the transmitter and the receiver. This, of course, is difficult to confirm, but it does suggest that the wise consumer ought to examine the developmental tests conducted by the manufacturer to determine whether physical objects falling between the transmitter and the receiver interrupt the signal and jeopardize the system. Such information is important in training the probationer in the proper use of the system.

Finally, one should realize that the probationer must have a home and a phone to qualify for the program. While this seems obvious, the requirement may play havoc with the potential cost-benefits to be realized from the technology. For instance, one obvious use of electronic monitoring is to divert pretrial detainees from a crowded jail. However, if the reason they can't make bond or qualify for recognizance release is due to their indigency or lack of a permanent residence, they may not be able to qualify for electronic monitoring either. Similarly, some offenders who would otherwise be prison bound but who are good candidates for ISP and electronic monitoring may not qualify, since their indigency prevents them from finding an appropriate residence and or paying for telephone installation and service. While it's easy to dismiss this problem with the *quid pro quo,* "no home, no phone, no program," the circumstance of indigency may work against the cost-benefits to be achieved with the technology. This raises the question of whether the department should absorb the cost of telephone installation and service in deserving cases or whether this should be passed on to the probationer. Obviously, there is a point of diminishing returns in how much the probationer can contribute to the operation of the system and how far the department can go in under-

writing the indigency of the probationer.

Good Candidates for the Technology

There is a wide variety of correctional clients that might be good candidates for the technology. Before discussing the use of the technology with different offender groups, however, it seems appropriate to raise the issue of the purpose of the technology. Among the probation administrators surveyed, most agreed that its primary purpose should be to divert individuals who would be otherwise incarcerated, since the use of electronic surveillance with individuals who would normally be probated raises several issues. First, it defeats the primary cost-benefit of the technology. Secondly, there is no evidence to date that electronic surveillance of conventional probationers is any better than conventional approaches to supervision. Thirdly, the idea of indiscriminately "wiring up" offenders put on probation would probably only widen the surveillance net without noticeable benefit.

In addition to diversion, however, there are other reasons to employ the technology. If a department currently requires officers to telephone probationers under ISP to determine whether they are complying with their curfew, the technology has the benefit of freeing these officers to do other things. The technology can also serve as an additional increment in the continuum of correctional alternatives from simple probation to incarceration.

Thus, the ends to be served by the technology are broader than just diversion. It can be used to several good ends, and the wise consumer should look for a balancing of purposes.

Pretrial Diversion

Typically, most of a community's jail population is composed of pretrial detainees. As the jail population reaches capacity, policy makers are faced with the choice of either constructing additional space, or diverting some of the population, particularly pretrial detainees. If diversion is the policy of choice, then the first question concerns why these individuals did not make bond.

Typically, a plurality are indigent and simply cannot afford to make bond. However, some will be found who can afford the bond but would rather use their limited resources to retain an attorney. Others believe, and maybe correctly, that if they use their limited resources to make bond, the court will deny their request for a court-appointed lawyer on their claim of indigency.

The alternative in such cases is release on recognizance. Communities vary substantially in the stringency in their recognizance release criteria. Some communities have liberal policies and divert substantial numbers of pretrial detainees. Others have more conservative policies, while still others will only release individuals under conventional security bonds.

Electronic monitoring is not a panacea for the pretrial jail crowding problem. The use of the technology in communities which do not have a recognizance release program is probably a waste of money. Their approach to pretrial release is probably unnecessarily conservative in the first place, and the establishment of a recognizance release program would be a more cost beneficial solution.

By similar reasoning, communities with overly strict recognizance release criteria may not realize much benefit from the use of electronic monitoring. Such communities would be better advised to determine whether their criteria are overly cautious. It might be wise to first lower release standards and determine whether there is any appreciable effect on either public safety or the failure to appear rate. Lowering the recognizance criteria to the point that a noticeable difference appears on one or both criteria provides an empirical indication of the point at which electronic monitoring might be a cost beneficial alternative. The point is that electronic monitoring should not be used if conventional diversionary tactics which are less expensive work equally well.

Weekend Sentences

Weekend sentencing is a correctional alternative which combines the elements of punishment and deterrence with the economic benefit of leaving an individual in the community to work.

While this appears meritorious, weekend sentencing creates a variety of problems for the jail administrator. Typically, weekends are the busiest of times in the jail. The added responsibility of booking and releasing weekend prisoners simply increases the burden. Because of the added responsibility and the perception that weekend offenders do not represent a major threat to public safety, the jail administrator may subvert the process by booking such individuals at 11:59 p.m. on Saturday night and releasing them at 12:01 a.m. Sunday morning. This defeats the purpose of the sentence and decreases respect for the law. Another problem is that the weekend prisoner can be easily extorted and victimized by the jail's permanent residents. Inmates can force the weekend prisoner to do favors for them during the week or face retribution when they return the next weekend.

Electronic monitoring may be a cost-beneficial and productive alternative to weekend sentencing, particularly for persons convicted of drunk driving. It has at least three advantages. First, it may be cheaper. Secondly, it relieves the jail of additional administrative duties during its busiest time. Finally, it eliminates a source of potential extortion, which while undesirable is difficult to control.

Work Release

One of the earliest applications of electronic monitoring was as a complement to a county jail work release program.[4] It appears to be a very attractive application, since it is cost beneficial in two ways: prisoners can live in their homes vis-a-vis the jail and, by working, they can contribute to their own support and that of their families.

Under this application, prisoners would work for several weeks under a conventional work release program. They would leave the jail each morning and return to the institution at night. After a period of adaptation, they would be released from the institution under an electronic monitoring program and expected to work during the day and be in their homes during specified curfew hours. If the system reported a curfew violation, the offender would be returned to the institution and lose the privilege of participating in the program.

Intensive Supervision

Because of prison overcrowding, a number of states have instituted ISP programs to divert individuals who would otherwise be sentenced to prison. Typically, ISP caseloads are small, and the probation officer is expected to make weekly, or in some cases daily, contacts with the offender. For the most part, ISP probationers represent high risk cases and must be watched carefully if the department is to ensure public safety.

The technology could be very useful in an ISP program. If a department decides to use the technology with everyone put under ISP, then such action would free the probation officer from the time required to either physically or telephonically confirm that the probationer is complying with curfew restrictions. If using the technology with all ISP cases proved to be either unnecessary or cost prohibitive, then the department could use it selectively as an increment in the degree of control exercised in the program. For example, if an ISP probationer was found in violation of one or more of the conditions of probation, the technology could be imposed in lieu of revocation. Since the probationer has much to lose from revocation, the impact of the technology could be significant.

Juveniles

It has been suggested that the technology could be used with juveniles. Several of the administrators surveyed found this application abhorrent, suggesting that enough has been done already to criminalize the juvenile justice system. Others, however, suggested that the juvenile justice system does not respond strong enough or early enough to the deviancy of youngsters. One administrator speculated that short periods of electronic curfew imposed early enough in the career of a delinquent might be very beneficial, since such action would indicate that the system is prepared to respond immediately to deviant behavior. Common sense dictates, however, that if a community is already concerned over the criminalization of the juvenile justice process, it might be best to first use the technology with adults in the least risky category. As success is achieved, the technology could be extended to more serious adult offenders and if still successful, then experiments might be tried with juveniles.

Other Applications

Enough has been said to this point to suggest the wide range of potential applications of the technology. The use of the technology in conjunction with shock probation may permit judges to sentence more serious offenders to this alternative. It could also be used by prison and jail administrators in conjunction with educational or home furlough programs. An interesting, but as yet unexplored, possibility is the use of the technology for medical purposes. It is not uncommon, for instance, to find women in jail or prison who are pregnant. In such cases, the institution must make special arrangements to assure the physical well-being of both mother and child. Depending upon the level of risk involved, the woman could be released to her home or the home of a relative during the course of the pregnancy. This would not only be cost-beneficial, but would likely provide a more conducive atmosphere to foster the health and welfare of both mother and child. Other medical applications include diversion of persons with AIDS or other communicable diseases, those requiring long-term post-operative recovery, mentally ill or retarded offenders, generiatric offenders, or offenders with physical handicaps.

The above considerations suggest several conclusions. First, the technology has broad potential application in corrections. Secondly, it should be used primarily for diversion, since other applications may have the effect of widening the correctional net and offsetting the cost-benefit of the technology. Finally, the technology should only be used in lieu of alternatives which are either less effective in assuring public safety or more costly.

Administrative Considerations

Regardless of the perceived cost-benefits, the introduction of the technology may require administrative changes affecting personnel policy, revocation procedures, and relations with the external environment.

Twenty-Four Hour a Day Service

By its very nature, electronic monitoring is a 24-hour

[4] Palm Beach County Sheriff's Department.

a day service. The system has to be monitored, particularly during the evening hours and on weekends. Violations must be reported and responded to.

Prior to implementing a system, the department must carefully specify the procedures to be followed in the event that a curfew violation is reported. Several alternatives are possible. The monitor can simply call the probationer on the phone to determine whether a report is false. Alternatively, the monitor can record the alleged violation and forward the report to the probation officer, who would confront the probationer the next day. A third alternative is for the monitor to call the probation officer or a surveillance officer who would then proceed to the probationer's residence to determine whether the report is false. Obviously this is more costly and raises the prospect of potential personnel problems.

Unlike law enforcement agencies, probation departments vary in their perception of whether they are a 24-hour a day service or an 8 to 5 service. If the technology is to be effective, the department needs to respond rapidly to reported curfew violations. If conventional wisdom is to be believed, the benefit of the technology will be best realized if the department responds immediately to reported violations. Since these violations will occur most commonly during the evening hours and on weekends, a timely response necessitates that the department perceive itself as a 24-hour a day, 7-day a week service.

Departments which foster the perception that officers are on call 24 hours a day are not likely to encounter personnel problems in implementing response procedures. However, if the probation officers rigorously cling to an 8 to 5 mentality, personnel policies and employee attitudes will have to be modified, or the benefits of the technology will be lost. Morale problems may develop in such agencies if departmental policy requires that evening hour and weekend curfew violations be followed up immediately. Union contracts may either prohibit this or contain provisions that overtime compensation must be paid if the officer is contacted after five o'clock. Such provisions may defeat the cost-benefit of the technology.

Surveillance Officers vs. Probation Officers

Good probation officers may argue that they are too highly paid and skilled to be spending their evening hours and weekends checking curfew violations reported by a computer. They may be right, but it also can be argued that the technology provides an opportunity to free the officer to do that which she or he does best. The department could hire surveillance officers to actually follow up the curfew violations. Surveillance officers need not be as highly paid or trained as a probation officer, since their sole function would be to follow up reported violations.

Depending upon the number of probationers monitored, one surveillance officer could be assigned to each caseload or possibly to two or three caseloads. The actual number needed would depend upon the number of offenders on the system and the number of violations reported. Although it may appear at the time of implementation that the number of surveillance officers required is an open-ended question, it really is not. Obviously, if a large number of violations are reported, then a larger number of surveillance officers would be required. However, if reported violations are high, the wrong offenders are being put on the program in the first place. If screening procedures are effective, the number of reported violations should be low, in which case few surveillance officers will be needed. If the number of violations goes beyond a certain number, then the question is not how many surveillance officers to hire, but what is wrong with the screening procedures used to select offenders.

Action on False Alarms

Four kinds of events can occur under an electronic monitoring system:

- The system reports that the offender is home when she or he is.
- The system reports that the offender is not home when she or he is not.
- The system reports that the offender is home when she or he is not.
- The system reports that the offender is not home when he or he is.

The system is functioning reliably when the first two conditions exist. Under the first condition, no action is required. Under the second condition, a probation or surveillance officer is dispatched to confirm the violation and take appropriate action.

Under the third condition, nothing happens. The system "thinks" that the probationer is home when she or he is not. Although the technology is designed to avoid this type of error, it may occur. The frequency of occurrence is difficult to determine, since the department would not be aware of a violation unless the probationer were arrested during the period of the curfew. In all likelihood this type of error is rare.

It is the last condition which can be most vexing for the department. The system reports a violation, but—upon checking—none has occurred. This can be caused by power surges and electrical outages, telecommunication problems, metal objects being imposed between the transmitter and receiver, and so on.

Some users have experienced serious difficulty with this

problem during the early stages of implementation. The errors are frustrating, because they consume manpower needlessly and create doubt in the minds of both probation officers and probationers as to the reliability of the system. If the system cries wolf too often, officers are not likely to follow up on reported violations, and the integrity of the system will be eroded. Problems of this sort are best avoided by studious comparative shopping among the various systems being offered. The consumer is wise to check with other users of a particular system to determine their experience with false alarms.

Procedures and Training

To some extent, procedures and training may vary depending upon the particular system purchased. However, notwithstanding which system is purchased, procedures need to be developed and training instituted in a variety of areas.

It is recommended that the consumer design operating procedures and training programs prior to implementing the system. It would be counterproductive to purchase a system, place probationers under surveillance, and then, only as they gain experience, figure out what procedures and training would have been appropriate.

One of the first procedures to be considered is the screening criteria to be used in determining appropriate candidates. Different procedures may have to be established, depending upon whether the potential candidates will be pretrial or post-trial, juveniles or adults.

The probationer will require some training in the operation and maintenance of the equipment. A short orientation program should be instituted which explains the purpose of the technology, how it works, care and maintenance of the equipment, what to do if the equipment fails, and the department's policy in the event of a curfew violation.

Monitors will have to be hired and trained to operate the equipment. Procedures to be considered include how to enter, update, modify, and expunge information in the computer and what to do in the case of reported violations. An important training consideration is what to do if the system crashes, as in the case of a power outage or mechanical failure. Depending on the manufacturer, the monitor may have to be trained in backing up and recovering the information contained in the system in order to protect the data against a system failure.

An important consideration is system security. It is a general principle of computer security to administratively separate computer operators from those authorized to make changes in the system. It is recommended that one individual, possibly the supervisor of the electronic monitoring program, be empowered to authorize changes but be prevented from having physical access to the hardware. All changes would be made by the computer operator, and the system should produce a daily log of all changes and modifications. It would be the supervisor's responsibility to verify whether the changes made corresponded with those which were authorized. This check and balance should protect the system from inadvertent as well as unauthorized changes.

Finally, the department will need to develop procedures for probation and surveillance officers on what to do in the case of reported violations. Certainly discretion must be exercised in the case of a false alarm, since the reported violation could be a function of system error rather than a curfew violation. As with conventional probation, a curfew violation should not necessarily result in a revocation.

External Relations

Electronic monitoring does not operate in isolation from the rest of the criminal justice community. If the technology is used as a form of diversion, then the courts and the prosecutor must be involved in establishing policy. For instance, if it is used as a compliment to recognizance release, then the various judges in the community should be of one mind with respect to the criteria used for this application. If the technology is used to divert offenders from the state prison, then both judges and prosecutors must be involved in the development of appropriate screening procedures. It would be regrettable, for example, if the technology simply became a bargaining chip in plea negotiation, with the net result that the wrong people were diverted. Before purchasing the technology, the prospective probation department should conduct a thorough feasibility study involving not only people within the department, but also representatives from the various external agencies which will be affected by the technology. Without prior planning and establishing mutually agreed upon procedures for its use, the benefits to be gained by the technology may well be lost.

Duration of Surveillance

Too much of a good thing can be bad. Sentencing an offender to 1 or 2 months of electronic monitoring is probably not excessive. Five to 8 years clearly goes beyond the point of diminishing returns. Unfortunately, the technology is too new to determine the optimal duration of its use.

A typical application would require the probationer to be home during weekday evenings and on weekends. Common sense would suggest that there is an upward limit to how long a person can be housebound before they begin to suffer "cabin fever," or before the condition proves detrimental to family members. In searching for an optimal duration, several principles might be kept in mind. First, an offender who is so recalcitrant or

dangerous to the community that she or he needs to be kept under residential surveillance for an extended period of time probably should not be kept in the community in the first place. Secondly, if one of the justifications for community supervision is the rehabilitation and reintegration of the offender into the community, then long-term residential surveillance which separates the offender from the community is antithetical. The third guideline might be cost. Although the technology is cheaper than institutionalization, it is expensive relative to other forms of supervision. Therefore, it is more cost-beneficial to use a fixed resource for shorter periods of time with more individuals than for longer periods of time with fewer individuals. Lacking empirical evidence in this regard, users will have to develop a duration policy incrementally.

Privatization of Surveillance

Should a department interested in electronic monitoring consider entering into a contract for the monitoring service?

It is quite conceivable, for example, for private investors to purchase electronic monitoring systems and offer monitoring services on a contractual basis. This could be a cost-beneficial arrangement, since the department would not have to make a capital investment in the equipment, be concerned with maintenance, or be involved in the hiring, training, or supervision of the monitors.

While the care to be exercised in this situation would be no different than that in contracting for other services, there is one caveat to be offered in this particular situation. The probation department should determine whether the contractor has a proprietary interest in the particular monitoring system being used. It would probably be better if the contractor had no financial interest in the hardware. In the event the hardware is unreliable, for instance, the contractor would be more likely to change systems. However, a contractor with a proprietary interest in the hardware may well be willing to live with an undependable system as long as the probation department is willing to pay for the service. This would be unwise, particularly if the unreliability of the system reduced its integrity in the eyes of both probation officers and probationers.

Media Involvement

It was mentioned previously that the use of electronic monitoring might have the benefit of enhancing the crime control profile of the probation department. By the same token, public awareness of the use of the technology may arouse concerns about an Orwellian invasion of privacy. Public reaction will probably vary from one community to another, and departments should consider what impact this reaction will have. In one community it may be wise to seek media exposure for the program, since such publicity may foster better community relations and a better public sense of safety. On the other hand, the department may want to keep a low profile, lest offenders be stigmatized by wearing an electronic device. Judges, prosecutors, and other members of the criminal justice community should be consulted during the planning phase on how best to handle media relations when the technology is implemented.

Feasibility Study

From what has been said, the importance of conducting a feasibility study before purchasing the technology should be obvious. Whether electronic monitoring will prove to be a cost beneficial investment will depend upon community need, the degree to which diversion is necessary, current sentencing practices, the extent to which the department, the judiciary, prosecutors, and other representatives of the criminal justice community can agree upon standards and procedures, and so forth. The complexity of the technology, along with the administrative and policy issues it raises, underscore the importance of planning. Failure to plan can result in several negative consequences: the consumer may make a less informed decision in selecting among the various systems currently available, implementation of the program will be slower, selection of appropriate candidates for the program will be less systematic, there will likely be greater disparity in the discretion exercised by officers in dealing with false alarms and violations of the conditions of probation, and, finally, the probability of arousing the public's ire may be increased by misapplication of the technology.

Potential Abuses of the Technology

Electronic monitoring technology can be a useful tool in the repertoire of probation's supervisory strategies. By the same token, it can be abused.

As mentioned before, the primary use of the technology should be the diversion of individuals who would be otherwise sentenced to prison or jail. Even allowing for the conservative nature of decisionmaking in criminal justice, many of those currently incarcerated need the added surveillance that an institution allows. Thus, the diversion of these individuals will require more extensive surveillance in the community. Other things being equal, the use of electronic monitoring in this circumstance seems appropriate. Using the technology with individuals who would be granted probation anyway is potentially abusive. It has already been pointed out that this application is likely to raise costs without necessarily increasing benefits. In addition, it widens the correctional net needlessly and is an undue invasion of privacy. It is

not inconceivable that judges and prosecutors enamored with the technology could adopt the policy of including everyone under community supervision in an electronic monitoring program. This excessive use of the technology should be avoided. To reiterate a caveat mentioned above, the technology should not be used if other surveillance technologies which are less expensive and less intrusive work equally well.

Being diverted from prison or jail is a benefit to the probationer, but excessively long periods of house arrest may have adverse effects. Some might argue, for instance, that it would be cost beneficial to use electronic surveillance to hold people under house arrest for 24 hours a day, 7 days a week. If this condition were imposed for any length of time, it would be abusive in two ways. First, if the offender represented such a threat to the community that prolonged house arrest was necessary, she or he probably needs to be in an institution. Secondly, such protracted and continuous confinement is antithetical to the purposes of probation.

To a lesser extent, and for the same reasons, long-term partial confinement during weekday evenings and weekends can be abusive. Such a regimen of confinement may be reasonable for several months, but if an individual has demonstrated that she or he can work during the day and obey curfew restrictions in the evenings and on weekends, why continue such extensive monitoring? Would it not be better to reduce the level of supervision and use the equipment on some other probationer in need of more extensive supervision?

Some suggest that the technology represents an unwarranted invasion of privacy, and sooner or later litigation will ensue. While one should never rule out the possibility of litigation, the authors believe that if the monitoring program is voluntary and used appropriately, litigation is unlikely. Since offenders diverted to the program would have been incarcerated otherwise, they are not likely to sue, since prison is a less desirable alternative. In fact, electronic monitoring is a "bird nest on the ground" for defense attorneys looking for leverage in plea negotiation, and therein lies a potential abuse of technology. The busy prosecutor may become too willing to negotiate pleas resulting in probation with electronic monitoring, when the more appropriate sentence would be incarceration. For this reason it is critical to involve both the prosecutor and the courts in developing diversionary policy long before the purchase of a system. In the absence of a well conceived and mutually agreed upon diversion policy, it is easy to see how the technology could be misused in the plea negotiation process.

Some of the administrators interviewed expressed concerns that the technology could replace the probation officer. This certainly would be an abuse of the technology. If the primary purpose of the technology is to divert offenders from institutions, then by definition these offenders need more human contact than conventional probationers, not less. All the technology provides is an automated means of monitoring during curfew hours. It would certainly be an ill conceived policy which suggested that high risk offenders be released into the community with nothing more than electronic monitoring. If such offenders needed no more supervision than that, they probably should not be under such an intensive and costly form of supervision in the first place. The properly conceived use of the technology is not as a replacement for the probation officer, but as a tool which frees the officer to make better use of his or her time.

The technology should not be conceived of as a quick fix for the complicated problem of a community's overcrowded jail or a state's overcrowded prison system. Overcrowding is a complex problem, unlikely to be solved simply by purchasing an electronic monitoring system. A community or state facing overcrowding problems needs to conduct an indepth analysis of why the problem exists and identify various alternatives which can ameliorate the situation. Electronic monitoring might be a useful tool but certainly not the sole remedy for the problem. It cannot be used as a substitute for sound correctional policy development.

Although practical experience is limited, common sense suggests that certain kinds of offenders may be inappropriate candidates for electronic monitoring. Given current public sentiment about the treatment of sexual offenders, it may not be wise to include them in the early stages of a program. This is not to say that such individuals could not benefit from the program, rather that subsequent violations committed by sexual offenders under electronic monitoring may arouse such strong community reaction as to jeopardize the use of the technology with other suitable offenders. Common sense would also suggest that offenders with a history of spouse or child abuse are not suitable candidates. In this case, the use of the technology may put the offender's family in clear and imminent danger.

Finally, one needs to carefully consider the potential use of the technology with juveniles. Communities vary, both in the extent of delinquency and in their corresponding tolerance for the criminalization of the juvenile justice system. Other things being equal, the technology could be a very effective means of responding to early signs of delinquency. However, the danger always exists that the juvenile justice net will be widened too far and that the ill effects of labeling, attendant with an over reaction to deviance, could become excessive.

Philosophic Concerns

Inteviews with probation administrators suggested that

there is a wide range of philosophic attitudes toward the technology. On the one hand, some see it as a useful tool which could find a proper place in probation. Others see it as one step beyond what probation is supposed to be. Most administrators, however, expressed a philosophic ambivalence about the technology. They realized that probation must change with the times but were uncertain whether electronic monitoring was an appropriate change for probation. These administrators might be characterized as sitting on the fence. While mildly interested in the technology, they would rather let some other agency experiment with its use before taking the plunge themselves.

It may be that the differences in attitude found among the administrators surveyed emanate from divergent views as to the purpose of probation. Some see probation as primarily a surveillance function, and although they are not opposed to the ends of rehabilitation, they are not likely to take risks when asked to choose between these two objectives. In all likelihood, administrators who hold this view will come more readily to the use of electronic monitoring technology.

Other administrators approach probation from a more humanistic perspective. While they do not discount their responsibility to assure public safety, they give relatively more emphasis to the rehabilitative goals of probation. These administrators are more sensitive to the Orwellian connotations of the technology and view it as one step beyond the appropriate function of probation. They might characterize the philosophy of probation in the following way. Offenders make mistakes, but some have enough going for themselves that society can take a chance on letting them remain in the community. The purpose of probation, therefore, is to allow offenders to demonstrate that they are trustworthy enough to live among their fellow citizens. While some degree of human surveillance is prudent, the probationer must be given enough room to demonstrate trustworthiness. Given this philosophic point of view, some administrators feel that electronic monitoring goes beyond trust and therefore beyond the scope of what probation should be.

Summary

It should be clear that the prospect of using electronic monitoring in probation raises a variety of concerns. From the narrow perspective of direct cost, the technology is cheaper than the operational or new construction costs associated with institutions. But the cost-benefit tradeoffs become more murky when indirect costs and benefits are assessed and the lost opportunity costs are factored in. While it may be a helpful technology for the manager of an overcrowded institution, it may be less cost beneficial to the probation administrator with other pressing needs. Careful reflection indicates that the technology cannot solve the overcrowding problem, nor can it be used as a substitute for long-term correctional policy development. At best, it can be used in conjunction with other alternatives to help resolve the overcrowding problem.

The introduction of the technology into a probation department will necessitate various administrative and organizational changes. The department will be put on a 24-hour a day footing, which may be contrary to its current personnel practices, history, and traditions. New personnel may have to be employed. New procedures will have to be instituted to screen candidates for the program, to determine the appropriate length of time that probationers should be under surveillance, and to direct decisionmaking in cases of false alarms and curfew violations. The technology should be used primarily for diversion, not as a substitute for or as an addition to, conventional supervisory practices which work equally well.

Finally, it should be said that the technology is probably not appropriate for every department. The utility of the technology must be weighed against other pressing needs. Departments which have already established proven conventional supervisory strategies may find that the technology offers little. The ultimate empirical question is whether the technology reduces risk to the public or enhances the opportunity for rehabilitation any better than conventional supervisory strategies which cost less.

REFERENCES

Berry, B. "Electronic Jails: A New Criminal Justice Concern." *Justice Quarterly*, 2/1, 1985, p. 1-22.

Bureau of Justice Statistics. *Probation and Parole, 1982.* Washington, D.C.: U.S. Government Printing Office, 1983. p. 2.

Conrad, J. P. and M. G. Rector. *Should We Build More Prisons?* National Council on Crime and Delinquency, 1977.

Funke, G. S. "Economics of Prison Crowding." *The Annals*, Vol. 478, March 1985, p. 86-99.

Ingraham, B. L. and G. W. Smith. "The Use of Electronics in the Observation and Control of Human Behavior and its Possible Use in Rehabilitation and Control." *Crime and Justice 1971-1972.* J. Susman, Ed., New York: AMS Press, 1972, p. 363-377.

Nogel, S., P. Wice, and M. Neef. *Too Much or Too Little Police: The Example of Pretrial Release*, Sage, 1977.

SIXIEME PARTIE

PART VI

TECHNOLOGIES AUDIOVISUELLES

AUDIO VISUAL TECHNOLOGIES

VIDEO TECHNOLOGY IN CRIMINAL JUSTICE:

LIVE JUDICIAL PROCEEDINGS AND PATROL AND SURVEILLANCE

By

Ray Surette, Ph.D.
Florida International University

Introduction

There are basically two ways of using video technology in the criminal justice system: in live electronically connected gatherings or in lagged proceedings in which activities are pre-recorded and shown later (Doret, 1974:233). This essay will discuss the incorporation of video technology into the criminal justice system focusing on examples that emphasize live electronically connected applications. The first example will focus upon live video connected judicial proceedings. The second will examine the use of video technology for surveillance and patrol in law enforcement. Due to the effects of news coverage, the impact of video has, of course, been a long standing concern within the criminal justice system. The key difference however, between these new applications of video technology and news media video coverage, is that in news coverage the equipment is tangent to the activity and normally the goal of justice system personnel is to have the participants ignore the equipment. With news coverage the desire is as much as possible for the media and its technology to be an unobtrusive addition to the activities. But in these new applications, the participants must interact with the equipment, which has become central to the activity and therefore cannot be ignored. From a practical standpoint the equipment has changed from a temporary passive visitor to a permanent active tool and this change has raised new concerns and issues.

Live Judicial Proceedings involve the electronic expansion of the traditional courtroom so that the defendants, witnesses, judges, or lawyers can be separated but electronically linked for live visual communications. In a real sense, what occurs is the "diffusion" of the traditional courtroom to physically isolated but media connected locations, usually connecting a judge with other criminal justice personnel or defendants. The available technology allows various configurations and technical ways of achieving these communication links and this flexibility has resulted in numerous applications in the criminal justice system.[1]

The most extensive use of live interactive video for judicial proceedings has involved misdemeanor arraignments. Not only does the handling of misdemeanor cases comprise a large proportion of a judicial system's caseload, it also invokes a number of logistical and practical stresses in the system. In response to these pressures, video misdemeanor appearances were introduced to reduce the number of court and correctional personnel

---

[1]The first recorded use of video in the courts was in 1962 in Michigan to connect a courtroom to a law school to permit viewing of trials by law students. Picturephone service was first used to carry out a remote video argument of an appellate case between Washington, D.C. and New York in 1975 (Weis, 1977). Currently, there are numerous potential uses of media technology available to the courts. Traditional trials, first appearances (sometimes called preliminary arraignments), and misdemeanor arraignments have been videotaped in order to create a visual and audio record of courtroom proceedings. It has been used to record physical evidence for courtroom presentation. It has been used to recreate or simulate a crime, accident, or other event. It has been used in line-ups, confessions (particularly where the voluntary nature of the confession is questioned (cf. Benowitz, 1974), drunken driving tests, (Greenwood et al., 1978) Miranda warnings, shoplifting cases, police surveillance of narcotics transactions (Salvan, 1975), and the booking of suspects.

involved in first appearances, to reduce costs, to increase courtroom security, to alleviate courtroom crowding, and to speed up the handling of cases.

Despite the fact that many commentators have nodded approvingly at the judicial use of video,[2] these applications raise a number of questions. For example, what effect does the introduction of video equipment into the judicial process have upon the relationships between the participants? What effect does it have upon the ability of defendants to interact with their attorneys and judges? How do defendants feel about the use of videotape? The unresolved questions revolve around three basic issues: the efficiency in cost and effort in using video technology versus traditional courtroom methods, legal questions regarding admissibility and due process, and effects upon courtroom participants, atmosphere, and decorum. The search for answers to these questions begins with research conducted in the 1970s concerning videotaped testimony, for a number of the concerns currently expressed about live video proceedings are similar to previously raised concerns regarding the use of pre-recorded video testimony and videotaped trials.

Of relevance for live usage, a loss of the completeness in the information communicated was thought to be likely and it was felt that video could not capture the total psychological and physical essence of a witness

---

2See Monteleon, 1982; Greenwood et al., 1978:27; Murray,1978; Barkel, 1975:956; Kosky, 1975 :231; Burt 1976:66; Lieberman, 1976:89; Salvan, 1975: 225; Benowitz, 1974: 86-88.

(Brackel, 1975:957).[3] Perceptual distortions were also a concern in that video would favor some witnesses who appear more positively on television and disfavor others who are not telegenic. To the extent then, that video increased the degree to which credibility is assessed on the basis of the looks of the witness, it was felt to emphasize a factor extraneous to determining the truth of the testimony (Doret, 1974:244). Lastly, a loss of courtroom decorum and the innate biasing of the information communicated through television was cited. One of the chief problems attached to the use of video dispositions was that of boredom (Benowitz, 1979:90), particularly when such presentations were compared with commercial television. It was feared that a juror would bring their television experience to judicial viewings, expecting similar entertainment style, engaging sessions (Doret, 1974:245; Monteleone, 1982:863).[4]

Spurred by these concerns, the research conducted on the effects of videotaped testimony focused on jurors' attention span, boredom, ability to

---

[3] In terms of videotaped testimony, but not a major concern for live proceedings, the crux of these early complaints involved the loss of a two-way communication system with feedback. Videotaped testimony is changed from a total communication system to a one directional process and feedback information is lost not only for juries but for attorneys, witnesses, and judges.

[4] This concern is best stated by Hartman (1978:256-257):

> Research has demonstrated that the whole juror comes to court: he brings to the courtroom his entire experience with the media. That experience includes watching soap operas, tv westerns and gangster movies, where actors may die ghastly deaths, but spring to life to play new roles again. Further research is necessary to tell us whether we can fully separate television as reality from television as entertainment. We don't know what unconscious forces might be at work affecting our judgment when we see a criminal trial in the form of a television program or movie

retain information, reach decisions, and detect lying. The largest amount of work was conducted by Miller and Fontes over a four year period at Michigan State.[5] They concluded (1979b:207): "Within the confines of our research, there is no evidence to suggest that the use of videotape exerts any deleterious effects on the juror responses studied; in fact, as far as retention of trial related information is concerned, it appears that videotaped testimony sometimes results in higher retention levels." Hence, despite a number of initial concerns regarding this technology, video passed its first crucial test. And while issues remained, procedural barriers fell and videotaped testimony became regularly accepted within the judicial system.[6]

---

[5]Their studies involved civil trial reenactments in courtrooms with real judges and jurors from regular jury pools. Jurors were told that video trials were actual cases and that their decisions would be binding. In examining the effect of viewing taped testimony on the judgment of the jurors for four editing modes (clean edit, video only edit, blackout, and blackout and fast forward) Miller and Fontes report that, "Juror responses to the live and taped trials did not differ significantly (1979a:96); our findings do not support the argument that videotape will curtail jurors' abilities to assess the demeanor of witnesses" (1979a:100). In fact, non-verbal cues may hinder rather than help a juror make accurate judgments and the highest percentage of correct judgments were with written transcripts. Miller and Siebert (1974, 1975) also conducted studies that support the general conclusions of Miller and Fontes. The conclusion from this body of research is that video does not affect significantly juror verdicts or monetary awards. It should, however, be noted that this research involved civil cases for the most part and did not involve criminal concerns. The question remained whether videotape has differing effects in criminal cases, whether it dehumanizes a proceeding, or whether it results in the loss of legitimacy for the judicial system (cf Hartman, 1978).

[6]Videotaped dispositions were first sanctioned in the Federal courts in 1970 and now all but a handful of jurisdictions accept videotape as a disposition medium.

But more extensive uses of video were still resisted. Even some authors who advocated its use for dispositions, argued that it was inappropriate to present entire trials or even large portions of a traditional trial by videotape (cf Farmer et al, Brackel, 1975; Shutkin, 1973). Their hesitation lies in the extension of its use from a small segment of the total testimony in a trial to being the sole or primary method of testimony presented in a trial. One U.S. jurisdiction in Ohio has experimented since 1971 with the use of videotape as the sole means of presenting testimony in a trial, creating Pre-Recorded Videotaped Trials (hereafter PRVTT).[7] As such, PRVTTs constitute a marked departure from a traditional trial in that video becomes the exclusive means of presenting testimony without regard to the availability of the individual witnesses, all extraneous and objectionable statements are eliminated from the jurors' knowledge, and the presence of counsel, judge, and ligating parties are not required while the testimony is being shown to the jury (Coleman, 1977). It has been reported that after participating in PRVTTs, jurors have generally favorable reactions to their use (Coleman, 1977 citing Bermant et al, 1975) and according to proponents, PRVTTs have been very successful in reducing

---

[7] In a PRVTT an entire trial is pre-recorded, edited, and subsequently shown to a jury. "Although similar, the videotape trial is more than a procedural extension of videotape depositions. Videotape is not incorporated into the normal trial framework but is the sole means by which evidence is introduced to the jury. ... The essence of the videotape system is that it allows the trial to be subdivided into three units - testimony (involving lawyers and witnesses) rulings (trial judge and lawyers) and presentation (jurors). These units proceed chronologically but relatively independently, each impinging only slightly on the schedules of the others" (Shutkin, 1973:362-363).

crowded court dockets and in cutting the amount of time needed to complete a case.[8]

Irrespective of its advantages however, critics have argued against the expanded use of video to incorporate entire trials. PRVTT's have not been accepted outside of Ohio and their use is not expected to increase in the near future. The reluctance appears to revolve partly around constitutional questions[9] and more significantly around the effects of total videotaped trials on the normative atmosphere of a courtroom. Critics of video technology frequently mention the resultant changed social relationships between courtroom actors. For example, Brackel (1975:958 see also Doret, 1974 and Shutkin, 1973) argues that one is inescapably drawn to the conclusion that expanded use of video will produce drastic alterations in the trial process, in interstitial experiences and procedures, and ultimately in verdicts. The presumption behind the formal court setting and proceedings is that they have an impact on witness performance and perception, as well as on the behavior of other trial participants and observers. Brackel (1975;957,958) states:[10]

> The trial process itself will be altered as will the relationships between and among lawyers, parties, witnesses, and judge. From a drama

---

8See McCrystal, 1976; McCrystal, 1978:253-254; Murray, 1978:260-261; Miller and Fontes, 1979:92). The acceptance of the empirical evidence of positive PRVTT effects must be tempered, however, as PRVTTs have yet to be fully evaluated in a rigorous manner.

9Among the problems foreseen in such extended use of videotape in the courtroom is the constitutional issue of the right of confrontation, the right of the accused to be present during his trial, the right to a public trial, and the requirement of the presence of the judge at the trial.

10See Shutkin, 1983:391 also.

> directed and to various extents controlled by a professional and "impartial" judge, the trial will be transformed to a far more "partisan" event, directed and controlled by a larger variety of participants - lawyers in all their variety of competence, personality, and partisanship: cameraman of varying degrees of neutrality and proficiency: and witnesses who will be less readily surprised or otherwise made to lose their poise.

Doret (1974:256) and Koskey (1975) further note the importance of the courtroom as a mechanism of legitimization. Its symbols and processes are important in and of themselves and by severing the testimony from the courtroom a crucial function of the trial in the larger social community may be sacrificed. Kosky (1975:26 quoting Ramsey Clark) concludes:

> A jury in a room with a witness will produce a much more sensitive human evaluation and clean video trials may be too sensitized: "That perhaps some of the apparent disadvantages of present trial procedures are good in that they are educative and socializing....[live judge rulings and corrections] convey a metacommunication that what the juror is viewing is an important and dignified social event.

Similar to videotaped dispositions, live video proceedings have also enjoyed increasing applications in judicial systems, particularly for preliminary hearings.[11] But like them, live video proceedings have raised concerns regarding the constitutionality of the proceedings, the restriction and distortion of communications, the loss of system legitimacy and decorum, and the effects on the normative and social environment of the system. A survey of the publicized systems used for arraignments reveal both successful and unsuccessful programs.

---

[11]The first live video proceeding was most likely a bail bond hearing in Cook County Circuit Court in 1972.

Since 1974 the city of Philadelphia, for example, has linked its 9 police divisions, its 22 district police headquarters, arraignment court, and the central police administration building into a closed circuit multi-purpose video system (Target, 1979:1). For an arraignment, the judge reads the charges to the defendant, asks about the assignment of counsel, sets bail, and schedules another court appearance date. No pleas are heard (New York City, 1983:21). However, the Philadelphia police believe that the savings in transportation costs gained by the use of their video system is more than offset by the additional police staffing needed.[12] Although still in use, according to the Court Administrator's Office, the system will most likely be dropped in the near future when a new court building becomes available.

In addition to Philadelphia, Phoenix, Arizona; Santa Barbara, California; Suffolk County, New York; Boise, Idaho; Las Vegas, Nevada; Los Angeles, California; and Miami, Florida also have installed systems to conduct live video proceedings. The system in Phoenix, a videophone system that used existing telephone lines, was discontinued because of the expense (approximately $3000 per month phone service) involved (Rockwell,1983). While in operation, however, this system did not elicit any serious opposition from participants and if a need for a remote site developed

---

[12] Two officers are needed to operate each console, which, on a 24 hour basis, entails assigning 8 officers to the operation of the CCTV (New York City, 1983:18).

in the future a less expensive video system would be favored.[13] Santa Barbara's system has been in operation since 1981 and is used primarily by probation officers and public defenders to communicate with their inmate-clients at the Santa Barbara County jail (Court Vision Communications, n.d.). Since 1985 it has also been used in the Maricopa Superior Court to arraign defendants held in custody in county jail who are entering a plea of not guilty (Coleman, 1977:17). Despite reports of this microwave system being down approximately half the time and the Public Defender's Office opposition to its use in any judicial proceedings, there are no plans to discontinue the system.[14] Suffolk County, New York's system began in 1982 and linked the police precinct headquarters with the courthouse some twenty miles away (New York City, 1983:9). This system also has been dropped due to expense and cost overruns.

Boise, Idaho's system went on-line in 1979 (Gilmore, 1980:397). Unlike other jurisdictions, Boise judges also conduct the preliminary arraignments of felony offenders. In addition to its use during arraignments and first appearances, the system is used by the public defender's office to interview clients and by

---

[13] Transportation and prisoner security are not currently concerns in Phoenix and therefore there is not a perceived need for a system (comments based upon interview conducted with G. Allison, 6/30/87 Maricopa County Criminal Court Administrator's Office).

[14] Comments based upon interview with G. Maurer, Public Defenders Office 6/30/87.

the prosecutor's office to interview sheriff and police personnel. This system is still in operation and there are no plans to discontinue or limit it. Like Boise, Las Vegas's system was fully operational in 1979 (Brown, 1980). An average of 2300 hearings a month are processed by this system and its use will probably be expanded in the near future.[15] Los Angeles County has a pilot video arraignment system in use in its Glendale Municipal Court. Used for both felony and misdemeanor hearings, the system connects defendants and public defenders with judges and prosecutors one block away and is well accepted and thought reliable by bench and attorneys (Antonovich, 1987). Of more than 3000 defendants processed, only three have refused video arraignments. The first year report is positive and it is expected that the project will be continued.[16] Lastly, the Miami, Florida 11th Circuit Court program began in 1982 (Surette and Terry, 1984).[17] When

---

[15] Las Vegas, 1978; Interview conducted with Judge Brown, City Municipal Court 6/30/87.

[16] Interviews conducted 6/30/87 with M. Judge, Public Defenders Office and R. Mimura, Criminal Justice Committee, Glendale, California.

[17] Additional systems in all likelihood exist. Rockwell (1983) reports, for instance, that the Louisiana Judicial Newsletter of May-June 1982 reported the approval of $75,000 for the construction of a closed circuit T.V. link between the Baton Rouge downtown jail and the Baton Rouge City Court. In addition, Gilmore (1980: 398) notes that a vendor told him of receiving 30 orders from various judicial units to install equipment as soon as grant applications had been approved. How many of these systems were installed is unknown. Moreover, since the installation of these systems has frequently rested upon the availability of federal funds, the cut back of these funds in recent years has probably affected the introduction of these technologies into the courtroom.

arraigned, Miami defendants are called to a podium in the county jail chapel where they are informed via video of the charges against them and pleas are heard. To date, some 40,000 defendants have been arraigned and there are plans to expand the system in the near future.

As can be seen, the life of these projects has been mixed with five jurisdictions satisfied with their use of live video proceedings and three not. The expense of a system is the most often cited reason for their discontinuation and technical reliability, even when downtime seems significant, has not been forwarded as a major problem. Also despite the fact that video images have been criticized as inadequate substitutes for live interactions, appeals based upon the loss of due process protections and the inherent inability of a video proceeding to be fair have all been unsuccessful. However, early published reviews have largely ignored questions of the effect of the technology on attitudes of the participants, concentrating instead on the efficiency and cost of the equipment. Therefore, unfortunately little is understood regarding the dynamics of the successful versus the unsuccessful implementation of the technology or its systematic effects after installation. Based upon conversations with personnel in the various cities, the initiation and continued support of the judiciary appears to be crucial for long term success[18] and at

---

[18] Ironically, the primary advantages of these programs accrue not to judges, but to other system personnel in that they save time traveling and waiting for a judge to be available (Doret, 1974).

least in these surveyed systems, hard wire set-ups appear to perform somewhat better than microwave systems. In sum, the successful programs appear to have employed less expensive approaches, have early organizational support of the people who will operate and use them, and have limited initial set-ups and applications. More complicated and expensive systems seem to lose support and experience more difficulties, perhaps because the initial expectations are higher or unrealistic.

In terms of broader systematic effects, a program that has been evaluated is the Miami, Florida program.[19] Within the evaluation, all of the judicial participants involved and a sample of the defendants were surveyed to explore sentiments towards the use of video equipment in a judicial setting. The results revealed that the four judges using the video all agreed that it is an improvement over previous means of conducting arraignments and that there is less general disruption during video arraignments. The judges also reported that the use of video either increases or has little effect upon their ability to maintain control, to evaluate demeanor, or to communicate with defendants. They all felt that video either increases or has little effect upon the speed of the arraignments, the effectiveness of the defendant's legal representation, or the humanization of the arraignment process. Judges' complaints focused upon the techni-

---

[19] See Surette and Terry, 1984; Terry and Surette, 1985.

cal quality of the video picture and sound system, especially feedback and echo problems. All of the judges felt that the system should be expanded. None felt that it should be restricted.

The four state prosecutors in Miami also viewed the video arraignment system favorably, but slightly less than the judges. Two felt that the video was an improvement over prior arraignment methods. Two did not. Nevertheless, they all felt that the use of video did not detract from the overall quality of legal representation and that the speed of arraignments and sentences received were unaffected. In criticism of the system, several prosecutors felt that the video system made it difficult for defendants to communicate. Regardless, all four prosecutors concluded that video arraignments are a good idea. In fact, they thought that more cameras should be added to the system and that it should be expanded. None felt that the system should be restricted or eliminated.

Unlike the judges and prosecutors, all seven public defenders involved in the video arraignments felt that their use of video decreased the judge's ability to control the courtroom. Six felt that there was more general disruption during video arraignments and that the quality and effectiveness of legal representation were negatively affected. They felt that video arraignments were more impersonal and less humane and that their defendants were nervous, intimidated, and more likely to plead guilty. In sum, none of the public defenders felt that the video arraignments are

a good idea, or that it represents an improvement over previous methods.[20] The thrust of their criticisms focus upon the normative environment of the courtroom. In the Miami system, public defenders are confined to the jail's chapel, a non-judicial location; whereas the judge and prosecutor remain in the more familiar surroundings of the courthouse. Consequently, they feel that the traditional courtroom atmosphere has been lost and their ability to act as an effective advocate for the defendant has been diminished.[21]

Contrary to how public defenders feel, however, Miami defendants largely support their video arraignments. Based upon a survey of 352 video arraigned defendants, the majority felt that their ability to argue their case was unhindered (64.3%), as was their ability to ask questions (78.4%). More than three-quarters

---

[20] The public defenders volunteered the following comments (Surette and Terry, 1984):

> "The video system presents only an image of the accused. The personal confrontation which is essential is effectively removed." "No courtroom atmosphere - the prison chapel with a T.V. screen on the altar beneath the crucifix totally lacks any courtroom atmosphere" "By having the arraignment in the chapel, judges can "turn us off." The state attorney, however, is 5 feet from the judge. It makes our positions very unequal." "It puts the judge and prosecutor on the same side and the public defender and the defendants on the other - the good guys versus the bad guys."

[21] In the Las Vegas system, the public defenders remain in the courtroom with the judges and prosecutors and not surprisingly according to developer Judge Brown, they are as supportive of the system there as their judicial counterparts. They are also provided pre-hearing access to the system to conduct confidential conferences with their clients.

of these defendants (79.1%) felt they acted and spoke as they would have, had they been in a "regular" courtroom. 85.5% felt their plea was the same as it would have been had they pled in "regular" court. In short, 72.1% felt that using video for misdemeanor appearances is a good idea and 78.5% were happy with their court appearance.[22]

The Miami system's evaluation shows that video can achieve its manifest objectives, namely, easing the mechanics and costs of processing misdemeanor defendants without being contrary to constitutional concerns of due process. In the process, however, its operation has lead to the development of at least one latent, unintended consequence; a disruption of the "traditional" courthouse culture. The development of this unintended consequence raises questions regarding the technology's effects on the public image of the criminal justice system as well as the normative working relationships between criminal justice personnel. The public image of the criminal justice system is particularly significant as it is related to the perception of the legitimacy of the entire criminal justice system. Legitimacy and public image arise as issues for programs in the second example area as well.

---

[22]However, a substantial proportion (24.9%) of these individuals were not happy with their arraignment. This proportion of dissatisfied defendants was found to be similar to the proportion found in a non-video group of defendants. Analysis of these findings indicates that negative perceptions are related to the arraignments' outcomes (i.e, release or return to jail) more than the use of video equipment (see Surette and Terry, 1984).

Patrol and Surveillance via video technology involves the electronic deterrence and detection of crime. Specific site deterrence programs such as bank, subway, and department store surveillance cameras have, of course, been in use for a number of years. These prior uses differ from the new applications in that the areas surveyed are small, there is a voluntary nature to the surveillance, and large areas of public domain are not involved. In contrast, the new programs use video technology directly in general crime prevention and focus upon large public geographic areas. Video surveillance programs take one of two basic forms: completely hidden systems that give potential offenders no indication that they are being observed or open systems that are clearly marked. Although the former is more geared as an evidence and apprehension mechanism, both types can take advantage of a "surveillance effect." That is, the deterrence of crime through the psychological impact of creating the belief that one might be under surveillance.[23]

---

[23] For example, with a hidden system, deterrence is accomplished by having and publicizing a mobile system that can be set up and moved at will so that one cannot be sure when it is being employed. Such systems can easily be secreted in vans. The idea of increasing community surveillance to deter crime was theoretically forwarded and given prominence in the early 1970s by Newman whose concepts of defensible space employ the guiding premise that community and building design can minimize the opportunity and likelihood of crime by increasing the sense of community or by not providing favorable sites for crimes to occur (Newman, 1972; 1975; 1976; see also Jacobs, 1971).

The importance of examining a program in this area revolves around several issues. The most obvious issue is the effectiveness of these programs, do they result in a reduction in crime? A second issue is the trade-off of privacy versus security. In response to crime, the criminal justice system, often prodded by the public, has begun to increasingly turn to media and video technology for more innovative countermeasures against crime (Surette, 1985; cf Marx, 1985:23). However, because of their nature, such programs inevitably result in a reduction in citizen privacy. A basic question is how these programs social costs compare against their benefits (Surette, 1985:79). Lastly, surreptitous electronic surveillance invariably raises the issue of "1984" governmental abuses and the legitimacy and image of law enforcement.

Interest in the use of surveillance as a crime reduction aid is not new and is based upon the idea that a surveillance effect will increase the perceived risk of committing crime (cf Mayhew et al, 1979). Generally, developments in this area have been encouraged by rapidly improving technology but have been hampered by a general lack of research regarding the most effective applications. Research based largely upon offender interviews does suggest that criminals take into account the perceived level of surveillance and likelihood of intervention when choosing to commit certain crimes (cf Reppetto, 1974). It is also likely that efforts to increase surveillance by the general public is probably

the least effective approach for using surveillance in deterring crime, but that increasing the surveillance capability (or the perception of its increase) of law enforcement officers, residents, and employees in that order does have promise (Mayhew et al, 1979). In addition, the impact of surveillance is related to the actual threat of intervention; that is, an initial surveillance effect without subsequent intervention is likely to soon wane (Mayhew et al, 1979).

Practical advantages that have been forwarded regarding the use of video technology in surveillance efforts include the reduction of the number of officers needed for patrol; an increased ability to provide full 24 hour a day patrol capability; a reduction in citizen fear of victimization; improved deterrence of street crime; an increased ability to apprehend and convict street criminals; increased response time; and lastly, an increased ability for supervisors to oversee and command line personnel and review field decisions.

On the other hand, critics have raised concerns that such use of video technology will be difficult to control and could lead to "1984" scenario abuses (Marx, 1985:23):

> Yet there are also potential dangers in institutionalizing such systems. They may encourage paranoia, suspiciousness, and vigilantism. They can weaken trust and offer a vehicle for malicious reporting from anonymous sources. In a different political climate, [they] would lend themselves equally well to informing on those who are merely different or unpopular rather than criminal.

Even when actually ineffective, these systems and the associated surveillance effect are criticized as psychologically too powerful and therefore dangerous (Marx, 1985:21):

> ...agents are clearly limited in the surveillance and coercion they can carry out, but they are free to create the impression of police omnipresence and omnipotence. What they cannot do by force or by the actual power of their technology, they may attempt to do by creating a "myth of surveillance."

The projects have also been questioned regarding their costs and the effectiveness and reliability of the equipment; the community image that the deployment of such systems project, and the probability that their use will have merely a crime displacement rather than a crime reduction effect.[24]

Despite these cited advantages and concerns and the increasing use of video surveillance by law enforcement agencies,[25] there are no definitive studies of the actual impact that video surveil-

---

[24] Nearly a decade ago a prophetic assessment was offered on the difficulties of using surveillance based programs in crime prevention by Mayhew and his colleagues (1979:12):

> The use of surveillance to reduce crime shares some of the usual problems of methods which attempt to reduce opportunities of crime (cf Mayhew et al, 1976; Clarke, 1977); they do not tackle underlying factors that may motivate offenders; they can appear negatively 'defensive'; and they cannot guarantee that crime is not merely displaced in time, place or method.

[25] For example, the City of Indianapolis Police Department makes extensive use of video technology. In crime prevention efforts the department employs a mobile van to supply video surveillance as needed. It has been used to tape crowd and people movement in gay areas in an attempt to trace and solve gay related murders, and is periodically used to tape in areas of high prostitution to deter both prostitutes and their customers (based upon interview with representative of the Indianapolis P.D. Public Information Office, 6/30/87). It is unknown how many police department have similar capabilities but most likely the number is quite high.

lance systems have on crime. The best known effort in this area involved the placement of closed circuit television cameras in the London subway system in the 1970s. This effort placed cameras in 4 London stations with transmissions sent to a central monitoring site. The cameras provided viewing of all principal station areas, were conspicuously mounted, and accompanied by notices stating the closed circuit television was in use. Monitor operators could either contact the station staff or nearest police station; make a public address announcement; or contact train drivers (Mayhew et al, 1979:25-26). The evaluation showed that the cameras reduced the incidence of both theft and robbery, with some evidence of displacement of theft offenses to other non-camera stations. The evaluators caution, however, that the effectiveness of the system might have resulted from its novelty and that in time offenders may discover that the system is less to be feared than they had imagined. Analogous to the announcement effect noted for highly publicized increases in traditional law enforcement efforts (cf Ross et al, 1970; Campbell and Ross, 1968), they warn that only the installation of cameras without actual intervention strategies would not likely be effective for a very long period (Mayhew et al, 1979:28).

The single examined effort covering a large outside public area involved the placing of microwave television cameras atop traffic lights in a downtown shopping district in Miami Beach, Florida (see Surette, 1985). This video "patrol" program was

designed to give a small city police department a significantly greater presence in its prime retail shopping district without the addition of patrol personnel by blanketing the retail area with television surveillance. The department reported that to provide the same level of police coverage it would have had to double its personnel deployed in the area (Miami Beach Police dept., 1982). The stated goals of the program were "to accomplish a reduction in elderly fear of street crime and to create anxiety and a sense of paranoia among the criminal element in that they [will] fear that their activities may be televised and recorded by the police" (Wooldridge, 1981:6). Thus, it was expected that the project would drastically lower the perceived fear of crime among the elderly and simultaneously deter street crime from the city's shopping district.

The specifics of the project included the strategic placing of 100 video camera housings along approximately two miles of the two retail shopping avenues of the city. A prominent sign stating "Police Television" was mounted with each camera housing. Of the 100 video housing located in the target area, 21 would actually contain a movable camera at any given time; therefore, "at no time [would] a criminal be able to determine which of the 100 housings actually contained a camera" (MBPD, 1982:1).[26] The focus of

---

[26]The entire assembled system consists of the following:

1. A portable TV camera which is wireless and controllable from a remote site. The unit has a self contained power source and receives TV images that are then transferred via microwave to a monitor.
2. A portable transmitter is contained at the same location as the camera. It transforms the TV images into a microwave and

deterrence in Miami was a specific class of crimes: strong-arm robberies, muggings, purse snatchings, and other street crime.

After implementation it was found that the microwave equipment was highly sensitive to wind and weather and suffered significant amounts of down time. The central pan/tilt camera was not operating 80% of the time and frequently as few as 3 of the traffic light cameras were working. Technical problems with the equipment most certainly had an impact on the effectiveness of the project.

An assessment of this project reported that an effect on crime in the target area is indicated but not fully established despite a recorded drop in crime with the installation of the cameras (see Surette, 1985). Police statistics did show a reduction in strong arm robberies.[27] However, without access to other city area crime statistics it cannot be ruled out that the target area reduction was part of a general decline in crime in the city and not due to the video system or whether the cameras had a displacement effect, lowering crime committed in their presence but

---

(continued)

sends them to a receiver.
3. A micro-video receiver captures the microwave, interprets it, and transfers it as a TV picture to a monitoring screen located in a central command center.
4. There is also one manually operated pan/tilt camera located at the main intersection which can move vertically and horizontally and has a telescopic lens.

[2]From a 4.83 per month average prior to the program to a 3.09 per month average after program startup (sig. .026).

increasing it in adjacent areas (Surette, 1985:83). Also area merchants did not perceive a reduction in their victimization rate, but irrespective of its impact on crime, the merchants did report support for the project.[28] Generally the clearest effect of the video system was psychological in that area merchants and the public were supportive of its continued use.

Despite this evidence of support and an apparent positive effect on crime, however, the project was dismantled by the city soon after the funding grant ended.[29] Designed as an open fully publicized deterrence system, the Miami Beach system nevertheless came to be faulted by the police department for not being a crime detection and apprehension system,[30] even though at the end of its first year of operation the department was crediting it with aiding a 70% decrease in area crime (Security Today, 1983:13). It is argued that this program suffered more from its political liabilities than its effect on crime[31] and it is likely that such

---

28 3.9% felt business had decreased due to the cameras, 26.2% felt business had increased, 67.2% no difference, 71.5% felt more secure, 27.2% did not; 89.5% would like to see the project continue, 6.2% would not (MBPD, 1983:83-84).

29 The equipment is being used in a traditional building security system within a new city courthouse.

30 "The system has failed totally. In the two years of operation, not one crime was recorded by the cameras" (Crime Control Digest, 1984:2 comment based upon interview with Miami Beach Police Chief Glassman).

31 Between the time of its development and its initiation, the Miami Beach held municipal elections in which 5 of 7 city commissioners were replaced and the video project became identified with the prior administration. The project also developed problems with segments of the tourist industry who where concerned with the image of the city projected by such a system (Surette, 1985:81).

general public surveillance systems are likely to be sensitive political issues when employed (cf Surette, 1985). The Miami Beach effort is best summed as: "Technologically a disaster, politically a liability, but psychologically a success."

Conclusion

This review indicates that video technology is useful in the criminal justice system, especially as a substitute for personal in-court testimony and as a means of presenting evidence and court room exhibits. There is less agreement, however, about its use as a substitute for live proceedings and as a means of providing patrol and surveillance. These concerns are traceable partly to technological feasibility questions but are even more rooted in social issues. The use of the technology is in most cases, efficient and legal questions of admissibility, privacy, and due process have been answered in support of the continued use of the technology in the United States. The technology's reception seem to lie in whether it is felt that a crucial element of justice is lost when transmitted via video. For preliminary and short procedural steps, most participants, including defendants, appear to feel that the integrity of the process in unaffected.[32] For longer, more significant, and more symbolic steps such as trials,

---

[32]However, it should be noted that public defenders largely remain unconvinced of the technology's advantages even for short procedures.

concerns and resistance rise. However, while initially promising, effects of this technology upon participants, upon the atmosphere and decorum of the judicial system, upon the perception of the legitimacy of the entire system, and thereby ultimately on justice in our society have not been fully answered.

Legitimacy. A prime unresolved issue is what is lost in legitimacy, symbolic impact, and public image of justice when video technology is employed? The justice system is a mechanism of adjudicating guilt and administering punishment. It is also a means of legitimizing the overall social system. As such, the courtroom and its personnel and the police have a symbolic value. In the courtroom actions contain a "majesty" and "mysteriousness" pointing to the sanctity and well-being of the larger society. On the street, the presence of a live policeman or conversely the assurance of knowing when one is being observed underlie the values of voluntary consent and involvement, privacy, and public control of law enforcement. Loss of these symbolic qualities may diminish the aura of legitimacy supporting the entire system and as was shown in Miami Beach, can undermine an entire project.

For example, one possible unexamined effect of video systems is their effect on courtroom visitors and family of defendants. These external observers also gather impressions of the criminal justice system, impressions which will affect how they view the legitimacy of the entire system. It is reasonable to expect that defendants, who are immediately threatened by punitive sanctions,

would be more concerned with "processing outcomes" than "processing mechanics." However, unthreatened observers may gain an image of the system that is unacceptable if they see the video as a degrading process in which the judge will not even allow the defendant into the courtroom. Inasmuch as these observers represent a larger body of individuals than the actual defendants, effects upon them should not be ignored. There is considerable desire to make the court system more effective and efficient; nevertheless, the system must remain a moral system if it is to remain a viable system of justice. In that family and visitors represent a larger body of individuals than the actual defendants, if the effect of video proceedings on courtroom visitors and defendant friends and family is to alienate them from the system, the gains in efficiency made with the employment of video may be worthless.

Workgroup Disruption. Comments, especially those from pubic defenders, indicate that the normative system of courtroom workgroup relationships can be upset by the introduction of video equipment. These systems also have the as yet unutilized potential to increase the supervision of law enforcement line personnel and thereby decrease line officer discretion. This could be accomplished either under live set-ups where supervisors could make actual field decisions or in lagged systems where actions and decisions are recorded for later review. What effect this would have on police morale or effectiveness or whether this would be a

positive or negative change is unknown?

Regarding lawyers, even if video is not constitutionally an issue, the question remains whether attorneys deliver equivalent representation if they feel legally and organizationally disadvantaged in video conducted proceedings? If their morale suffers, does their subsequent effort also suffer? An examination of case outcomes in Miami reveals no significant aggregate differences between video and non-video cases in terms of case outcomes (Surette, 1984). The possibility remains, however, that such an effect would develop only after a large number of cases over a significant period of time have had a chance to impact upon attorney attitudes and behaviors.[33]

Depersonalization. Planned expansions of these current systems will lead to the increased depersonalization of criminal justice processes.[34] Adjudication within the criminal justice

---

[33] The realignment of communication channels and changes in behavior and attitudes seldom occur simultaneously (Lipeta, 1980).

[34] The future experimentation with media technology in the courts seems assured with an extension of tests to additional procedural steps and the addition of new technology and capabilities. Miami for example has begun a test of video felony arraignment hearings and discussions are now underway about expanding the present system to include six other correctional facilities. Miami also plans to expand the use of the system to include hearing motions. In the planned expanded system in the console room at the courthouse, as well as in a room adjacent to the jail's arraignment room, there would be two booths with closed circuit television networks allowing defendants to talk privately with counsel or family members before, during, or after the proceedings. When court is finished, these networks could be used by the public defender's office so that they could interview their clients without having to drive to the jail. Other developing applications include the use of suitcase wireless video recorders and transmitter system (Security World, 1986), the mounting of video cameras on patrol cars to record driving behavior and vehicle stops (analogous to airline flight recorders), expansion to felony bond hearings, and multi-site full system networks linking

system is based upon the principle of face-to-face interaction, particularly that the accused are entitled to face their accusers. With the extended use of video technologies, however, there would be a decline in face-to-face encounters between police and the public, attorneys and their clients, and judge's and defendants thereby seriously altering the current normative and communicative structure of the system. This process will most likely be hastened by equipment advances that make this technology more economic and less obtrusive. Here again, the full overall effects of these changes may become apparent only after such practices have been in place for a longer period of time.

These and other unanticipated changes in the socialization process and the relative status and perception of work group roles and participants are crucial (cf Casper, 1978; Sudnow, 1965). For example, if these systems ultimately result in the significant loss of prestige or credibility of public defenders within the courtroom, either in the eyes of judicial work groups or defendants, or in the further isolation and separation of the police from the policed, the social costs of such losses would outweigh any organizational benefits that might accrue from them. As these systems are increasingly instituted, long term studies

---

(continued)

jails, stockade, public defenders offices, state attorneys offices, courthouses, and police stations using fiber-optic systems.

are needed to address whether such policy relevant effects are in fact developing.

References

Antonovich, M. (1987) Video Arraignment Pilot Project Gendale Municipal Court. Year End Report, Countywide Criminal Justice Coordination Committee xerox.

Benowitz, A. (1974) "Legal Applications of Videotape." The Florida Bar Journal 48/2 (February): 86-91.

Bermant, G., et al (1975) "Jury Responses to prerecorded videotape trial presentations in California and Ohio 26 Hastings Law J. 975

Brackel, S. (1975) "Videotape in trial proceedings: A technological obsession: American Bar Association J. 61:956-959.

Brown, C. (1978) "Video Arraignment Statistics" inter-office memorandum from Judge Seymore Brown, Chief Municipal Judge to Lloyd Zook, Court Administrator, March 21, 1980. Las Vegas, Nevada Video Arraignment Demonstration Project, LEAA Grant Proposal.

Burt, L. (1978) "The case against courtroom T.V." Trial 12/7 (July):62-63,66.

Campbell, D. (1969) "Reforms as experiments" American Psychology 24:409-429.

Campbell, D. and Ross, L. (1968) "The Connecticut crackdown on speeding" Law and Society Review 3:33-53.

Casper, J. (1978) Criminal Courts: The Defendants Perspective. NIJ/LEAA Government Printing Office.

Clarke, R. (1977) "Psychology and Crime" Bulletin of the British Psych. Society, 30:280-283.

Coleman, G. (1977) Video Technology in the Courts. Wash. Department of Justice

Court Vision Communications, Inc. (n.d.) Xeroxed news release.

Crime Control Digest, (1984) August 27:2-3.

Criminal Justice Newsletter, (1980) 11:7-8.

Dean, C. (1986) Electronic monitoring and control" Corr. Today, 48,#5 (July):36-38. [very light overview, mentions use of video equip. in prisons]

Doret, D. (1974) "Trial by videotape -- can justice be seen to be done?" Temple Law Quarterly 47 (Winter): 228-268.

Farmer, L., et al (1976) "Juror perceptions of trial testimony as a function of the method of presentation" in Psychology and the Law. C. Nemeth, N. Vidmar (eds), D.C. Heath Pub. Lexington Mass.

Gilmore, J. (1980) "Arraignment by television" Judicature, 63:396-401.

Greenwood, M., et al (1978) "Audio/video:technology and the courts." State Court Journal 2/1 (Winter):26-28.

Hartman, M. (1978) "Second thoughts on videotaped trials." Judicature 61/6 (December- January): 256-257.

Jacobs, J. (1961) The Death and Life of Great American Cities. Random House.

Kosky, I. (1975) "Videotape in Ohio: Take 2." Judicature 59/5 (December): 220-238.

Lieberman, J. (1976) "Will courts meet the challenge of technology?" Judicature 60/2 (August-September): 84-91.

Marx, (1985) G. "The Surveillance Society" The Futurist, June:21-26.

Mayhew, P et al. (1976) Crime as Opportunity. Home Office Research Study No. 34. London: HMSO.

Mayhew, P. et al (1979) Crime in Public View. Home Office Research Study no. 49. Her Majesty's Stationery Office, London.

Miami Beach Police Department. (1982) Miami Beach News Release. Public Information Office, February.

Miami Beach Police Department. (1983) Micro-video Project Yearly Report. Miami Beach P.D.

Miller, G. (1976) "The effects of videotaped trial materials on juror response" in Psychology and the Law. C. Nemeth, N. Vidmar (eds) D.C. Heath Pub. Lexington, Mass.

Miller, G. and Fontes, N. (1979a) "Trial by videotape. Psychology Today (May): 92,95,96,99, 100,112.

Miller, G. and Fontes, N. (1979b) Videotape on Trial. Sage.

Miller, G. and Siebert, F. (1974, 1975) Effects of videotaped testimony on information processing and decision-making in jury trials Progress reports no. 1 and 2 Michigan State University, RAND. N.S.F.

McCrystal, J. (1976) "The case for PRVTTs" Trial 12:56-57.

McCrystal, J. (1978) "Videotaped trials: A primer" Judicature 61:250-256.

Monteleone, Charles Darryl (1982) "Videotape depositions: Basic pointers for a skilled presentation." American Bar Association Journal 68 (July):863-865.

Murray, T. 1978 "Videotaped dispositions: The Ohio experience" Judicature, 61/6: 258-261.

Newman, O. (1972) Defensible Space: Crime Prevention Through Urban Design. MacMillan.

Newman, O. (1975) "Community of interest - design for community control" in Architecture, Planning and Urban Crime. Report of NACRO Conference, 12/6/74, London.

Newman, O. (1976) Design Guidelines for Creating Defensible Space, NIJ/LEAA Government Printing Office.

New York City (1983) New York City television Arraignment: Feasibility for New York City Criminal Courts. Unpublished report, February.

Reppetto, R. (1974) Residential Crime. Ballinger.

Rockwell, N. (1983) Videophones and Closed Circuit Television in Pretrial Proceedings. The research and Information Service of the National Center for State Courts, Memorandum, Ref. no. RIS.83056. May 6.

Ross, H., Campbell, D., and Glass, G. (1970) "The British breathalyser crackdown of 1967" American Behavioral Scientist 13:493-509.

Salvan, S. (1975) "Videotape for the legal community" Judicature, 59/5:222-229.

Shutkin, J. 1973 "Videotaped trials: Legal and practical implications. Columbia j. of Law and SOcial Problems, 9:363-393.

Sudnow, D. (1965) "Normal Crimes" Social Problems, 12:255-276.

Security Today. (1983) September:13-14.

Surette, R. (1984) "Two Media Based Crime Control Programs" in Justice and The Media, (ed.) R. Surette, Charles Thomas Pub.)

Surette, R. (1985) "Video Street Patrol: Media Technology and Street Crime" The Journal of Police Science and Administration, 13:78-85)

Surette, R. (1986) "The Mass Media and Criminal Investigations: Crime Stoppers in Dade County, Florida" J. of Justice Issues, 1:21-38.

Surette, R. and Terry, C. (1984) "Videotaped Misdemeanor First Appearances: Fairness from the Defendant's Perspective" in Justice and The Media, (ed.) R. Surette, Charles Thomas Pub.)

Target, S. (1979) "Philadelphia;s popular police station" International City Management Association March/April.

Terry, C. and Surette, R. (1985) "Video in The Misdemeanor court: The South Florida Experience" Judicature vol. 69, June-July:13-19).

Weis, J. (1977) "Electronics expand Courtrooms' Walls" Am. Bar Assoc. J. 63:1713-1716.

Wooldridge, F. (1981) Micro Video Patrol. Grant application - Community Development Block Grant Program (HUD).

AUDIO VISUAL TECHNOLOGIES - THE VIDEOTAPING OF POLICE QUESTIONING OF SUSPECTS AND ACCUSED PERSONS

By

Professor Alan Grant
Osgoode Hall Law School
of York University

INTRODUCTION

Over a period of two years, from July 1, 1985 to June 30, 1987 I have been collecting empirical data on the videotaping of police questioning of suspects and accused persons and comparing them to traditional police methods of recording such transactions in police notebooks and on written statement forms.

This research has been carried out at the Halton Regional Police Force in Ontario and the independent evaluation of the results is being sponsored by the Law Reform Commission of Canada. Three interim reports have already been produced and short descriptions of the early stages of the research have also been published in the literature[1].

When all the results are tabulated we expect that well over 2000 cases will have been compared, approximately one thousand of them involving videotaped interviews. In short, one of the Halton Districts (Burlington) has used videotaping procedures for interviews at the station with suspects and accused persons and another District (Oakville) has recorded such interviews on traditional police statement forms. The data collected involved both adults and young offenders.

Prior to this experiment, a great deal of prophesying had occurred in the literature about the perceived advantages and

INTRODUCTION

Over a period of two years, from July 1, 1985 to June 30, 1987 I have been collecting empirical data on the videotaping of police questioning of suspects and accused persons and comparing them to traditional police methods of recording such transactions in police notebooks and on written statement forms.

This research has been carried out at the Halton Regional Police Force in Ontario and the independent evaluation of the results is being sponsored by the Law Reform Commission of Canada. Three interim reports have already been produced and short descriptions of the early stages of the research have also been published in the literature.[1]

When all of the results are tabulated we expect that well over 2000 cases will have been compared, approximately one thousand of them involving videotaped interviews. In short, one of the Halton Districts (Burlington) has used videotaping procedures for interviews at the station with suspects and accused persons and another District (Oakville) has recorded such interviews on traditional police statement forms. The data collected involved both adults and young offenders.

Prior to this experiment, a great deal of prophesying had occurred in the literature about the perceived advantages and

disadvantages of taping these interviews in some form. As a result of the experiment we are now able to move from the a priori to the ex posteriori stage. In what follows I shall first identify the issues raised in the literature and then give some indication of the types of answers which can now be put forward on the basis of our, not yet fully completed, analysis of the empirical data collected from Halton.

PERCEIVED ADVANTAGES OF VIDEOTAPING CONSIDERED.

1. Police would be protected against unwarranted allegations of misconduct[2]

Under traditional recording practices involving notebooks and written statements Crown counsel relies heavily on the recollection of police officers to recreate the circumstances of the interview during a voir dire, and the defence, for this purpose, relies just as heavily on the recollection of the defendant. During a voir dire it is often a matter of dispute whether or not an allegation made against the police is "unwarranted". There being no objective record of the circumstances under which the interview occurred, counsel must often probe conflicting accounts of an interview to test the truth of the contradictory recollections of the principal witnesses. Under this system there appears to be no forum for such a contest other than the voir dire proceedings in court.

> Under videotaping procedures there can exist a record of the interview if the accused so desires. That record, on videotape, can be viewed outside the court by prosecution and defence counsel who, after reviewing it, can decide whether any voir dire need be held at all. Experience to date shows that in practice this consultation removes the voir dire from the courtroom.

The possible outcomes of this consultation are various and include the following:

a) Defence counsel may indicate that a plea of guilty will be forthcoming.

b) Crown counsel may decide not to use the tape at all, either because the case is strong without it or because he sees some chance of a successful challenge by the defence, e.g. an inducement.

c) Crown counsel may wish to use the tape for some purpose other than guilt, e.g. an aggravating or mitigating factor on sentencing.

d) Defence counsel may wish to use the tape to support a so-called drunkenness defence, where appropriate.

e) Neither counsel may feel that the tape helps either the prosecution or the defence and no further use of it is made.

f) Counsel may disagree on admissibility and a voir dire would occur before the judge. In practice this has proven to be the least likely possibility.

In this way it can be seen that not only are "unwarranted" allegations not made in court but also perhaps "warranted" allegations may not be made in court either, e.g. where Crown counsel decides not to offer a tape on the basis of a possible challenge. This is not, perhaps, a problem because both the accused and defence counsel have access to the tape: not only may they proceed with a complaint against the police or with some other civil or criminal remedy but they also have "evidence" supporting their grounds. In addition, the Crown prosecutor and senior police officers are in possession of a tape which allows them to judge the propriety or otherwise of police interrogation practices and to consider remedial action by way of advice and training or by way of disciplinary or other actions, if appropriate.

Not surprisingly, no cases of gross police misbehaviour have appeared on any of the tapes. If anything, police questioning appears to be excessively careful to avoid all possible suggestions of force, threats, inducements, or the creation of an atmosphere of oppression. In fact, defence counsel have, on occasion, expressed surprise at how undemanding some of the police questioning has been.

2. An element of publicity and accountability would be introduced into interrogation procedures.(3)

Prior to the advent of videotaping procedures, police officers gave evidence in court about how interviews were conducted but no one who was outside the room where they took place could really know what occurred. Even the officers themselves did not know how they looked and sounded when conducting an interview. Now they do know, as do their colleagues who view the tapes, either as part of the investigation or in a training session. Police officers now say that the experimental procedures have made them much more conscious of the need to be properly prepared before going into an interview. There is a great deal of professional pride involved in being regarded by one's colleagues as a competent investigator. An area of police activity once shrouded in mystery is being opened up not only to lawyers and the courts, but also to the police officers themselves.

3. The danger of "verballing" and similar problems would be minimized. (4)

Obviously the camera is at the station in the videotaping interview room. It is not peering over an officer's shoulder at the scene of a crime or other incident being investigated by the police. There is, therefore, no video record of what is said to the

officer at the scene or on the way to the station or even outside of the videotaping room when at the station. An unscrupulous officer, minded to invent a "verbal", continues under the Burlington procedures to have the opportunity to do so. But is it likely that an accused, who calmly denies all involvement in a crime and plausibly explains all of his actions at the relevent time to the police in front of a camera, would have blurted out some incriminating verbal admission in the period before the camera rolls or after it has stopped? How likely is a trier-of-fact to believe in such a "verbal" in the face of a timely "video" denial? It is still possible but the unscrupulous must now bear these factors in mind.

This evaluation has not encountered an actual allegation of a "verbal" during this project. "Verballing" appears to be a rare phenomenon in Halton courts, but even so the video technology could, at best, only reduce the likelihood of it occurring; it could never by its nature - being back at the station away from the on-scene action - provide a guarantee against it. Even audio-recording, while more flexible and more easily transported to locations away from the station, cannot provide such a guarantee.

4. Decreases in the number and length of voir dires.[5]
As indicated above, the voir dire has virtually disappeared from the Burlington court room. It has been replaced by an out-of-court conference between counsel, often following a joint-viewing of the videotape in the case. It is also true, however, that there are very few voir dires held at Oakville court. Even without video-technology, counsel in the Halton region do not very often challenge police evidence on the alleged verbal and written statements of accused persons.

5. There would be a reduction in disputes about who should testify on the voir dire.[6]
Since voir dires tend to disappear when video-technology is used this subsidiary problem disappears with it.

6. The Court's ability to assess, objectively, the accuracy of the testimony and the credibility of the witnesses would be enhanced.[7]
As already indicated, it is really counsel's ability to assess the strengths and weaknesses of their respective cases which appears to be enhanced by the use of videotape interviews. Indeed, the out-of-court conference between counsel usually results in tapes not

being used in court at all, either because there is a plea of guilty (by far the most common result) or because neither counsel sees the tape as advancing the case they wish to make (the next most common category). In cases where videotapes are shown to the court, the tapes are not submitted to a voir dire because counsel can agree on admissibility beforehand, and when they are shown in the trial proper it is often for purposes other than to prove admission of guilt (e.g. state of mind of accused) or at sentencing (e.g. a circumstance of aggravation or mitigation).

7. The admission into evidence of statements of accused persons would be facilitated.[8]

It is clear that police officers take great care to see that an accused is informed of his right to counsel and of his right to remain silent and since this is on the tape for everyone to see it reduces much of what defence counsel could do to undermine the admissibility of the content of the videotape. Hence, pleas of guilty or waivers of the voir dire are common results.

8. Elimination of doubt about the accuracy of the record and the contents of the statement.[9]

The healthy and growing case law on "accuracy of the record" that has been spawned by the traditional police

note book and written statement has not been contributed to by videotape procedures. That the tape is an accurate record of the interview in the videotaping room seems to be common ground amoung police, Crown and defence counsel.

9. Increasing "waivers" of voir dire by defence counsel.(10) Since we have no figures for defence counsel waivers in the period before videotaping began, we cannot say if waivers are on the increase. That waivers are a common phenomenon is certainly true of the Burlington experience but the same appears to be true also of the Oakville experience.

10. More "guilty" pleas, forthcoming more quickly. (11) There are more guilty pleas at Burlington than at Oakville. This is true not only in "video" cases, but also in cases where no police interviewing of any kind occurred. One source suggests that case preparation is generally of a higher quality at Burlington than at Oakville and that this explains the higher guilty plea rate. It has not been possible to confirm or refute this suggestion.

11. Reduction in police time in giving evidence in court.(12)
We have no longitudinal study to tell us how much time was spent giving evidence in court on voir dires and therefore cannot say whether it has decreased. Certainly neither Burlington nor Oakville officers spend a great deal of time in giving evidence on voir dire because they are not very often challenged whether under video or under traditional systems.

12. Positive effect on the public image of the police. (13)
No attempt has been made to discern the public image of Burlington or Oakville police before, or during this study and even if such a study were undertaken it would be extremely difficult to show that videotaping per se has had any effect on the public image of police in these areas.

13. There would be an improvement in police interviewing techniques. (14)
There is certainly a heightened consciousness among police about how they conduct interviews. Tapes are now viewed by the officers themselves, their colleagues, Crown and defence counsel, judges and juries, as well as the public at large either those present in court or those who may see on television an excerpt from a videotape used at a trial. (This latter

event happened in a recent murder case in Toronto where a videotape, introduced into evidence as an exhibit, was permitted by the trial judge to be copied for use (in part) on the evening news.) Whether this consciousness of exposure has, in fact, resulted in better interviewing is not known but it could well be a powerful stimulus towards competent professional performance.

14. Reducing the need for additional officers to be present at the interview.[15]

Traditional police note-taking and statement writing usually employs two officers at an interview with a suspect or accused. Usually one asks the questions and the other writes or types the exchange between the questioning officer and the accused. Videotaping technology does away with the second officer in the interview room. There is simply no role for such an officer to play. The statistics from Burlington and Oakville show clearly that with videotaping the single officer interviewer is the norm but that with written statements two officers often continue to be used at Oakville.

15. Reduction in stress in giving evidence on voir dire.(16) No records exist from which it could be determined if this is or has been a problem. Certainly with videotaping the voir dire tends to disappear and with it any associated negative effects.

PERCEIVED DISADVANTAGES OF VIDEOTAPING CONSIDERED.

1. Suspects being inhibited from making confessions they might otherwise have made.(17)

About 70% of the people who accept the opportunity to have their statement to police videotaped make confessions or admissions useful to the Crown's case. Only a small minority refuse "on camera" to be videotaped (about 4%). Serious as well as minor offences have been the subject of confessions and on occasion additional, previously unsolved crimes have been admitted to "on camera". There is little evidence that the suspect/accused pays much attention to the camera. The interviewing officer, relieved of the need for a typewriter, note book and statement forms, can concentrate on the issues which are relevant to the investigation in progress. The suspect/accused is also relieved of extraneous objects upon which to concentrate and tends to focus attention solely on the interviewer. It should also be noted that many more

interviewees make "video denials" of their involvement in crime than ever have had such denials recorded, in writing, by police using traditional procedures. In short, the videotaping procedures produce more recorded interviews of every type, be they confessions, admissions, denials or refusals to be interviewed.

2. Malfunctioning equipment and tampering with tapes.(18) No problems have arisen with malfunctioning equipment although isolated cases of operator error have occurred, e.g. failing to ensure that the recorder was in operation before commencing an interview whereby a confession was "lost". (On being advised of this the accused "confessed" again, not something the officer felt he deserved or could expect.) There have been no allegations, so far, that tapes have been tampered with in any way. In an experimental case, prior to the commencement of this evaluation, there was a rigorous test of the taping process during a voir dire in a case of false pretences. This interview had been taped by the investigating officer as part of the orientation process at Burlington. The videotaping procedures were upheld on the voir dire and the resulting interview was admitted in evidence.[33]

3. Imposition of a serious capital burden on law enforcement agencies. (19)

If a system can be validated which does not use multi-recording apparatus, universal transcription and professional camera crews then one is dealing with a cost burden significantly lower than if these factors are included. The Halton scheme is a low-cost scheme which uses a video-cassette as an electronic notebook, makes copy tapes available in lieu of transcription and employs no professional camera or lighting personnel. As such it is a "bare-bones" operation and if, over a two-year period, it can be shown to have produced accurate records of police interviews leading to satisfactory resolution of criminal cases from the varying perspectives of the police, Crown, defence counsel and judges, then costs can be looked at in the context of overall police budgeting allocations. By the end of the study it is hoped that the cost will be known of extending videotaping technology to the whole of the Halton Regional Police Force. From this one may be able to extrapolate costs more generally.

4. Allegations of police misconduct will continue to be made about the period before taping. (20)

This very obvious concern which, if experience proved it true, would greatly undermine - though not destroy -

the case for taping, has not turned out to be a problem to date. Neither in the allegations raised in court nor in the questionnaires returned to this evaluation are defence counsel suggesting that the situs of the problem has just moved to locations other than the videotaping room. There have been some suggestions that police in Burlington have, on occasion, run a "rehearsal" of what would happen on tape, before the videotaping occurred. This has been raised in court on two occasions, admitted in cross-examination by the officers concerned, and the judge has nevertheless allowed the tapes to be entered into evidence on the basis that no threats, inducements or other circumstances of a like nature had occurred during the "rehearsal".

5. Prejudice to the accused exceeding the evidential value of the tape.(21)

This concern takes several forms, mainly that the accused's appearance in the taped interview, whether by behaviour, speech, dress or language, may prejudice a trier-of-fact who may see a very different individual being presented at trial - i.e. differently dressed or behaving in a quite different manner from that portrayed on the videotape. Defence counsel recognize this as a possibility yet none of them would favour audio-tape as a means of lessening any possible prejudice. They point out that some of these matters can be helpful to the defence and even if they are not, an accurate record of the interview is worth the price of some risk of prejudice.

6. Lack of accurate portrayal from the fixed position of the camera.(22)

This does not seem to have been a problem. In fact, the very absence of anyone actively controlling the scene as it appears on the tape is seen as a neutral factor. While none of the tapes show professional camera work, all parties seem to be satisfied that they do show an accurate record of what happened in the interview room.

7. Differential effects of some police forces having videotaping and others not.(23)

It is inevitable that, as more judges obtain experience with videotaped interviewing, they may become less permissive of the worst features of inadequate note-taking or statement writing but most judges will no doubt take into account the actual facilities with which the individual investigator has to work. It can hardly be the fault of an individual officer if his police force, or his division or section of it, does not have access to videotaping for interviewing suspects or accused persons. At the same time, a judge may be entitled to draw a negative inference if audio-visual technology was available to an interviewing officer who ignored it and relied instead on some notes in his police notebook for the details of his interview

with a suspect/accused. This would be particularly true if the accused had offered to have the interview videotaped, if the technology had been available at the station and if the interviewing officer had declined to take up the offer. All of these are questions for permissible inference-drawing which judges are well suited to handle either as triers-of-fact or in instructing a jury.

8. Reduction in the supply of information about other crimes. (24)

We have collected information on this specific point from interviewing officers at Burlington and Oakville and it does not appear that Burlington officers are in any way impeded by the videotaping procedures in obtaining information from suspect/accused to clear up other offences. In fact, if anything, it appears that Burlington officers may receive more of such information than do Oakville officers although that may be a function of factors other than the tape per se. Certainly the taping process does not appear to have had the effect, feared by some officers, of "drying up" the flow of such information.

CONCLUSION

Final conclusions cannot be made until all of the data amassed over two years have been fully analysed. At this penultimate stage, however, the following observations can be made:

* Police officers at Burlington are very enthusiastic about using the videotaping technology and have obtained many more confessions and admissions with it than are being obtained in writing at Oakville. Oakville officers are now keen for the videotaping technology to be extended to their District.

* The videotaping process does not appear to inhibit suspects from making confessions or admissions (in two years at Burlington only 4% of the suspect/accused refused "on-camera" to be taped and around 70% of those interviewed on videotape made admissions or confessions).

* No distinction has emerged between the most common profile of suspects and accused persons who make videotaped confessions and of those who make denials or refuse to be taped.

* Suspects are continuing to admit major as well as

minor offences on tape.

* There have been no allegations at court or elsewhere of police tampering with tapes but some officers are "rehearsing" the interview "off-tape" before taping the interview in "official"form.

* Crown counsel indicate that there have been no problems in having the tape introduced into evidence in the few cases where this has proved necessary.

* In some instances, the case has not reached a contested trial because defence counsel has entered a plea of guilty after viewing the taped confession prior to the proceedings and assessing any other evidence.

* The videotaping process has saved court time in those cases where following a viewing of the tape outside court by the Crown and defence counsel, it has been agreed that the tape will or will not be used, without any need for a voir dire to take place before the court.

* The audio-visual equipment has been reported as functioning well, with no reported cases of mechanical failure.

* Maintenance requirements on the equipment have been negligible.

* So far, the quality of picture on the tapes, which are in colour, has been excellent. Sound quality is improved by mounting the microphone on the wall by the interview table and not, as at present, on the camera. Although this has not created any major problems, the site of the microphone at Burlington is in the process of being changed.

* There has been no evidence that costly professional camera crews or other special technical assistance is necessary to produce a clear and reliable record of the interview.

* The police budget costs involved in the videotaping process, when viewed in the context of the total police budget, do not appear to be a significant factor in deciding whether to implement a project of this sort.

* Defence counsel practising in the Halton Region are very positive about the videotaping project. They are satisfied that videotaping provides a more accurate account of an interview than do traditional police notetaking practices, about which defence counsel still have reservations.

* In the view of defence counsel, the accuracy and reliability of the videotaped interview outweighs any

disadvantage or prejudice to a defendant that may arise in some cases through a judge or jury seeing the accused as he/she appeared when interviewed as opposed to their actual appearance at trial.

* So far it has been possible to avoid almost all transcription of videotaped interviews with suspects and accused persons but both prosecutors and defence counsel would like to see interviewing officers provide a more detailed synopsis of the interview for the Crown brief to assist in case preparation and disclosure.

* The incidence of use of the two audio-visual interviewing rooms at Burlington suggests that only one such room is necessary for a police operation of this size.

ENDNOTES

1 Law Reform Commission of Canada: The Audio-Visual Taping of Police Interviews with Suspects and Accused Persons by Halton Regional Police Force, Ontario, Canada: An Evaluation.
First Interim Report dated December 31, 1985,
Second Interim Report dated June 30, 1986,
Third Interim Report dated January 5, 1987
by Professor Alan Grant. The Final Report is due on August 30, 1987. See also, Grant A., Video-taping Police Interviews, (1986) 2 Policing 184; Grant A, Video-taping Police Questioning: A Canadian Experiment [1987] Crim. L.R. 375.

2 Law Reform Commission of Canada, Questioning Suspects, Working Paper 32 (1984) at 59; id. Report 23 (1984) at 19; Peter Solomon, "The L.R.C. of Canada's Proposals for Reforms", (1985) 27 Crim. L.Q. 321 at 343.

3 Ibid., Working Paper 32 at 60.

4 Ibid., Working Paper 32 at 59.

5 Ibid., Working Paper 32 at 59; Report 23 at 18; Marquita Inman, "The Admissibility of Confessions" [1981] Crim. L.R. 469 at 480; Julie Vennard, "Disputes Within Trials Over the Admissibility and Accuracy of Incriminating Statements: Some Research Evidence" [1984] Crim. L.R. 15 at 24.

6 Ibid., Working Paper 32 at 59.

7 Ibid., Working Paper 32 at 61.

8 Ibid., Working Paper 32 at 61; Report 23 at 18.

9 Ibid., Report 23 at 18; Elliot Goldstein, "Using Videotape to Present Evidence in Criminal Proceedings" (1985) 27 Crim. L.Q. 369 at 377 and 383.

10 Ibid., Report 23 at 18.

11 Ibid., Report 23 at 19; Peter Solomon, note 1, supra at 343; Glanville Williams, note 12, post at 17; David Roberts, note 14, post at 543.

12 Ibid., Report 23 at 19.

13 Glanville Williams, "The Authentication of Statements to the Police", [1979] Crim. L.R. 6 at 22; "Report of the Investigation of Allegations Made Against Some Members of the Metropolitan Toronto Police Hold-Up Squad", (1984) Office of the Public Complaints Commissioner at 109.

14 Editorial, [1985] Crim. L.R. 693; Editorial, 135 New Law Journal 877.

15 Carole Willis, "The Tape-Recording of Police Interviews with Suspects: An Interim Report", Home Office Research Study 82, at 26 and 32; David Roberts, "Tape Recording the Questioning of Suspects - The Field Trial Guidelines", [1984] Crim. L.R. 539 at 543.

16 This possibility was suggested to the author by Halton Police Chief James Harding.

17 Report of the Office of the Public Complaints Commissioner, note 12, supra at 109; Carole Willis, note 14, supra at 32; Glanville Williams, note 12, supra at 21; McConville and Morel, "Recording the Interrogation", [1983] Crim. L.R. 158; Editorial, [1985] Crim. L.R. 693.

18 Supra, note 1, Working Paper 32 at 59 and 61; Report 23 at 19; Carole Willis, note 14, supra at 30.

19 Ibid., Working Paper 32 at 60; Report 23 at 19; Marquita Inman, note 4, supra at 480; Glanville Williams, note 12, supra at 15 and 17.

20 Ibid., Report 23 at 19; Report of the Office of the Public Complaints Commissioner, note 12, supra at 106; Glanville Williams, note 12, supra at 10.

21 Marquita Inman, note 4, supra at 480; Report of the Office of the Public Complaints Commissioner, note 12, supra at 106; Peter Solomon, note 1, supra at 342.

22 Chief A.H. McCart, Haldimand-Norfolk Regional Police, unpublished manuscript entitled "Take a Look at the Audio-Visual System" (February, 1984) at 34.

23 Glanville Williams, note 12, supra at 16. This would be seen as a disadvantage by police forces not using taping procedures but it would, no doubt, be viewed as an advantage by accused persons and their counsel.

24 An experienced detective in the Halton Regional Police Force mentioned this concern to the author during informal discussions prior to the start of the current project.

SEPTIEME PARTIE

PART VII

IMPACTS SOCIAUX

SOCIAL IMPACTS

The Maximum Security Society*

Gary T. Marx

Massachusetts Institute of Technology

Cambridge, Ma. 02139, U.S.A.

I do not believe that the kind of society I describe necessarily will arrive, but I believe.... that something resembling it could arrive.

George Orwell

These are the days of miracle and wonder
This is the long distance call
The way the camera follows us in slo-mo
These are the days of lasers in the jungle
Lasers in the jungle somewhere
Stacato signals of constant information
These are the days of miracle and wonder

Paul Simon, The Boy in the Bubble

The death of democracy is not likely to be assassination from ambush. It will be a slow extinction from apathy, indifference and undernourishment.

Robert Maynard Hutchins

Buck Rogers and Dick Tracy have come to the criminal justice system. At a recent University of Montreal conference on technology and criminal justice, information was presented on a broad array of defence and space age technologies that are now available for domestic application. Entrepreneurs --whether economic, political or academic justify these by reference to shared values --justice, equity, crime prevention, deterrence, the reduction of fear, and greater efficiency and effectivness. Yet with roses there are always thorns. In these observations I raise some critical questions about current developments in the technology of social control. I draw upon my recent work on undercover police, computer matching and profiling and work monitoring. [1]

I write as both social scientist and social critic. As the former I identify and label trends in the society. As the latter I predict what the future could be like if current trends continue. After the American journalist Lincoln Steffens visited the Soviet Union in 1919 he remarked "I have seen the future and it works." In what ways is that prophecy likely to be true for technology and criminal justice? While I do not know enough about the future to be absolutely pessimistic, I certainly do not share Steffens' optimism, particularly with respect to questions of individual privacy and liberty.

As we incrementally adopt benignly presented technical changes --whether involving electronic beepers, biometric identification, computer data bases, video surveillance, pharmacology, or robot guards, where are we as a society headed? What kind of a world will we see in the years 2000 and 2050? With respect to liberty, privacy and the dignity and autonomy of the individual, is it one we will gladly pass on to our children and grandchildren? [2]

In the U.S. we are celebrating the 200th anniversary of the Constitution, a document that extended liberty. Unfortunately, the bi-centeniary of another important document that restricted liberty has been virtually unnoticed --the publication of Jeremey Bentham's Panopticon or the Inspection House.

I think the image that Bentham developed almost 200 years ago is of great contemporary significance. In the book Bentham offered a plan for the perfect prison. There was to be constant inspection of both prisoners and keepers; cells were to be constructed with bars (rather than opaque doors) around a central inspection tower. His ideas helped give rise to the maximum security prison, which today is characterized by perimeter security, thick walls with guard towers, spotlights, and a very high degree of electronic surveillance.

Individuals are classified and categorized on the basis of extensive general tests and measures of a predictive nature. Dossiers play a prominent role. Collusive relations between prisoners and guards and informing are central features. Control is embedded in the physical environment (e.g. by buidling furniture into walls) or physiological environment (e.g. tranquillizers). Prisoners may

move from area to area only when accompanied by a guard or with a pass. There are frequent checkpoints. Video surveillance is omnipresent. Prisoners may be under surveillance even while showering or using toilets. There are frequent "head counts" and highly intrusive involuntary searches can occur at will.

The stark situation of the maximum security prison can help us understand the broader society. Many of the kinds of controls found in prison and in the criminal justice system more broadly are diffusing into the society at large. Techniques and an ethos once applied only to suspects or prisoners are now applied in the most benign settings. It is important to ask if recent developments in technology, culture and social organization are not pushing us towards becoming a maximum security society.

As the prison ethos diffuses ever more into the society at large, the need for actual prisons may decline. Society becomes the functional alternative to the prison. This of course is what the community corrections reform movement has long sought. Yet it did not envision that the broad population would in a sense become the prisoners, not just those who have been found guilty through a process of adjudication.

The trend in North America and perhaps in other industrial democracies is toward, rather than away from a maximum security society. What Erikson and Shearing (1986) refer to as the "scientification of police work" offers not only new ways of doing things, but a new means of legitimizing police power. It is both instrument and ideology. We face a major intellectual challenge in understanding how, and to what extent, traditional

democratic societies may now be vulnerable to the destruction of liberty through ostensibly non-violent technical means.

Here I do not consider traditional police states, whether of the right or the left, since to find a parrallel there is hardly news. In addition their repressive systems have historically been maintained by low, rather than high-tech means, though this of course is changing.

In the maximum security society, the line between the public and the private is obliterated; we are under constant observation, everything goes on a permanent record, and much of what we say, do and even feel may be known and recorded by others we do not know--whether we will this or not, and even whether we know about it or not. Data from widely separated geographical areas, organizations, and time periods can easily be merged and analyzed. Control is embedded and preventive, and informers, dossiers, and classification are prominent.

Surveillance is both laser-like and absorbent. There is an expansion and joining of intensive forms of monitoring traditionally used only in the investigation and surveillance of criminal and espionage suspects, or prisoners, with the more shallow forms of categorical monitoring directed at broad populations.

Elements of the self are subtly redefined into commercial objects to be involuntarily parcelled out to experts. [3] The individual has less control over and knowledge about, his or her own person and must assume a more passive role in the face of specialists who work the levers of the machine. [4] Through an abstract, distant, depersonalized, automatic, bureaucratic and

largely invisible and incomprehensible process, the machine generates information and may, as well, engender action. [5]

The technology becomes ever more penetrating, intrusive and precise. [6] If we think about the information gathering net as being parrallel to a fishing net, then as Stan Cohen (1985) has observed, the mesh of the net has not only become finer, it has become wider. The state's traditional monopoly over the means of violence is supplemented by a new monopoly over the means of gathering and analyzing information --this may even make the former obsolete.

Control is better symbolized by manipulation than coercion, by computer chips than prison bars and by remote and invisible tethers than by handcuffs or straight-jackets. We see the paradoxical combining of decentralized and centralized forms. As Foucault (1977) observes control is not excerized from afar, as with monarchiacal power, but is expressed directly from within the social relations and settings to be controlled. Like a pace-maker, it is implanted within the very context to be managed.

The "Maximum security society" is composed of six interrelated sub-socieites:

1) an engineered society
2) a dossier society
3) an actuarial or predictive society
4) a porous society
5) a self-monitored society
6) a suspicious society

Let me briefly consider these six major components.

In the engineered society, choices are limited and determined by the physical and social environment. The goal is to design problems out of existence. This is done through either target hardening or suspect weakening (or their elimination altogether). Why bother with the messyness and cost of locating violations and violators when you can prevent them? [7] The criminal justice system is perceived as an anachronism whose agents serve only to shoot the wounded after the battle is over.

Among the clearest cases are those involving the body --psycho surgergy for the violent, literal or chemical castrastion for sex offenders, cutting off the hands of pickpockets, the morphine derrivative trexan for heroin users or antbuse for alchoholics, [8] tranquillizers for the mentally ill and Depo-Provera in institutions to change hormone levels. Improved locks and vaults, or developments in bank architecture --bank buildings without first floor windows and what are called "bandit barriers", the bullet resistant glass or plexi-glass which prevents thieves from vaulting the counter are other obvious examples. A more radical step aims to eliminate robbery by eliminating cash --the move toward cashless retail transactions (by credit or the emerging "debit" cards).

The governors available for trucks and buses which limit speed and the anti-theft interlock system for automobiles are other examples. An anti-drunk driving interlock device is available (involving a breath analyzer attached to the ignition system). [9] Telephone call blocking, a rapidly spreading technique, makes it possibe to restrict the types of calls made by certain telephones or callers (e.g. the switch may be

programmed to block long distance calls or freequently called numbers such as the weather, the time or dial-a-joke).

Where it is not possible to actually physically prevent the violation or that is too expensive, the system may be engineered so that enjoyment of the fruits of the crime are prevented, its occurence is documented, and the violator is trapped or at least identified. The exploding red dye packs that stain the money taken in bank robberies, the "safety seals" on food jars that pop up once opened, a floor super-glue that can literally glues unauthorized entrants in place, and various bio-metric access identification devices based on voice, fingerprint, photo, retinal patterns, DNA, signature or typing rhythms are examples.

Many basic facts about the dossier society are well known. Computerized records and what Kenneth Laudon (1986) refers to as our "data image" are central to the workings of the society. Sweden with its universal identifyer and more than 100 government data bases for each adult may offer the prototype of the dossier society.

Credit card companies, airlines, hotels and car rental agencies record what we spend, where we went and how long we stayed. Health records are increasingly computerized: more than nine out of ten working Americans have individual or group health insurance policies. Even pharmacies have begun to keep computerized records on patient's drug use and health characteristics. Individual financial transactions increasingly involve electronic tellers and electronic check and credit card authorization. Electronic Funds Transfer has become central to

banking. Cashless transactions (electronic funds transfer at point of sale) are an increasing percentage of all sales. The size and reach of criminal justice data bases such as the FBI's National Criminal Justice Information Center continues to grow. [10]

Beyond the increased amount of information available, the nature of the surveillance is qualitatively altered with computers. While bureaucrats checked records before the advent of computers, this tended to be for errors, internal consistency, and missing information. Cross checking vast data bases was simply not practical. But with computerization surveillance is routinized, broadend and deepened. Bits of scattered information that in the past did not threaten the individual's privacy and anonymity can now be joined. Organizational memories are extended over time and across space. Observations have a more textured dimensional quality. Rather than focusing on the discrete individual at one point in time and on static demographic data such as date of birth, surveillance increasingly involves more complex transactional analysis, interrelating persons and events (for instance the timing of phone calls, travel, bank deposits).

A thriving new computer-based, data-scavenging industry now sells information gleaned from sources such as drivers' licences, vehicle- and voter registration lists, birth, marriage and death certificates, land deeds, telephone and organizational directories, and census-tract records. Matching and profiling wherein information from various sources are combined are increasingly common (Marx and Reichman, 1984).

It becomes impossible to escape from one's past and there is the danger of permanent stigmatization. Solzhenitsyn observes:

> As every man goes through life, he fills in a number of forms for the record, each containing a number of questions....there are thus hundreds of little threads radiating from every man, millions of threads in all....They are not visible, they are not material, but every man is constantly aware of their existence...Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the records.

Very much related to the computer is the actuarial or predictive society in which decisions are made about you not as a unique individual or on the basis of your current behavior, but as a member of a statistical category with a given probability of behaving a certain way in the future.

The expanding fields of artificial intelligence and expert systems are central to this. In criminal justice in the last decade computer aided risk and related forms of prediction have become widespread. There are elaborate systems for classifying inmates and for making parole and probation decisions. But the use of predictive profiles for letting people into, or out of systems (and for how they are treated if in a system) extends to an increasing number of areas including--bank loans, consumer credit, insurance, employment, medical treatment, college admissions and whose luggage is likely to get searched at the airport, or car stopped on the highway.

In the self-monitored society, those watched become active partners in their own monitoring, although not always voluntarily or with fore-knowledge. This is the ultimate in decentralized social control. It is conistent with a trend involving the

generalization of control. (Shearing, NR) The security function becomes a general expectation of all roles (whether we are watching others or ourselves) and not just of those formally designated as control agents.

Monitoring is often self-activated and automatic. To an unprecedented degree we have become co-conspirators in our own surveillance --whether as a condition of work, traveling by air, receving a government benefit, going to a shopping mall, making consumer purchases or using the telephone. We seem increasingly willing and even eager to offer personal information and to submit to self-scrutiny because of the benefits thought to result. [11]

Survelliance systems may be directly triggered when a person walks, talks on the telephone, turns on a TV set, takes a magnetically marked item (whether library book or consumer good) through a checkpoint, and enters or leaves certain controlled areas. Voice and language recognition systems that record, or send a message, when certain words or sounds appear, electronic beepers, station message detail recording on telephone systems, video surveillance, card control access cards, and computer monitoring are further examples, as is drug testing. The spectacle of the President of the United States and his cabinet officers voluntarily providing urine samples to prove they are drug free must surely be one of the decade's more bizzare and surreal examples of participatory monitoring. [12] There is also the case of the politician who challenged his opponent in an election to take a urine test to prove he did not use drugs. There are a variety of at home monitoring kits available as well.

Wallet size "Smart cards" are being tested which can contain up to 800 pages of information.

Hotlines are increasingly available for reporting a vast array of problematic behaviors (drugs, suicide, depression, crime) whether about one's self or others. With telephones now available in backyards, bathrooms, cars, and call-forwarding and message recording, it becomes ever easier.

Mention can also be made of the intermediate form of subliminal communcation. At the extreme of science fiction we have the Manchurian Candidate, but more realistically we have music in department stores which contains buried messages saying "don't steal" "honesty pays", we have computer programs for video-terminal display operators which can flash messages such as "my world is peaceful". But for all their recipients know, they might also flash "if you love them, buy an expensive gift", "work faster" or "vote yes". We are at the dawn of subtle self-programing.

A related form of self-policing involves mass communication. Rather than the greater expense and impracticality of having the state watch everyone all the time, it is far more efficient to have all eyes riveted on a common mass media stimulus which offers direct and indirect messages on how to behave and morality tales about what happens to those who stray. [13]

In the <u>porous society</u> not only our actions, but our feelings and thoughts are made visible. In the porous society information leakage is rampant. Barriers and boundaries --be they distance, darkness, time, walls, windows and even skin, which

have been fundamental to our conceptions of privacy, liberty and individuality give way. [14]

Surveillance can be carried out inexpensively and often remotely and with low visiblity. It becomes increasingly intensive, extensive and categorical. Like the discovery of the atom or the unconscious, new control techniques surface bits of reality that were previously hidden, or didn't contain informational clues. People are in a sense turned inside out, and what was previously invisbile or meaningless is made visible and meaningful. This may involve space age detection devices that give meaning to physical emanations based on the analysis of heat, light, pressure, motion, odor, chemicals or physiologial process, as well as the new meaning given to visible individual characteristics and behavior when they are judged relative to a predictive profile based on aggregate data.

When the pan-opticon is combined with the pan-auditron, the pan-sensitron, and a vast array of other panoramic devices, we have a very comprehensive record. Consider for example the multiple indicators found in the security systems of many 24 hour retail convenience stores. So called "integrated management security systems" are now available that offer visual, audio, and digital information about the behavior of employees and customers. [15] Participants in Behavior Scan, a marketing research endeavor, automatically have their television viewing correlated with records of their consumer purchases. There are efforts to combine the electronic beepers used in house arrest with the breathanalyzer and video systems.

Like workers or parts used in mass production, surveillance

data --whether in the form of computer records, video and audio tapes, or various bio-metric "signatures" are increasingly standardized and combinable. The information can be converted into digital form which makes it portable, and easily reproduceable and transferable.

The transparent society is nicely illustrated by the recent hit song "Every Breath You Take" sung by a celebrated rock group known as the Police. It is a love rather than a protest song, yet it nicely captures elements of the new surveillance. It contains these lines:

every breath you take [breath analyzer]
every move you make [motion detector
every bond you break [polygraph]
every step you take [electronic anklet]
every single day [continuous monitoring]
every word you say [bugs, wiretaps, mikes]
every night you stay [light amplifier]
every vow you break [voice stress analysis]
every smile you fake [brain wave analysis]
every claim you make [computer matching]
I'll be watching you

If this song were written a few years later the author might have added "every bathroom trip you take", "every blink you make", "every blood test you give", and "every haircut you get" to accomodate forms of drug testing based on urinalysis, hair analysis and brainwaves. [16]

The essence of the suspicious society is captured by an exchange in the novel Gorky Park. The police

inspector asks a central character who she suspects of having stolen her iceskates. She replies "everyone". To which the inspector responds "so do I." In the technical implementation of Kafka's nightmare, modern society too, increasingly suspects everyone and all the time. The camera, the tape recorder, the identity card, the metal detector, the obligatory tax form which must be filled out even if one has no income, and, of course, the computer, make all who come within their province reasonable targets for surveillance. The new, softer forms of control are helping to create a society where people are permanently under suspicion and surveillance. To paraphrase a famous observation "suspicion, like the rain, falls on the innocent as well as the guilty". The Napoleonic assumption that everyone is guilty until proven innocent -- increasinlgy extends beyond criminal justice and the French influenced countries.

Categorical suspicion is facilitated by inexpensive technologies which permit continuous and comprehensive monitoring and the skeptical view of science. One can disprove an empirical assertion, but never fully prove it. In a classic line from a Woody Allen film about the Joseph McCarthy era in the United States, an investigator says about a character "there is no evidence that he is a communist, on the other hand there is no evidence that he is not". What is true today may not be true tomorrow. Thus a polygraph, drug or AIDS test may be valid at the time it is administered, but that offers no proof that it will be valid two months later.

A theme running through all of the above is the prevention

of violations. This is aided by technologies which transcend the barriers that traditionally required police to wait until a violation occured before responding and by predictive technologies. [17] Rather than simply reacting to what is served up around us, anticipatory strategies seek to reduce risk and uncertainty. Bureaucratic organization and modern management, consistent with the idea of rationality, attempt to make control more predictable, reliable and effective. As little is left to chance as possible. Control is extended to ever more features of the environment. The openly antagonistic model of social control, where authorities are clearly identified by uniforms and coercive action, is supplemented by a more vieled and manipulative model.

The Good News and the Bad News

In suggesting a parrallel between the maximum security prison and contemporary society I am of course speaking metaphorically. [18] The former is an ideal type against which we can consider how close, or far away, a given society or practice is. Some societies are closer to it than others and institutions vary enormously in their ability to create such conditions.

It is of course a leap from contemporary society to the iron cage of a totalitarian future. I certainly don't wish to rain on anyone's parade. Yet it is important to see the broader picture and to view changes in criminal justice as the cutting edge of a broader set of changes that may well alter our basic institutions and values.

I am not suggesting that the news is all bad, nor am I willing to conceed to Brecht that "the person who smiles

is the one who has not yet heard the bad news". The topic is fascinating because its implications are so contradictory and values are in conflict.

Social engineering may prevent victimization and one need not spend resources on after-the-fact social control agents. It may channel the behavior of social control agents, as well as those they watch. It can increase accountability among both groups by offering a documentary record and the identification of actors. Yet the freedom to innovate in positive, as well as negative ways is lessened. The society may become less humane and more mechanical. It is no longer necessary to socialize people into the legitimacy of conformity. One need not ask about the roots of the motivation to deviate, or what it is about the organization of society that may produce it. A social system based primarily on conformity induced by external technical means is likley to be highly unstable.

The dossier society can extend organizational memories in positive ways --identifying stores where tainted canned goods were sent, reducing fraud in government benefit programs, keeping irresponsible drivers off the road, keeping embezzlers and child molesters from employment in banks and day-care centers and more finely tuning services to needs. Yet it also means one's past can never be escaped, even once a debt to society has been paid. Because of concern of what it may look like on the record, persons may not seek psychiatric help when it is needed, they may fail to protest unsatisfactory housing or employment conditions for fear of landing in a data bank, and risk taking and

innovation may be lessened. The subjective sense of being watched may increase and feelings of liberty decline.

Actuarial decision-making certainly offers a higher probability of correct decisions across many cases. Playing the odds is a basic societal strategy. It may eliminate gross discrimination based on overtly racist or sexist factors. But when issues of justice, health or employment are involved, the costs for the statistically atypical individual can be great. Decision-making on the basis of group criteria can conflict with our notions of due process and fairness, and the right to be judged as an individual. What is rational in the aggregate may be unfair, and/or wrong in any given case. Instead of responding to the whole person and relying on the judgement of a human, decisions may automatically be made on the base of impersonal and disembodied data images, using "expert systems".

The porous society rests on a fundamentally democratic principle of visibility --to hold individuals or organizations accountable we need openness and documentation. Secrecy can breed and protect dastardly deeds and errors. The French notion of "transparency" with respect to informtion in personal data bases and the Freedom of Information Act in the United States reflect awareness of this, as do "paper trails" [19] and a variety of surveillance devices used to control the controllers. [fn 100] But the techniques of contemporary surveillance can also be highly intrusive and destructive of privacy, liberty and dignity.

Self-monitoring can be seen as the highest form of social control since it is voluntary. Its decentralized nature is also likely to be the least expensive. Yet if one does not find the

society to be just, it can also be seen as the ultimate degradation --as individuals are manipulated into digging their own graves. The compulsion underlying the system is masked and false consciousness is created.

Observers of the fragility of democratic society have long noted the importance of vigilance and a healthy distrust of rulers. To not take the world at first appearances and skepticism are important ingredients of wisdom and scientific advancement. Yet taken too far, suspiciousness is destructive of community and the trust that is central to meangingful human relations.

A remark made by the manager of former heavyweight boxing champion Sonny Liston: "he has lots of good qualities. It's his bad qualities that ain't so good" applies here. Its the same for the new technologies, "it's their bad qualities that ain't so good." The fact that there is a positive side hardly warrants unbridled optimism. Short run advantages are usually much more apparent than long run costs. In addition, the economic and ideological forces advocating technical changes are in general much more powerful than those arguing for caution and restraint. [20]

We are at the dawn (or judged from another perspective perhaps the sunset) of a new age of techno-control. The technology is not about to go away. Yet we need to keep our eye on the ball park, as well as the ball, and to realize that what causes the individual tree to thrive may eventually cause the forest to decay. We must be as aware of the dangers as we are of

the advantages and maintain an appropriate balance between means and ends. Our ability to do this is increased through critical analysis of the assumptions surrounding the technology.

Techno-Fallacies

The discussion above has sought to offer a broad framework for approaching these changes. It is a sensitizing, macro perspective. I now turn to some more specific observations that may help guide policy in particular contexts.

The move toward a maximum security society is accompanied by a number of empirical and value assumptions which I think are techno-fallacies. Before technical innovations are blithely adopted, it is important to examine the empirical, as well as the value assumptions on which they are based. Consider the following:

1) The fallacy of the free lunch or painless dentistry. This involves the belief that there are cost free solutions. Any expenditure of scarce resources involves foregone opportunity costs. Any format or structure both channels and excludes. A good computer profile for example may increase arrests among the less competant, but make it easier for skilled offenders, knowledgable about the system, to avoid detection.

2) The illusion of the free lunch is aided by the fallacy of quantification (which involves defining costs and benefits only in terms of things that can be easily measured). This often comes down to money. In the United States it is greatly aided by the dominant role in public policy played by economists, rather than by philosophers or "soft" social scientists. A good illustration is to base one's position on capital punishment on whether or not it costs more to execute someone than it does to keep them alive. A recent study in the United States found the former to be true.

3) The fallacy of the short run involves a focus only on the immediate time period. We are aware of this in the case of the exploitation of the natural environment, but it equally holds for social practices. It is particularly likely in pragmatic socieites with electorial politics that stress individual social mobility.

4.The fallacy of re-arranging the deck chairs on the Titanic instead of looking for icebergs. This may involve a focus on the wrong problem, or erroneous causal analysis. It can mean exclusive emphasis on symptoms rather than a search for causes. Technical fixes (e.g. improvements in security hardware and psychological adjustment approaches) often offer only stop-gap measures. They must be supplmemented by attention to deeper causes and bigger pictures.

5) the fallacy that the means will never determine the end. To a person with a hammer the whole world looks like a nail. The fact that something can be done often generates pressure to do it, without adequate consideration of unintended and undesireable consequences. In the words of a Deputy Superintendent of the New York State Police, "if the technology is available, why not use it?" [21] President Truman is reputed to have said something similar regarding the atomic bomb. Some police departments have found that computers can greatly aide in the collection of revenue from parking and traffic violations. This is relatively clean work and it creates impressive success statistics. What then can happen is an expansion in the enforcement of traffic regulations at the expense of more traditional police goals. Problems must drive the search for solutions, not the reverse.

6) The fallacy of containment or non-escalation (or the fallacy that technology will always remain the solution rather than become the problem). Contrary to the lesson of Dr. Frankenstein, this involves the belief that we can control the technology, rather than the reverse. When they are first being sold to the public, powerful and potentially threatening means are put forth for use in very limited conditions, or only for the most serious offences. But as a police supervisor put it "tactics developed for use against killers and kidnappers come to be used against junkies and whores." Tactics applied first to animals may next be applied to prisoners, then to persons dependent on state welfare and children, and finally to the general population. Unfortunately in the United States we can witness "surveillance creep" with respect to the use of the social security card number as a personal identifier, the polygraph, drug tests, and computer matches.

7) The fallacy that greater expenditures and more powerful technology will continuously yield benefits in a linear fashion. Or, in the words of a children's poster that shows a boat filled with hippopotomuses sinking when an additional passenger is added, "more is not always better". Contrary to our enlightenment tradition this can be the case regarding information. (Michael 1984) It is possible to suffer from "information overkill" and, as with any medication, there may be threshold effects. [22]

8) The fallacy of permanent victory. The idea of a war on crime in which there is a final victory ignores the role of human inventiveness in a free market economy with civil liberties protections. There is no solution which one smart group of people can create which another equally smart group can not find a way

around --if not through technical means, then through tradtional means of corrupting or compromising social control agents. This also involves the trade-offs any solution involves. There are parrallel dialectics as new forms of control and deviance generate new efforts of neutralization --by either controllers or violators. In the case of the latter, the anti-theft steering wheel inter-lock system rapidly gave way to an evasive tool and ways of beating the polygraph and drug test have become public knowledge.

9) The fallacy of the 100% accurate or fail-safe system. This involves the belief that machines don't make mistakes, or can't be fooled. [23] This involves issues of reliability and validity. As we know, the polygraph, voice print and drug testing are far from perfect. And apart from any self-conscious effort to thwart, a technology, what is highly effective in a controlled laboratory may fail in the messyness of the real world. Thus the transmission from electronic beepers can be blocked by water in a bathtub or waterbed, the metal in mylar wallpaper and trailers, not to mention problems from the failure of electrical power and telephone systems.

10) The fallacy of a passive, non-reactive environment. This is relevant to the consideration of unintended consequences. Innovations must be viewd as new variables in dynamic situations. There is a Social Heisenburg principle which over time lessens the effectiveness of many solutions. New controls create new challenges and new opportunities for violations.

11) The fallacy of technical neutrality. Misplaced notions about the neutrality of a technique can mask political, social and ethical aspects. George Orwell's response to the assertion that technology was neutral: "so is the jungle" is applicable. The technology is developed and applied in a social context which is neither neutral nor equal. In some cases, to reverse Sartre, this might also be seen as "the illusion of clean hands". Just because there is a distancing between the action delivered by some automatic process and the agent, this does not mean that moral responsibility has been eliminated. It has merely been masked and diffused. We have all encountered frustrating situations where petty bureaucrats respond "but the computer says", oblivious to the role of human agents in setting rules and collecting and entering data into the computer. This mechanical distancing and obfuscation may make it easier to take inhumane actions and it complicates efforts at controlling the controllers.

12) The fallacy of delegating decision making authority to the machine without human review of the action recommended. Computer programs are "acontextual" and for many purposes can not deal with reality's richness the way a human can. This is particulary the case for atypical, or extenuating circumstances. In computer jargon there must be some "human interface in the loop". The most obvious example is the science fiction (?) image of a war automatically generated in response to faulty data from electronic sensors.

13) The fallacy of believing that because it is possible to successfully skate on thin ice, that it is acceptable to do so. This involves issues of acceptable risk. It is not enough to show that a tactic can be effective without disastrous consequences. We must ask about the probability and cost of catastrophic failures.

14) The fallacy of assuming that if a critic questions the means he or she must also be against the end. The reverse is the comforting fallacy that if your intentions are good your results will be good, or if not, your failings are excusable. The former is a classic smear tactic which implies that those who oppose unregulated, highly intrusive means somehow favor the drug abuse, subversion or theft which the tactics may be directed against. As both a strategic and humane matter, critics should acknowledge the often deeply felt moral concerns that can motivate surveillance crusaders. It is sometimes possible to suggest alternative means. If not, one must point out that there are times when the cure is worse than the disease.

15) The fallacy of assuming that only the guilty have to fear the development of intrusive technology (or if you've done nothing wrong you have nothing to hide). This ignores a fundamental principle of western society --means as well as ends have a moral component. A society which can not draw a moral distinction between crime and criminal justice is in deep trouble.

Of Guillotines and Criminologists

Thomas Edison expressed the hope that "what the hand of man creates, the head of man can control". Yet even if the above fallacies are rejected, it is important to see that the changes considered here do not stand alone. They occur incrementally and for ostensibly benign reasons. Considered in isolation and for narrow purposes they may be socially desirable, but when seen in totality over a period of decades they suggest a very different kind of society. Their cummulative impact must be noted.

If totalitarianism ever comes to the Western industrial democracies, it is more likely to come by accretion than by cataclysmic event. As Sinclair Lewis argued in his novel, It Can't Happen Here, it would come in traditional guise, with the gradual erosion of liberties. Voluntary participation, beneficent

rationales, and changes in cultural definition and language will hide its negative aspects. It is said that if you drop a frog into very hot water it will immediately jump out, but what happens if you drop it into cold water and slowly turn up the heat?

In a great many areas of domestic affairs we are of course far from the society George Orwell described. [24] Yet to judge the state of freedom and liberty only by traditional standards results in a vision which is too narrow and an optimism which may be unwarranted.

Drawing on recent European experience Orwell's state had both violent and non-violent forms of social control ("a boot stamping on a human face" and Big Brother watching). In linking these Orwell offered only one of several models of totalitarian control. In contemporary society, violent and non-violent forms of social control have become uncoupled and the latter is in the ascendance.

Over the last four decades subtle, seemingly less coercive forms of control have emerged. Their existence within societies which have not become less democratic, and in which the state makes less use of domestic violence, can blind us to their ominous potential. Threats to privacy and liberty need not be associated only with the the use of force, nor with the state. They may appear in the service of benign, as well as totalitarian ends. Huxley with his seemingly benign technocracy is likely a better guide to the future than Orwell.

The absence of physical oppression is a necessary, but not a

sufficent condition for liberty. The existence of new softer forms of control within democratic states certainly does not call for a lessening of vigilance. While we are far from being a maximum security society, we are moving toward --rather than away from this.

What Orwell did not anticipate or develop was the possibility that one could have a society where significant inroads were made on privacy, liberty, and autonomy, even in a relatively nonviolent environment with democratic forms and the presumed bulwarks against totalitarianism in place.

The first task of a society which would have liberty and privacy is to guard against the misuse of physical coercion on the part of the state and private parties. The second task is to guard against the softer forms of secret and manipulative control. Because these are often subtle, indirect, invisible, diffuse and deceptive and shrouded in benign justifications, this is clearly the more difficult task.

There is an apocryphal story about three criminologists who are about to be guilloteened. The first is led to the block, the rope is cut, yet the blade fails to fall. This is viewed as a sign from God and the prisoner is set free. The second criminologist is led to the block and the same thing happens. While the third is being led to the block he looks up and says "Wait a minute I think I can fix that." I hope in our noble efforts to use technology to fix the criminal justice system that none of us will be parties to self or social destruction.

G.T. Marx
M.I.T.
Cambridge, Ma. 02139

References

1. Some of themes developed in this paper are treated at greater length in Undercover Police: Paradoxes and Problems of a Necessary Evil. Berkeley, Cal.: Univ. of California Press, forthcoming, especially chapter 10; "Monitoring on the Job", Technology Review, (with S. Sherizen) Nov./Dec. 1986; "The Interdependence of Private and Public Police as Illustrated by Undercover Investigations" in Crime and Justice System Annuals, 1987; "Routinizing the Discovery of Secrets: Computers as Informants," (with N. Reichman) 1984, American Behavioral Scientist, March, 1986; Fragmentation and Cohesion in American Society. 1984 Washington D.C.: Trend Analysis Program, American Council on Life Insurance.

2. A sign my son saw in a nature reserve in New Zealand applies to much more than ecology and conservation: "True conservationists are people who know that the world is not given to them by their parents but borrowed from their children."

3. Jean Paul Brodeur (1984) observes "the self has become objectified and the inner person has been evicted by information technology."

4. See for example Egon Bittner's (1983) discussion of the role of technique in contemporary society.

5. Such action can be immediate as when a "hit" on a computer match automatically results in the cancellation of government benefits and the generation of a word-processed letter notifying the "guilty" party about this, or when an Automatic Teller Machine refuses to return a card if a faulty password is entered several times, or at may be advisory as with the results of expert systems for parole or the issuing of credit.

6. Consider for example the change in identifying blood specimens. Previously it was only possible to exclude a suspect by showing that blood types did not match, now with DNA analysis positive identification is possible. This may reduce the chance of erroneous convictions and increase convictions of the guilty, but it may also lead to broad population screens.

7. The idea of prevention via engineering the physical environment has a long history (e.g. the history of locks or indelible marks on property or persons). What is new is the scale of the undertaking, the resources available for it and its priority as a formal goal. There is also increased (if not equivalent) attention given to using these means to guard the guards.

For a nice contemporary example of the application of soft and hard social engineering to Disney World in Florida see Shearing and Stenning ( ).

8. The former prevents getting high and the latter causes vomitting or gagging when alcohol is consumed. These may be a condition of probation.

9. Efforts to get around this include saving "clean air" in a balloon, starting the car before drinking, or having a non-drunk companion start the car.

10. In the United States, a Federal Advisory Committee has endorsed a major expansion of this system that would permit federal, state, and local law enforcement agencies to exchange information on "suspicious persons" who have not been formally charged or tried. A simple name check would reveal if other agencies had made inquiries about the person. A proposal to link the National Crime Information Center with private sector data files was however rejected (this time).

11. Of course some compliance is voluntary in only the most superficial sense, whatever authorities may label it in the quest for legitimacy. The line between coercion and volunteerism seems increasingly blurred. Advertizing may play a role in convincing people they need things which are harmful or destructive. Some cooperation with requests for data, or to undergo a lie detector or other tests, are "voluntary" only at the risk of not obtaining a needed benefit or a job. For example an IBM spokesman reports with respect to a policy of testing job applicants for drugs, "it's any applicant's decision to make --they're not forced to take the test...but it is required if an applicant wishes to be considered for employment." Denver Post, Feb. 7, 1985. Signs in U.S. governemnt buildings which state those entering agree to the search of their packages and bags are similar. The signs may be present for legal reasons, but their logic leaves much to be desired since those subject to the search need to enter the building.

An interesting history could be written about the rise of compulsory governmental reporting requirements, tax and military draft laws would be good places to begin.

12. This is not the kind of "leak" those in government have traditionally provided.

13. Rule (1983) notes that both mass communications and mass surveillance are part of a broader mobilization of the population, wherein the direct ties between central institutions and citizens are intensified.

14. The techniques used for this constitute "the new surveillance". This section draws from G. Marx, 1986, "The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures," in J. Short (ed.), The Social Fabric Dimensions and Issues. Beverly Hills, Ca.: Sage Publications.

15. For example information may be recorded from cash register entries, voices, motion, or from persons standing on a mat with a

sensor. Audio and/or visual recordings and alarms may be programmed to respond to a large number of 'triggering devices'.

16. One technique claims to be able to identify drug useage through analysis of a strand of hair and another to determine how much, and what quantity of six kinds of drugs are in a person's system by analyzing eye movements. The radio imuno-assay technique can be used to extract drug residue from a strand of hair. Like rings in a tree, the distance from the root also gives temporal evidence. As one eager advocate put it "the beauty of the technique" is that it can't be diluted or switched, there are many samples and it does not demean the suspect, unlike urine testing.

17. See for example Stinchcombe's (1963) discussion of the role of spatial barriers in maintaining privacy.

18. A similar image is the intensive care unit in a hospital. More generally, in Erving Goffman's (1961) words society is becoming a "total institution." Use of the stretched metaphor can be an important communications device for increasing awareness of potential social problems.

19. Among the latter are vehicle and personnel locator systems ("cowbells for cops"), video and /or audio surveillance of police booking areas, radio and telephone communication, and drug tests and polygraphs for police are further examples.

20. It is interesting that in these matters critical criminologists who are the first to advocate change in other areas, usually adopt a more conservative stance.

21. This was said with respect to the extension of computer surveillance mentioned in fn. 10.

22. In the United States for example, the traditional social supports thought to work against totalitarianism are strong, --an educated citizenry committed to democratic ideals, a variety of independent channels of mass communication, a plethora of voluntary organizations, and Constitutional protections for civil liberties.

23. For example laser and other techniques for picking up latent fingerprints may mean a greater eventual success rate, but also a much greater expenditure of resources and the investigation of many innocent people whose prints will be discovered along with the guilty.

24. The source of the limitations vary. Computer matching may find valid correlations but can be no better than the original data it deals with which may be dated or wrong to begin with. The data it uses is often rather blunt and acontexual. Chemical analyses which may correctly identify drugs in a person's system can not reveal how they got there (thus THC may appear in the bloodstream because a person smoked marijuana or simply because

they were around people who were smoking it). Nor does such analysis determine whether a drug was used on or off the job. There may also be false positives, as a result of the effect of prescription drugs.

There are two distinct issues here. The first involves questions of reliability and validity and a false sense of certainty. The techniques are nowhere near as powerful as their advocates claim. But what if they were? Would that then justify their indiscriminate use? What would a society be like in which it was always possible to tell what a person was thinking, or when they were telling the truth or where they had been and what they were doing?

Bibliographie

Bramford, J. 1983. The Puzzle Palace New York: Penguin Books.

Burnham, D. 1983. The Rise of the Computer State. New York: Random House.

S. Bok, 1982. Secrets on the Ethics of Concealment and Revelation. New York: Pantheon.

Ball, R., Huff, R. and Lilly R. forthcoming, House Arrest and Correctional Policy: Doing Time at Home, Beverly Hills: Sage Publications.

Bittner, E. 1983 "Technique and the Conduct of Life" Social Problems, vol. 30, no. 3, Feb.

Brodeur, J.P. 1983. "High Policing and Low Policing: Remarks About the Policing of Political Activities." Social Problems, Vol. 30, no. 5.

Laudon, K. 1986. Dossier Society Values Choices in the Design of National Information Systems. New York: Columbia Univ. Press.

Cohen, S. 1985. Visions of Social Control. Cambridge: Policy Press.

Foucault, M. 1977. Discipline and Punish. New York: Pantheon.

Goffman, E. 1961. Asylums. Garden City. N.Y.: Doubleday Anchor.

Gross, J. 1984. "Social Control under Totalitarianism" in D. Black (ed.) Toward a General Theory of Social Control, Vol. 2, New York: Academic Press.

Donner , F. 1980. The Age of Surveillance. New York: Knopf.

Dertouzos, M. and Moses, J. The Computer Age.

Howard, R. Brave New Workplace.

Laudon, K. 1986. Dossier Society Values Choices in the Design of National Information Systems. New York: Columbia Univ. Press.

Lykken, D. 1984 "Detecting Deception in 1984", American Behavioral Scientist, March/April.

G. Marx, 1975. "Thoughts on a neglected category of social movement participant: Agents provocateurs and informants." American Journal of Sociology. 80 (2) pp. 402-442.

--------- 1979. "External efforts to dmage or facilitate social movements: Some patterns, explanations, outcomes and

complications." Pp. 94-125 in M. Zald and J. McCarthy (eds.), The Dynamics of Social Movements. Cambridge, Mass.: Winthrop.

--------1984 Fragmentation and Cohesion in American Society. Washington D.C.: Trend Analysis Program, American Council on Life Insurance.

-------and Reichman, N. 1984. "Routinizing the Discovery of Secrets: Computers as Informants," American Behavioral Scientist, March.

-----1986. "The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures," in J. Short (ed.), The Social Fabric Dimensions and Issues. Beverly Hills, Ca.: Sage Publications.

-----1986 with S. Sherizen, "Monitoring on the Job" Technology Review, Nov.

Mathiesen, T. 1983. "The Future of Control Systems" in D. Garland and P. Young, The Power to Punish, Atlantic Highlands, N.J.: Humanities Press.

McCarthy, B.R. 1987. (ed.) Intermediate Punishments: Intensive Supervision, Home Confinement and Electronic Surveillance. Monsey, New York: Criminal Justice Press.

Meyrowitz, J. No Sense of Place

Michael, D. 1984. "Too Much of a Good Thing? Dilemmas of an Information Society" Technological Forecasting and Social Change. Vol. 25, no. 4, July 1984.

O'Toole, G. 1978. The Private Sector: Rent-a-Cops, Private Spies and the Police-Industrial Complex. New York: W.W. Norton.

J. Perrolle Computers and Social Change

Rule, J. McDam, D. Stearns, L. and Uglow, D. 1983. "Documentary Identification and Mass Suvreillance in the United States" Social Problems, 31.

Shaiken, H. Work Transformed.

Shattuck, J. 1984 "In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States," Hastings Law Journal. July. pp. 991-1005.

Shearing C. and Stenning P. "From the Panopticon to Disney World: The Development of Discipline", Perspectives in Criminal Law.

Schudson, M. 1984. Advertising, The Uneasy Persuasion. New York: Basic Books.

Stinchcombe, A. 1963 "Institutions of Privacy in the

Determination of Police Administrative Practice" American Journal of Sociology, 69, 150-160.

An Overview of The Hallcrest Report; A Study of Private Security and Police Resources and Relationships in the United States

by:

William C. CUNNINGHAM
President, Hallcrest Systems, Inc. (McLean, Virginia, USA)

Between 1981-84, our firm, Hallcrest Systems, conducted a national study of relationships between law enforcement and private security under the sponsorship of the National Institute of Justice, U.S. Department of Justice. The primary purpose of the project was to develop strategies and recommendations to more effectively utilize the extensive resources of private security and law enforcement in their respective roles in crime prevention and control. Some of the specific research objectives were to:

- establish the role and contribution of private security to crime control;
- describe the operating relationships between private security and law enforcement;
- profile the growth and changes in the private security field in the past decade; and to
- conduct an economic analysis of the market for private security products and services.

Our work resulted in the 1985 publication called, The Hallcrest Report: Private Security and Police In America.

Today, I want to share with you some of the significant findings, projections, and recommendations. First, let me briefly describe how the study was conducted.

We reviewed substantial amounts of literature and interviewed more than 400 people in law enforcement and in all facets of private security throughout the United States, Canada, and the United Kingdom. Questionnaires were received nationally from 384 law enforcement agencies covering all 50 states, from 686 proprietary or corporate security managers and 545 local contract security firm managers and owners in approximately 150 metropolitain areas throughout the country. These questionnaires

Between 1981-84, our firm, Hallcrest Systems, conducted a national study of relationships between law enforcement and private security under the sponsorship of the National Institute of Justice, U.S. Department of Justice. The primary purpose of the project was to develop strategies and recommendations to more effectively utilize the extensive resources of private security and law enforcement in their respective roles in crime prevention and control. Some of the specific research objectives were to:

- establish the role and contribution of private security to crime control;
- describe the operating relationships between private security and law enforcement;
- profile the growth and changes in the prviate security field in the past decade; and to
- conduct an economic analysis of the market for private security products and services.

Our work resulted in the 1985 publication called, The Hallcrest Report: Private Security and Police In America.

Today, I want to share with you some of the significant findings, projections, and recommendations. First, let me briefly describe how the study was conducted.

We reviewed substantial amounts of literature and interviewed more than 400 people in law enforcement and in all facets of private security throughout the United States, Canada, and the United Kingdom. Questionnaires were received nationally from 384 law enforcement agencies covering all 50 states, from 686 proprietary or corporate security managers and 545 local contract security firm managers and owners in approximately 150 metropolitan areas throughout the country. These questionnaires

contained many common items for comparison of attitudes, opinions and perceptions on roles and operating relationships and problems.

In addition, a survey was later sent to senior executives of 40 major national and regional security companies. A separate survey was also directed to the 37 state agencies which license and regulate some elements of private security.

Hallcrest also did field study in two urban counties--one on the East Coast and the other on the West Coast. Techniques for information collection at these sites included questionnaires, structured interviews and observation of operational police and security personnel.

In the time available this afternoon, it is extremely difficult to summarize more than 3 years of national research involving volumes of data and hundreds of interviews. Some of you have already reviewed the Hallcrest Report. Without bogging things down with a recitation of too many statistics, let me cover the major highlights.

One obvious starting point is how many people are now involved in private security and what has been the growth of the so-called private security industry or sector. Overall, security employment has grown at 12 to 15 percent per year. Using trendline projections and compounded rates of growth, U.S. private security contract expenditures were about 15 billion dollars by 1985. Another 7 to 8 billion dollars was spent for proprietary or corporate security payrolls. So, we are currently spending more than $22 billion annually for private sector security--while the total annual spending for all Federal, State, and local law enforcement is about $15 billion.

We have conservatively estimated total employment in private security at about 1.10 million personnel compared to about half a million sworn law enforcement officers at the local, state, and Federal levels. Using 1970 data, the Rand study, the earliest U.S. study of private security, estimated total private security employment at less than 300,000 persons with revenues of $2.5 billion. Obviously, there has been a tremendous amount of growth in private security.

On the other hand, our national survey data have shown an effective decline in law enforcement personnel in relation to growth rates in population and crime. In our national surveys, the actual number of law enforcement personnel decreased or remained the same in the past five years in 44 percent of all agencies--almost one-third of responding law enforcement agencies reported decreases in personnel. While law enforcement resources remained stable or declined, over one-half of the contract security firms reported increases in annual sales of greater than 15 percent per year.

Let's back up a moment to the Rand Report. Our project duplicated a lot of the Rand survey questions, and we find a very different picture of private security today than 15 years ago. The Rand authors used the term "private police" to describe private sector initiated efforts that are considered supplementary or complementary to law enforcement. Their study placed private security into the role of a "junior partner" in the mutually shared goal of detection and prevention of crime. Our review of current literature and hundreds of surveys and interviews of security practitioners makes it clear that the Rand Report has inaccurately characterized private security as "private police" and has become a source in itself for misperceptions and stereotypes of private security that have

dominated the media and law enforcement and private security relationships over the past decade. The Rand Report has somewhat harshly dealt with private security in a very narrowly prescribed role, by not placing private security in the larger context of asset protection and loss prevention of which crime prevention is merely a component.

We can clearly identify some shared goals: e.g., protection of life and property, deterrence, discovery of crime, crime prevention, noncrime related duties, and recovery of stolen property. Law enforcement and private security are usually distinguished on the basis of the degree of legal authority exercised and for whom they perform their services--public or private interests. Even this distinction is not always clear, since occasionally private security personnel will be given special police powers within the area or premises in which they are employed. Unfortunately, most comparisons of law enforcement and private security tend to keep the focus on overlapping tasks of operational personnel--police officers and security guards. Yet, as a security director for a large national corporation noted: "Industrial security has evolved from the old uniformed watchman posture to an integral part of the overall corporate structure."

Private security, however, involves very comprehensive programs of physical, personnel, and information security to protect the assets of an organization and to reduce losses. We spend a good part of our report highlighting the very positive contributions made by private security to crime prevention and control in businesses and in the community. This is a significant point because the police too often invite comparisons of private security with themselves and it colors their perception of what private security does and how well they do it. Law enforcement

executives and operational personnel have a reasonably accurate perception when ranking the functions performed by private security, but do not always have a good understanding of what some of them imply--computer security, protection of trade secrets, etc. Overall, both law enforcement administrators and patrol officers rate private security poor in most areas of performance.

It sounds like much hasn't changed in fifteen years, doesn't it? But let's put the shoe on the other foot, and examine the contribution of law enforcement. Only this time let's not define it in terms of crime prevention and control. Let's look at the total protection resources of the community. With the exception of burglaries and robberies, law enforcement seldom investigates and has low response priorities for most of the crime confronting business and private security. Many of the cases investigated by the police, e.g., shoplifting, check and credit card fraud, are fairly well developed when they are reported or handed over to the police. Yet law enforcement often seems to operate from the assumption that if public resources were more plentiful, there would be little or no need for private security--denying the vast amount of private assets and interests in the community that would otherwise go unprotected.

A prominent police and security educator summarized the law enforcement position very well in an interview when he said:

> If one were to make a big pie of the protection of the wealth, health and welfare of a community, organized law enforcement would be a small part of the pie. Law Enforcement which is basically manpower is now seeing a manpower shift to the private sector. But manpower is a small part of protection resources. A shift of protection resources to the private sector has already happened; cops only see the change in their turf.

Despite a concern for protection their "turf," so to speak, law enforcement is receptive to transferring responsibility to private security for certain activities and criminal incidents occurring on property being protected by private security. Examples of these activities are: burglar alarm response, initial investigation, completion of incident reports where the victim declines prosecution or is reporting for insurance purposes only. In our national survey, law enforcement administrators also suggested a number of noncrime related police activities as "potentially being more cost effectively performed by contracting with private security." Our survey of major national security companies revealed that some of these tasks--parking enforcement, funeral escorts, court security, etc.--were already being contracted for or security executives see them as potential areas of growth for their business. As the president of one national security company stated:

> You need only write out the specifications and some definite performance guidelines (measuring tools for yourselves) and you'll have a nontraditional way to deliver traditional services at a much lower cost.

Harsh economic realities of the 1980's may be the catalyst for a new dimension and realignment of relationships between private security and law enforcement.

Let's briefly review a decade of changes in some of the major assumptions about police-security relationships held by the Rand authors and other national studies. Inadequate police knowledge about private security and mutual lack of respect continue to be a problem. Perhaps private security has not done a very good job of communicating to law enforcement what it is that they do, but for the most part we have found the majority of "good faith efforts" on the part of private security rather than law enforcement.

The lack of a unified professional voice in the private security field was also a concern, and there is still one lacking today. With more than 40 security-related organizations, it is difficult--if not impossible--for law enforcement to reach all segments of private security. This is not to deny the efforts and influence of the American Society for Industrial Security, National Burglar and Fire Alarm Association, National Council of Investigation and Security Services, and others including a number of security journals and newsletters. Rather it simply indicates the breadth and diversity of private security.

One of the largest areas of concern was the lack of cooperation between private security and law enforcement. This is still a problem today, five and ten years later, but significant steps have been taken to develop cooperative programs since publication of the Hallcrest Report: ASIS has established its Law Enforcement Liaison Council; the International Association of Chiefs of Police established its Private Sector Committee; and the National Sheriffs' Association established its Private Security Industry Committee. These committees meet together several times a year to pursue cooperative strategies.

The now infamous description of a typical security guard in the 1972 Rand Report was "an aging white male, poorly educated, usually untrained and very poorly paid...he averages between 40 and 55 years of age, has had little education beyond the ninth grade, and has had a few years experience in private security." Fifteen years later, our site survey data finds the "average guard" to be a young white male, a high school graduate with probably some college exposure, and having met at least the minimum 40-hour recommended pre-assignment training standard. The median age

range is about 33 years, and only about 15% had not completed high school while 45% have some college. Pay is still near minimum wage for many contract guard employees, but for others there are opportunities to earn higher wages in "premium" assignments. Despite the fact that 65% of contract guards felt that their pay was too low, they expressed basic job satisfaction--only about one-fourth of them said they took the job because they were unemployed and couldn't find anything else. Some proprietary or in-house guards earn as much as some police officers. In-house guards clearly see a career path, with over one-half of them expecting to hold their job until retirement. There are clearly differences in contract and proprietary security personnel--proprietary have greater levels of training, education and compensation.

We think this is a general reflection of the upgrading in security personnel that has been occurring over the past five to ten years. Similar to events following historic U.S. court decisions (Mapp vs. Ohio and Miranda vs. Arizona) over the past two decades that started a surge in police training, private security appears to be going through a growing period of its own. The growth of the largest security association, ASIS, is a good indicator. In 1981, total ASIS membership was about 17,500 and the 1986 year closed out with nearly 25,000 members with 400 new applications being received monthly. Since 1977, also, nearly 50 new chapters have been added. Since 1978, the number of certified protection professionals has nearly quadrupled. When ASIS first established academic guidelines about 10 years ago, there were only five academic certification programs in security and two associate degree programs in the entire country. Today there are certificate and associate degree programs at over 100 colleges and nearly fifty bachelor and graduate degree programs.

It is hard to mention private security personnel issues in the same breath without addressing licensing and regulation. A decade ago, the PSAC[1] developed a model guard statute and the PSTF[2] developed quite comprehensive standards for background screening, training and licensing of private security firms and personnel. Despite all the controversy surrounding these efforts and a general sense that contract companies feel somewhat encumbered by it, virtually everyone in our national and site surveys favors regulation--eight out of ten proprietary and contract security managers and law enforcement administrators and operational personnel. Yet, at the same time in those surveys and in the surveys of state licensing agencies, we couldn't get anyone--law enforcement, contractual nor proprietary security managers--to say that licensing is effective in "assuring good private security business practices and personnel." Sure, we found some interesting anecdotal material on abuses of authority, excessive force and guards shooting bystanders, but we also found a fair amount of police officer misconduct too. The origin of most complaints for licensing violations brought before the state licensing boards are competitor companies, relatively few seem to have originated from grievously wronged citizens. Again, this is not to deny that there is some wrong-doing by private security, it is just that there is no hard empirical data to support the level of private security misconduct seized upon by the media.

---

[1] Private Security Advisory Council (PSAC), U.S. Department of Justice

[2] Private Security Task Force (PSTF), U.S. Department of Justice

It probably looks at this point like we have painted ourselves into a corner to disapprove of licensing. We can't go that far. The fact that a large number of our surveyed contract security personnel and armed proprietary personnel met minimal model guard statute and PSTF standards suggests to us that it is not a big burden on competent, well run, ethical security firms - it is simply a good business practice. A strong argument could be made for laissez-faire economics--let the marketplace take care of itself. We believe that in the end the marketplace always is the best regulator, but in the absence of any security industry leadership in setting and gaining adherance to performance standards, licensing and regulation is needed. Efforts to regulate proprietary security personnel divert too much attention from contract personnel licensing. Again, good business practice and corporate liability dictates a good level of training by most proprietary security and in our site work we found infrequent interaction with the public, especially detention and arrest. (The only real exceptions are the shoplifting arrests by retail security.) However, the majority of firearms carried by private security personnel, contrary to media exposes, are by proprietary security forces not contract security guards. Again, most armed personnel in our site work met or exceeded the PSTF minimum training standards, so there is no great burden in meeting these requirements--it is simply a prudent business practice. The potential for abuse with a firearm--with the ultimate risk of death in a mishap--is such an overwhelming public safety issue that regulation is justified. In short, we feel that the model guard statute and most of the PSTF standards have stood the tests of scrutiny and time; in lieu of security industry self-regulation other nonregulating states should adopt the Model Guard Statute.

In some states there is a profound misunderstanding of the training needs of contract security because contract guards are viewed in the stereotype of "rent-a-cops." For many posts and client assignments there are not very high levels of knowledge, skills and abilities required. For these assignments, extensive training requirements impose unnecessary overhead on contract companies. We are also concerned with the increased interest by state and regional police officer training councils or agencies in establishing and conducting mandatory training for private security personnel. The legal authority of private security personnel is rooted in property, contract and tort law, not in criminal law. In general, unless economies of scale exist with the use of shared facilities or core course content, there is little need for law enforcement to become involved in the majority of basic security officer training. As a corrollary, we favor the independent state licensing board as a preferred administrative mechanism for licensing and regulation. Police should not be in the security licensing business. We have identified this in our report as a "controlling behavior" on the part of law enforcement which sustains the climate of suspicion and distrust and precludes effective cooperation between law enforcement and private security. The most effective action that law enforcement agencies can take to assure good security practices and quality security personnel is to actively lobby for public access to criminal histories or designated access for an independent licensing board.

Another major issue is moonlighting by police officers in private security. This was a concern expressed in earlier studies. It certainly is an extensive practice: 80% of law enforcement agencies permit secondary employment in private security. Nationally, we estimated 150,000 police officers moonlighting in private security. It is not a clear-cut issue. On the one hand, contract security complains of open competition but often employs off-duty police officers, and proprietary security is very receptive to their use and sees no conflict of interest. In some situations, proprietary security managers feel like they need a legitimate, well trained, "hired gun" that will not be a serious liability.

We join a number of law enforcement administrators who have real concerns about liability and conflicts of interest when police moonlight. Perhaps the most valid argument of chiefs and sheriffs is one of job fitness--becoming fatigued from working too many off-duty hours. Furthermore, local officers are always assimilating victim and location crime data and are at distinct advantage to sell their off-duty security services while on and off duty. Use of department uniforms and equipment should be discouraged during moonlighting because of potential liability and conflict of interest. Moonlighting is a pervasive, long-standing issue that will not go away overnight. In fact, the economy and reduced police pay settlements will heighten the problem.

Another significant issue is alarm response. The interest in contracting out burglar alarm response to private security is not a simple solution to a very complex false alarm problem. On the one hand, law enforcement seems to be saying that alarm response really is not a police problem anyway, since it just gives preferential response to businesses and residential subscribers who can afford alarms, or it provides a service to alarm companies who make a profit at the public's expense! If the police are motivated to contract out response from this position, then it denys the deterrent value of alarm systems and avoids an opportunity to work constructively toward reduction of a serious false alarm problem. Law enforcement complains of being overburdened when alarm response calls are on the average 10 to 12 percent of total dispatch calls, and when 95 to 98 percent of them are false alarms. Significant cable TV penetration into the middle income residential market, the increasing number of over-the-counter retail alarm sales, and the potential for a deregulated telecommunication industry to enter the alarm market in a large way would make the current false alarm problem look trivial.

Before I close I want to give you a glimpse of a few of our 90 plus recommendations for improving private security and law enforcement relationships, and topics which need more in-depth research.

- Economic crime in the workplace throughout the U.S.-- estimated at $100 billion annually-- is a serious problem about which very little is known, and Government has even stopped trying to measure it. There is a need for an independent, non-profit or economic crime institute supported by a combination of Federal and private funding for research and demonstration programs of successful public and private sector cooperation in crime control.

- The investigative and loss data files of the public and private sector should have greater exchange of information; private security personnel are often excluded from receiving information follow-ups on data originally supplied by them.

- Joint seminars should be held on business crime, involving public and private sector resources to develop ongoing working relationships and responsibilities for more effective resolution of business crime.

- The crime analysis data of local enforcement agencies used in public crime prevention programs should also be made available to corporate and contractual crime prevention programs and services. In general, there should be greater coordination of public and private sector crime prevention programs.

- Our surveys indicated at least a dozen areas where cooperative programs should be established, e.g., hazardous materials and precious metals movement and terrorism countermeasures.

- A series of seminars should be developed which better educate law enforcement as to the role of private security in their community. Specific seminars and workshops should be developed on transfer of police functions, responsibility to private security, and contracting out of certain police activities.

- Corporations and institutions should establish prosecution policies that are clearly understood by law enforcement.

- Various interest groups, neighborhood groups, and business and industry should be given an opportunity to "broker" a combination of public and private protection services on the basis of cost-effectiveness and levels of service desired.

- Finally, tax credits for significant private security expenditures by business and industry should be considered, along with limited special police powers in lieu of police protection or reduced levels of protection.

In summary, citizen fear of crime and awareness that public criminal justice resources alone cannot control crime has led to a growing use of individual and corporate protective measures, including security products and services. The early 1980's saw the beginning of an overall decrease in reported crime in the United States. In large part this has been attributed to community crime prevention programs, but it also must be attributed in part to the increasing use of private security services and products. In addition to the vast resources and technology of the private sector to fight crime in this country, our report notes the large amount of crime in the private sector that is diverted from the public justice system and is resolved by a large and little known private justice system.

Public police resources seem to have stabilized. This mandates greater cooperation with the private sector to forge a partnership for crime prevention and reduction. Law enforcement can ill afford to ignore this important resource. Finally, law enforcement and other government officials along with business leaders must be willing to experiment with some nontraditional approaches to relieve law enforcement of its large workload of minor and non-crime-related calls for service. The creative use of private security human resources and technology combined with strong law enforcement may be the one viable option left to control crime in our communities.

SOCIAL IMPACTS OF TECHNOLOGY ON CRIMINAL JUSTICE SYSTEMS

Edward W. Lawless
Midwest Research Institute
Kansas City MO 64110

Prepared for XXXVIIIth International Course in Criminology, Montreal August 17-21, 1987

The focus of this course is on new techologies, but the program announcement noted that it intended not only to survey and evaluate technologies that can be used by the criminal justice system, but also to assess their social impacts and their risks to human rights. A few years ago I made a study of 100 cases of public alarm and controversy over a diverse array of technologies, and I offer in this paper some lessons from that study and some recent observations that, I hope, will be of help to you in anticipating future problems and needs for the criminal justice system.

Introduction

Technologies are developed and adopted because they serve basic needs and wants of the individual or of society; they benefit at least some segment of the public. You have already heard in this course of recent developments in several technologies for the identification, apprehension, conviction, or monitoring of criminals. While most of the impacts of technology are hopefully beneficial, many clearly, and often surprisingly, are not. Indeed, science and technology have become so inextricably interwoven into the fabric of modern society that they impact every phase of our daily lives, from conception and birth to death and burial, and they affect societal institutions no less than they affect the global environment.

New technologies can provide the road to fame, fortune and improved quality of life. Technological innovation can also have its darker side unless it is managed properly in the public interest. Almost weekly the media carry a new story of some technology that is causing grave public concern or spirited controversy because of an observed or potential adverse effect on some segment of the public. At times, the problem discovered is one that never existed before in the history of mankind -- one that our people , private institutions and government are ill-equipped to understand, let alone to resolve in a rapid and enlightened manner. Hence we can realistically speak of the "Three Faces of technology". We recognize the "Happy Face" of technology in its many benefits - increased availability of food, medical care, communications, clothing, housing, transportation, industrial production, and crime detection, to name but a few. But we can also often recognize the "Partly Cloudy Face" of technology as it captures us and exerts its many unanticipated consequences, and indeed its "Cold Face" in its many shocking adverse side-effects.

The criminal justice system, like other social systems, is

also affected in many ways by technological developments, and experiences the multiple faces of technology. I wish now to draw on my study of cases of public alarm over technology and studies in risk assessment to identify impacts of technology on components of the criminal justice system. Of particular interest may be some examples of how changing technologies, changing laws and regulations, and changing social norms and practices can lead to new kinds of crimes, and how the news media can affect crime, and public perceptions of crime and criminal justice.

Technology and Social Shock

In a study of public alarms over technology a few years ago, we identified well over 200 cases that made headlines between 1945 and 1970. We defined "technology" broadly to include all varieties of applied physical and biological science and engineering, and also basic research that might soon lead to a proposed technological development. I believe we could have easily identified a thousand such cases of alarm. These figures translate to at least one new case per month and probably almost a new case per week in the United States. That seemed to be an amazing rate of disturbing developments for the knowledgeable public to adapt to, but judging by my daily paper, the rate may be even higher today - limited perhaps more by the competition for headlines, column inches and air time than by the number of events.

We prepared detailed case studies of 45 of the identified cases and prepared synopses of 55 other cases. Our cases ranged from controversies over police and medical practices to recalls of TVs, autos and diet sodas, and from scares over skyjacking and environmental damage to disputes over sports equipment and the authenticity of art works.

In addition to developing the case histories, we made a substantial analysis of the commonalities and peculiarities of the collected cases, with particular attention to the role played by the news media. The results of the study were published as the book *Technology and Social Shock*[1].

Ten illustrative cases are noted in Figure 1.

Figure 1. Example Cases of Public Alarm Over Technology.

1. The Chemical Mace
2. Illegal Use of Copying Devices
3. The Skyjacking Nightmare
4. Concern Over Video Violence
5. The Thalidomide Tragedy
6. Human Artificial Insemination
7. XYY Genotype and Antisocial Predisposition?
8. Disqualification of Dancer's Image
9. DMSO - Suppressed Wonder Drug?
10. The Bronze Horse - A Technological Definition of Art?

Preliminary study of a proposed new technology may conclude that it could be safely used, and it then begins a period of implementation and growth. A few thoughtful people might object at this point that the technology may have undesirable consequences, but they usualy lack proof and not much of anything happens; they are often burdened by an assumption that they have a conflicting interest or that they are simply "against progress." More often, their objections are just drowned out by the reassurances/advertising/propaganda of the industry or government agency involved and by the public's acceptance of the new technology.

Stimulating factors for the development of many technologies historically have been a need for increased personal, community and national security, or a drive to impose one's will on another individual or nation by force in matters of conflicting desires. And as we all know, the complexity of the technology increases dramatically with time. Technologies to prevent or solve the age-old crime of stealing have evolved from the simple mechanical locks to complicated access codes to protect important data bases. Identification of criminal suspects has evolved in a few decades from manual fingerprint matching to a host of sophisticated forensic techniques, including chemical or biological analysis of bits of material or tissue and computerized recognition of behavior patterns.

The human needs or wants served by the technologies in our study cases varied widely, but the most-represented categories (in decreasing order) were: food supply and agriculture; security and national defense; medical care and public health; industy and commerce; waste disposal; energy supply ; communications; clothing; and recreational/entertainment/cultural values. Chemistry, medicine, physics, military science and engineering were professional fields that were frequently associated with the development of the technologies studied, and foreign technological inputs were important in about 40% of our cases. Cases involving some of the "largest" technologies also had the largest numbers of people as users, but many of our cases served a relatively small percent of the total populace.

Discovering the Threat

The development of public concern over a technology may be either a gradual or sharp realization by society that a previously unrecognized threat exists, or that a previously accepted risk is no longer acceptable.

The early signs of difficulty frequently arises from changes in analytical methods (e.g. statistical, instrumental, chemical, biological, etc.) wherein an existing method is applied as it had not been before, a technological advance makes a method more sensitive, or a new technology produces an entirely new method. Application of the analytical method to some area that interfaces with the subject technology then yields evidence that it is producing undesirable consequences. In many cases these effects become observable only after the technology has grown very large, and in some cases they may even not be objectional if it doesn't pass a critical size. The time required may be a half century or more for a major technology, but in a some cases a fear of possible future effects can lead to public controversy even before the technology is introduced. The curiosity of the scientific community about the technology usually leads to an increasing number of publications about its potential adverse effects in the technical literature, and after a time in the popular press.

In our studies, the threat developed in over one-half of the cases because the technology had been used with less than adequate responsibility, early warnings were missed in nearly 40% of the cases, and "problem" technologies had been allowed to grow in nearly half the cases. Interestingly enough, new technological information, often in a different field, was important in discovering the threat in about two-thirds of the cases. The time lag may be greatly shortened or even eliminated if the undesirable consequence is exceptionally threatening or is keenly articulated by a government authority, a public spokesman (a scientist or other highly quotable person), or a particular news medium or journalist. In fact, a key spokesman, announcement of dramatization could be identified in about half of our cases.

Society' Institutions React

Society's first reaction to a suspected problem technology is often to ignore it as long as possible. Eventually this can no longer be done, and society' institutions are forced to spend vast amounts of time and energy trying to decide what to do about a technology that has produced a very large problem, but which may have become such a part of our daily lives that it almost seems indispensable. Governmental regulatory agencies are usualy drawn into the case as concern mounts, along with involved industries, commercial interests, military agencies, law enforcement agencies, unions, or professions.

By this time, the case is usually being widely played in the news media; typical stories may be composites of incomplete facts and controversial opinions under cryptic and overly dramatic headlines. The accused parties and government agencies involved may issue denials that a threat exists, assurances that a threat is minimal, or reassurances that it will soon be remedied. These statements generally have low credibility with the media, however, and possibly with the public. An investigation or interim action of some sort may be announced, or an extensive public relations campaign may be launched by those "on the spot". Their accusers, on the other hand, may make claims that the danger is even greater than previously reported and that the government or industry is lax in its remedial efforts. These charges are usually widely quoted and may raise the issue to a fever pitch.

The mayor, governor, president, or lawmakers may demand stern action, at some point, and the responsible law enforcement or regulatory agency may initiate a precipitate course - one that may subsequently prove either justified or ill-advised. If the pressures become intense, the issues may degenerate into a search for a scapegoat by elements of government, industry, the media, or citizens groups. More often, however, the case enters into a period of reasonably serious effort to find the facts and remedy the problem. Presidential panels, congressional hearings, reviews by regulatory or professional bodies, or experimental studies often occur during this time. The disposition of the case may well depend, however, as much on public perceptions as on the scientific information available.

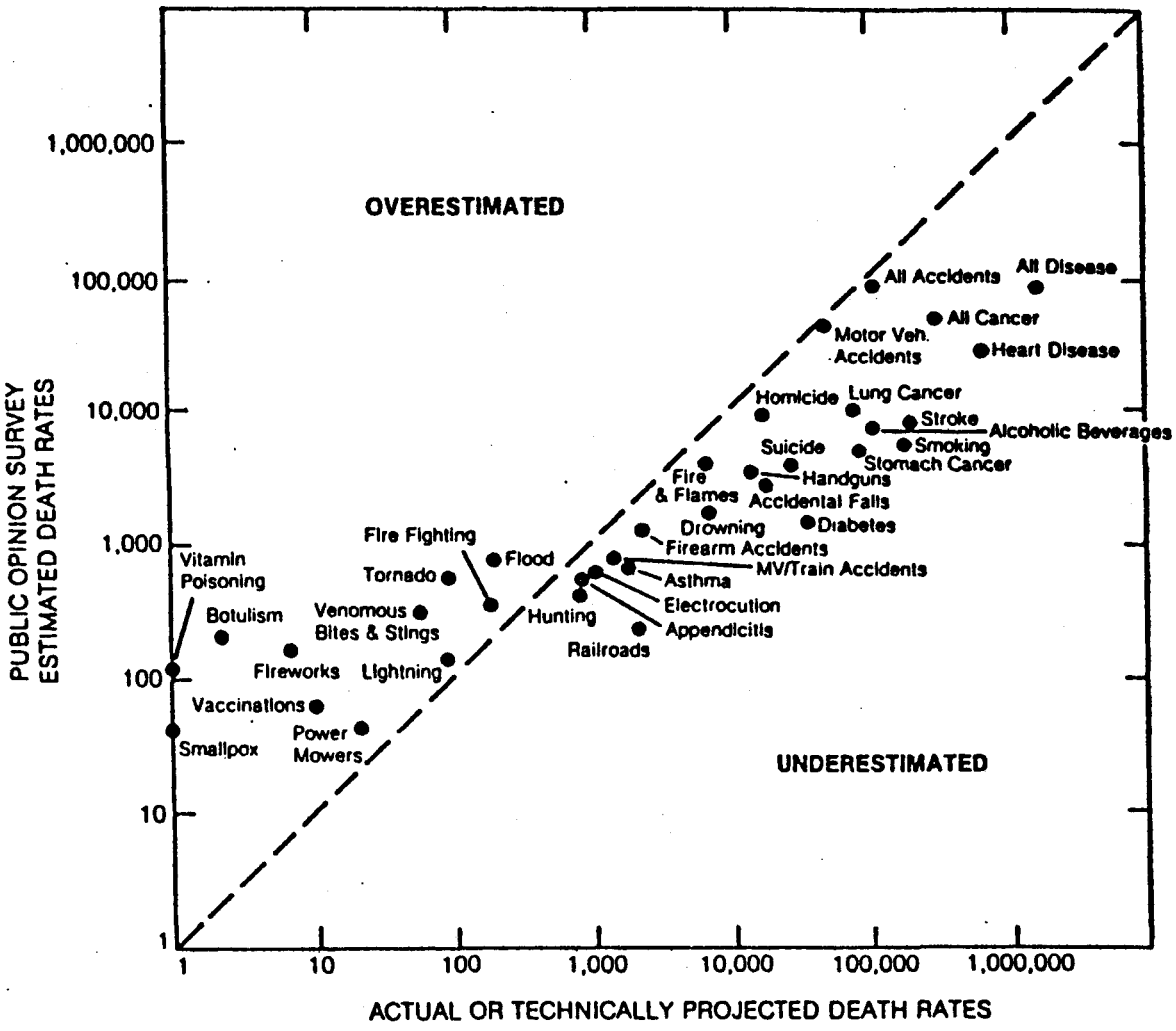


Figure 5. Public perception of U.S. annual death rates from selected causes (adapted from Slovic et al. 1980).

Public Perceptions

Many factors influence public perception of the threat and the attempts of society's institutions to come to grips with it. The public has considerable difficulty in gaging the degree of risk posed by natural hazards, let alone technologically-derived ones. In general, people tend to overestimate frequencies of death from rare causes and to underestimate fequencies from more common causes, as shown in Figure 5[5], adapted from Slovic, et al[4]. Note that the total range among estimated rates was only a thousand, wheras the actual range was a million, a reflection of the human difficulty in comprehending orders of magnitude ranges. The degree of misestimation appears to be closely related to news media coverage. This suggests that the public is getting substantial misinformation *in the aggregate* from the media, although media people may maintain that they merely reflect the public's interest in the events that happen.

The degree of media interest to a developing issue will vary substantially depending on several factors, as suggested in Figure 6.

Figure 6. Factors that tend to increase media attention to a developing controversy.

1. Nature of the value threatened
2. Magnitude of the threat
3. Special characteristics of threatened group
4. A previous related alarm exists
5. Sharp or dramatic articulation of the issue
6. Other media factors

Attention is usually high these days for subjects involving human reproduction, food and water safety, medical practice, transportation safety, environmental degradation, human rights, and entertainment. Attention is not necessarily proportional to the severity of the threat or the numbers of people threatened. It may increase greatly if the threatened group has special characteristics, if a similar alarm had occurred previously, or if a previous law or regulation was part of the problem. Interest maybe highest where the data suggesting the threat's realality is highly uncertain.

Characteristics of the media itself also come into play. The media focus best on simple events and conflicts of opinion rather than complicated technical matters. A demonstration at a nuclear power plant, a press conference by a whistle blower, or a congressional hearing will gain more attention than a series of definitive scientific papers. Attention will be increased greatly if the issue is particularly susceptible to a cartoonist's whimsy or to an expose' treatment. The media also focus better if a specific piece of technology can be tied to a narrow problem, and not so well to a broad, long-term effect on our quality of life. If the offending technology can be reduced to a "headline-sized" abbreviation, the more the attention, e.g. LSD, DES, DDT. Ultimately, of course, competition of other news

stories will limit attention.

On the whole, the performAnce of the media in reporting scientific and technological information to the public leaves much to be desired. They tend to overdo the bizarre, the catchy phrase, or the scare aspect at the beginning of a case, and seldom follow through to summarize adequately the resolution of the case.

In addition to media attention, several other factors can influence the degree of public concern over a threat, as suggested in Figure 7.

Figure 7. Factors that tend to influence public concern over technologically-derived hazards.

1. Media treatment of the issue
2. Avoidability, controlability, reversibility of the impact
3. Familiarity with the hazard posed
4. Familiarity with the technology
5. Perception of benefits of the offending technology
6. Perception of parties caught up in the controversy
7. Perception that someone is "in charge"

This "leading indicator" feature of the technical literature versus popular press coverage is shown for our study of the 1970 controversy over the safety of oral contraceptives (Figure 8). The media cannot, of course, give immediate attention to every scientific publication that sugests an adverse technological impact, but attention often builds as society's institutions react to the threat. In the case of DDT, the peak of popular press concern did not occur until the technology was quite "mature", and its use was in decline for other reasons (Figure 9).

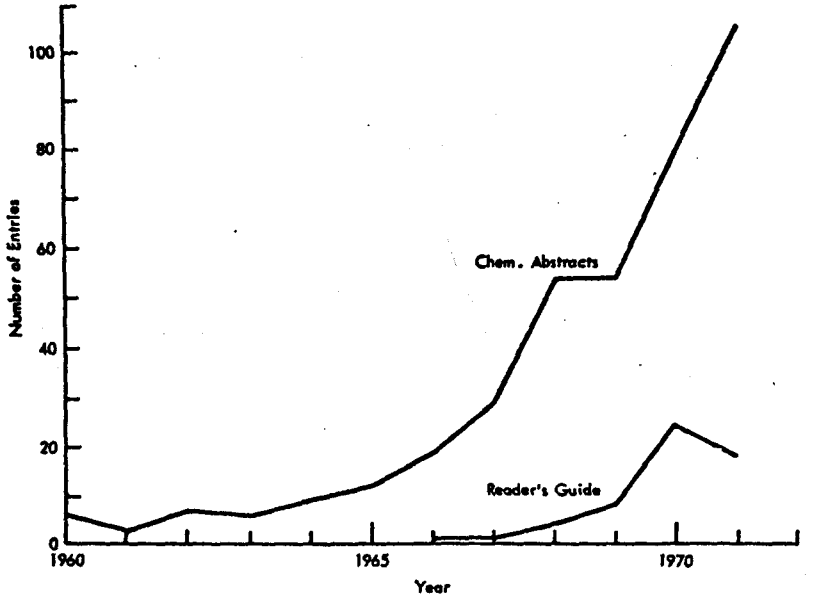


FIGURE 8. Time Lag of Popular Press Publications Behind Technical Publications for Oral Contraceptives. © 1977, Rutgers, the State University of New Jersey.

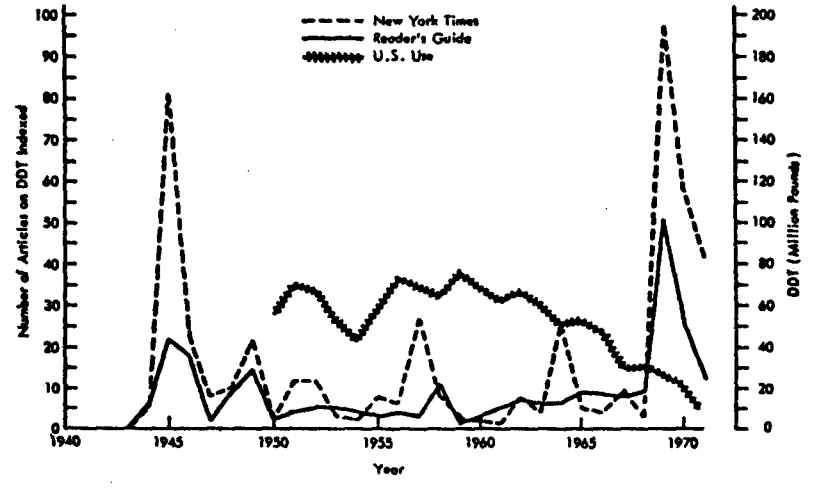


FIGURE 9. Popular Press Publications vs. United States Consumption for DDT. © 1977, Rutgers, the State University of New Jersey.

Disposition and Impacts

The initial public concern and media attention focused on the technological problem seldom lead directly to a remedy. If the public alarm does not bring about remedial action fast enough, frustration and a lack of confidence may result. In most cases subsequent hearings, research and forces of the market place, politial pressure, churches, labor unions and professional societies, ultimately lead to changes that reduce the threat or minimize its impacts. Sometimes the alarm will be found to have been far out of proportion to the true danger. Substantial confusion and psychological, social or economic damage may have been incurred unnecessarily. The public's confidence in its social institutions may have been decreased, or its skepticism of the media's reliability increased.

Negative economic impacts resulted in nearly half of our study cases, but individuals suffered actual losses in relatively few, and even some of theses may have eventually received reimbursement by government or private funds. Industrial or commercial interests incurred economic damages in several cases. Business firms have been held increasingly liable by the government for causing certain kinds of problems since our original study, but have been increasingly indemnified by government for incurring certain kinds of damages.

grow in nearly half the cases. Interestingly enough, new technological information, often in a different field, was important in discovering the threat in about two-thirds of the cases. The time lag may be greatly shortened or even eliminated if the undesirable consequence is exceptionally threatening or is keenly articulated by a government authority, a public spokesman (a scientist or other highly quotable person), or a particular news medium or journalist. In fact, a key spokesman, announcement or dramatization could be identified in about half of our cases.

Avoiding Future Technological Shocks

Can we anticipate social shocks over technology? Our studies[3] suggest consideration of four major classes of technologically-derived threats, dangers or risks can help: Prerecognized and accecptable risks; Big accidents; Misused of abused technologies; and Desultory dangers I will illustrated each of these with an example or two

Prerecognized and Acceptable Risks: This type is most familiar. Examples include making a personal wager or a plane trip, or government approval of a new highway speed limit or prescription medicine. Conscious decisions are made to accept the risks. Problems can arise ,of course, if the risks are misperceived or perceived differently by different people. In general, people tend to overestimate rare causes of death and underestimate more common causes, as noted previously. The degree of misestimation appears to be closely related to media coverage. Problems can also arise if different segments of the public have greatly different degrees of acceptance of a given risk, or if the degree of acceptance decreases greatly over time.

Big Accidents: Here we are talking about accidental events, often involving complex technologies, over which those at risk have little control, e.g. airplane crashes, building collapses, overturned tankcars. Such events make headlines, but do not usually involve crimes and will not be discussed further here.

Misuse and Abuse of Technology: Misuse or overuse of a technology may result from ignorance, carlessness overconfidence, or uncertainty. Familiar examples include overuse of medical X-rays, lab testing, lobotomies and radical mastectomies. A deadly flood in South Dakota was blamed on overuse of cloud-seeding to break a drought. Abuse may be opportunistic, such as with many cases of skyjacking a few years ago, and laetrile, the widely-promoted but ineffective cancer treatment. Abuse can also be malicious, as with the rash of letter bombs a few years ago and a recent case in which a man placed a capsule of radioactive material in his small son's shorts and caused serious damage. In Italy a few years ago a case involved surreptitious taping of guidance given in the confessional.

Desultory Dangers: This class of threats is the most difficult to envision beforehand. It includes the wide range of risks that are discovered as a result of technology's side effects, including indirect, delayed and synergistic effects. It includes cause-effect chains of events and effects that become apparent only with increasing technological scale or improvements in detection and analysis methods. In some cases the problem is soon recognized and remedied, e.g. the early, clinging thin plastic garment bags that suffocated many small children were soon made safer, thalidomide was banned, and atmospheric testing of nuclear weapons was suspended. In other cases, the problem is difficult to evaluate and remedy. For example, monocultural crop practices stimulate pest problems which stimulate pesticide use, which may destroy important natural control or nontarget species, but large populations depend on modern intensive agricultural methods that cannot be rapidly changed.

Technologies are sometimes developed and adopted to serve selfish or illegal purposes rather than real societal needs. Thus perceived needs to detect police radar units soon leads to "fuzz busters", development of police body armor leads to teflon-coated armor-piercing bullets, and magnetic and X-ray detectors for airport security will lead to concealable nonmetal plastic-composite handguns. A homemade laser device was reportedly fired at a helicopter in Los Angeles. We must anticipate that if science can do something new, someone will probably do it. If a cross between man and ape can be made, it will be, and not one, but a population of such creatures may be made for someone's purposes.

The important point for this group is that new technologies can not only lead to new crimes, they can force new definitions of what is a crime (e.g. tape pirating; joking about bombs at airports). In addition, new laws to regulate technologies regularly lead to new categories of crime (e.g use of studded snow tires where prohibited; midnight dumping of hazardous wastes along highways).

Conclusion

Modern technologies can exert subtle influence far from the point of their use, and modern communications methods can generate nationwide concern about a newly-discovered adverse effect almost overnight. People learn that technologies, of which they may know little, pose hazards which they may only dimly understand. They have little confidence in their own ability to judge correctly the actual danger to themselves or how to avoid it. For the most part, they are dependent upon the new media's frequently sensationalized and often inept descriptions of what the problem is and what is being done about it.

The development of intense controversy over technologically-related problems may force the public and private sector to seek rapid solution of a suspected or real problem. But as the cases discussed herein show, resolution of such disputes and remedy of such problems often do not proceed effectively in the glare of the spotlight. Minimization of the chances of occurrence of such controversies should be a goal of both those who promote and use new technologies and those who seek to protect society from technology's sometimes surprising effects

References

1. Lawless, E. W., Technology and Social Shock, Rutgers University Press, New Brunswick, New Jersey, 1977. 616 pages. (Summarized in paper of same title in Futurics 4 (314) 257-268 (1980).

3. Lawless, E. W., "The Nature of Controversy over Technology," pp. 248-256 in Weed Control in Forest Management: Proceedings of the 1981 John S. Wright Forestry Conference, H. A. Holt and B. C. Fischer, Eds., Purdue Research Foundation, West Lafayette, Indiana, 1981.

2. Lawless, E. W., "Anticipating Technologically-Derived Risk," Impact Assessment Bulletin, 1 (3), 54-66 (1982).

4. Slovic, P. B. Fischoff, and S. Lichtenstein. 1980. "Facts and Fears: Understanding Preceived Risk," p. 181-224. In Societal Risk Assessment, R.C. Schwing and W. A. Albers, Jr. New York: Plenum Press. 363 p.

HUITIEME PARTIE

PART VIII

IMPACTS SUR LES DROITS DE LA PERSONNE ET LES PROCEDURES LEGALES

IMPACT OF HUMAN RIGHTS AND CRIMINAL PROCEDURES

The Human Rights Context of Technological Innovation

David H. Flaherty

University of Western Ontario

London, Ontario

Technological developments are indeed changing criminal justice and its relationship to society. I am thinking in particular of advances in national police computer systems, such as the Canadian Police Information Centre, including computer matching; various forms of electronic surveillance, including electronic bracelets; the use of urinalysis for drug testing, and the use of the polygraph.

One novelty in North America and Western Europe in the last fifteen years is that such technological innovations have become 1) increasingly subject to the jurisdiction of privacy and data protection legislation, when they involve, as they customarily do, the collection and use of personal information, and 2) the overview, in all countries except the United States, of privacy and data protection commissions or commissioners.

In this presentation, I will discuss the attention given to such matters in a report tabled in the House of Commons on March 31, 1987: Open and Shut: Enhancing the Right to Know and the Right to Privacy. Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act (Ottawa, 1987). I was the privacy consultant for the work of the committee.

The report addresses the following issues that are relevant to controlling the impact of technology on criminal justice. Each of them are touched on briefly in my presentation below.

1. Oversight of computer-matching programs
2. Controlling uses of the Social Insurance Number
3. Removing the concept of exempt banks from the Privacy Act
4. Regulating the Canadian Police Information Centre
5. Controlling electronic surveillance
6. Controlling urinalysis for drug testing and the use of the polygraph

1. Oversight of Computer-matching Programs

"Computer matching" involves a particular type of record linkage or matching of personal data. It has been defined as "the comparison of different lists or files to determine whether identical, similar, or conflicting information appear in them. Comparisons can be made by matching names, social security numbers, addresses, or other personal identifiers."[1]

As noted in a June, 1986 report from the U.S. Office of Information Technology, computer matching can be used to detect unreported income, unreported assets, duplicate benefits, incorrect personal identification numbers, overpayments, ineligible recipients, incongruous entitlements to benefits, present addresses of individuals, and service providers billing twice for the same activity. The same report distinguishes computer matching, which involves comparing records after an individual is already receiving government benefits or services, and front-end verification, which "is used to certify the accuracy and completeness of personal informations at the time an individual applies for government benefits, employment, or services."[2]

The Privacy Commissioner has drawn particular attention to the risks of computer matching, because the existence of computers and automated data banks makes widespread matching truly feasible. In the

vivid language of the Privacy Commissioner, "Computer-matching turns the traditional presumption of innocence into a presumption of guilt: in matching, even when there is no indication of wrong-doing, individuals are subject to high technology search and seizure. Once the principle of matching is accepted, a social force of unyielding and pervasive magnitude is put in place."[3]

The process of government would indeed be more efficient if we were all watched and monitored; the problem is to establish acceptable and tolerable limits to computer matching. There is an especially strong resistance to far-flung matching operations that involve access to a broad array of personal data from various government institutions. The current mechanisms to regulate such practices are inadequate. In particular, a balance must be achieved between the privacy interests of individuals and other societal values, such as the reduction of fraud and waste.

The Privacy Commissioner concluded in his brief to the Committee that although a recent Supreme Court of Canada decision "reinforces the protection against cross-matching now implicit in the Privacy Act, growing pressure to use the technique in pursuit of some undoubtedly admirable causes may make it prudent to make the prohibition specific and explicit."[4]

Although the Department of Justice has stated that computer matching by federal institutions is currently covered by the Privacy Act, the Committee believes that certain aspects of this practice require stronger protections and controls in the legislation itself.[5]

At present, the Privacy Act does not deal with computer matching or record linkages in such explicit terms as would be desirable, although it does establish in section 7 the basic principle that personal information should only be used for the purpose for which it was collected. Yet as the Privacy Commissioner has pointed out, "Section 7(a) proscribes the use of personal information except 'for the purpose for which the information was obtained... or for a use consistent with that

purpose.' Since computer-matching involves the comparison of personal information collected for different purposes, the practice contravenes this provision of the Act. Only an unacceptably broad interpretation of the words 'consistent use' could be used in an attempt to justify computer-matching as now understood."[6] The Commissioner is concerned that, just as in the U.S. experience, where the concept of "routine uses" has facilitated the transfer of data for computer matching, the analogous Canadian standard of "consistent uses" may likewise promote unacceptable computer matching in this country.

For various reasons, some clarification of the Privacy Act is desirable to control the use of computer matching. A special survey by the Treasury Board Secretariat in 1984-5 revealed that federal institutions are indeed carrying on a considerable amount of data-matching.[7] However, many government institutions have failed to account adequately for their computer matching activities, as required by the Privacy Act. The President of the Treasury Board informed the Committee that sections 7 and 8 of the Act "do not deal adequately with the use of the new technology for data matching."[8] A legitimate matching procedure should be a matter of public record or be made subject to guidelines. Computer matching should be explicity prohibited if it involves using information collected for one purpose for another inconsistent purpose.

Recommendations:

5.6 The Committee recommends that the President of the Treasury Board issue guidelines requiring government institutions to follow the requirements listed below and also recommends that a specific section incorporating these requirements, and a definition of computer matching, should be added to the Privacy Act:

Government institutions should be required:

a) to give sixty days advance public notice (a comment period) of intented matches in the Canada Gazette and to describe all current matching activities and the type of information resulting from the match in the annual Personal Information Index;

b) to report in sufficient detail in the announcement of proposed matches to identify clearly the authority under the Privacy Act permitting the match; and

c) to regiter any new bank resulting from data-matching.

5.7 The Committee further recommends that the Privacy Act prohibit all but the most carefully circumscribed data matching, especially with respect to those matches involving the use of personal data from another institution.

5.8 The Committee recommends that the Privacy Commissioner be especially vigilant in his oversight of computer matching and make a particular point of drawing perceived abuses to the attention of Parliament, both in his annual report and in his appearances before the Standing Committee on Justice and Solictor General.

2. Controlling Uses of the Social Insurance Number

The Social Insurance Number (SIN) is the most common unique personal identifier in use in Canada. The basic reason for the development of SINS in the early 1960s was the need for numerical identification of individuals to use mainframe computers efficiently; this technological imperative largely continues to the present day. SINS were introduced for purposes of federal unemployment insurance and pension plans in 1964, but no controls were placed on additional uses of this new numbering system, despite some promises that this proliferation would not occur. In fact, the impetus to multiple uses of SINS as a numbering scheme began as early as the initiation of the system in 1964-5. Between 1965 and 1977, the House of Commons paid little systematic attention to the burgeoning uses of SINS.[9]

In 1981 the first Privacy Commissioner, Inger Hansen, Q.C., prepared a report on the Social Insurance Number in which she recommended the creation of a new criminal offence "against the privacy of another" in order to regulate its use .10 The Government took no action on this report.

The number of ways the Social Insurance Number is used today worries many canadians. This identifying number is so important, so special, and so much a symbol of the need for data protection that it demands certain controls over its use. In 1985-86 the Office of the Privacy Commissioner heard from more than 100 individuals who "either wanted to complain about an organization's use of social insurance numbers or sought clarification about the requirement to provide a SIN."[11]

The simple problem is that Canadians are constantly being asked for their SIN. It is used as a unique personal identifier in a wide variety of settings in all sectors of society .12 It is alleged that certain police departments require a SIN from persons calling its emergency number. Some funeral homes require the number of the deceased to obtain a burial permit from municipal authorities. Persons seeking access to some federal office buildings are asked to produce their SIN. It is thought that credit bureaus use the SIN as a primary means of linking pieces of information about a specific person. Insurance companies regularly ask policy holders to supply their SINS in making policy claims. In the private sector, persons who refuse to divulge their SIN risk the denial of services.

Although it is a very important tool in the operation of our increasingly automated society, the Committee's view is that the Social Insurance Number should not be employed in ways never intended or authorized by Parliament. Individualized numbering systems should be devised to meet the needs of specific systems. The fundamental problem at present is that "the elected representatives of the Canadian people have failed to ensure the existence of adequate policies for controlling the development and uses of social insurance numbers."[13] The 1964

legislation creating the SIN failed to provide any safeguards on its use for other purposes. Thus, the uses of the number as a unique personal identifier have proliferated. The general public seeks controls over the unauthorized uses of the SIN - by the private sector, in municipal and provincial governments, and at the federal level.

Federal employers should take the lead in the judicious use of the SIN. Specifically, as the current Privacy Commissioner has noted, Social Insurance Numbers "should be protected from indiscriminate and trivializing uses."[14] At present, there are 11 Acts or regulations giving federal agencies the authority to collect the SIN, primarily for purposes of unemployment insurance, income tax, and social security.[15] Federal government institutions must question why they are collecting the SIN and whether they truly need it.

The Privacy Commissioner poses the dilemma quite clearly by noting that "if a (Social Insurance) number is requested for any other purpose, an individual is simply not obliged to provide it. Of course, by not providing it, he or she may not receive the goods or services which are desired. That is a decision for each person to make". The Privacy Commissioner further noted that "Uncontrolled and general use of the SIN establishes a de facto national identifier with all its ominous and de-humanizing implications."[16] This theme has also been recently emphasized in the U.S. Congressional Office of Technology Assessment's study of Electronic Record Systems and Individual Privacy.[17]

In the 1970s, the Progressive Conservatives made the use of SINs a major political issue. The Clark Government prepared legislation for controlling the uses of the social insurance number, but it was not introduced before the Government fell at the end of 1979. The bill was part of the Conservatives initiatives on access to government information and improvement of privacy protection. Perrin Beatty, M.P., and Senator Jacques Flynn subsequently introduced Bill C-535 in the House and Senate in May 1980.

The 1980 Progressive Conservative Bill, which was essentially

a revision of the original privacy legislation, (Part IV of the Canadian Human Rights Act of 1977), also proposed a new section of the act, which would have limited the government's use of the Social Insurance Number to the administration of an Act of Parliament or seven basic programs: pensions, student loans, family allowances, old age security, income tax, and unemployment insurance. Otherwise, "no right, benefit or privilege shall be withheld from and no penalty shall be imposed on any individual by reason of a refusal by the individual to disclose to a government institution the Social Insurance Number assigned to the individual..." Except for the authorized the Privacy Commissioner to review complaints about Social Insurance Numbers.

Since 1980, three Members of Parliament from the Progressive Conservative party, Messrs. Hnatyshyn, Gamble, and Stackhouse, have introduced identical bills "respecting the use of Social Insurance Numbers."[19] The preamble to these private members bills is as follows:

> Whereas it is desirable to prevent Social Insurance Numbers from becoming an employee identification number, a student identification number, a patient identification number, a customer identification number, and generally a national single identification number;
>
> And Whereas it is desirable to ensure that any further disclosure or use of Social Insurance Numbers is specifically authorized by prior Act of Parliament after full consideration and public consultation.

The Committee shares the continuing concerns expressed in these private members bills.

The Committee notes that at its 1986 annual meeting the Canadian Bar Association passed a resolution on the Social Insurance Number expressing "its deep concern over the philosophy of using a compulsory identification number as a means of tracing or locating persons for purposes other than income tax, social assistance and pensions, as initially instituted."[20] Furthermore, the Committee also takes note of the fact that, after the unauthorized removal of tax records

containing Social Insurance Numbers of 16 million Canadians form an office of Revenue Canada Taxation in November, 1986, La Ligue des Droits et Libertés announced the organization of a coalition of Quebec organizations to demands controls on the use of such numbers.[21]

Recommendations:

5.9 The Committee recommends that a new section of the Privacy Act limit the collection and use of Social Insurance Numbers to those activities explicitly authorized by federal Act or regulations. Otherwise, there should be a statutory prohibition against the federal government, the provinces, or the private sector denying services or goods to an individual, because of a refusal to provide a Social Insurance Number. The Committee also urges the creation of a statutory cause of action under the Privacy Act for individuals faced with such refusals.

5.10 The Committee recommends that the Privacy Act be amended as follows:

> It shall be unlawful for any Federal, provincial or local government institution or the private sector to ask any person for his or her Social Insurance Number, unless such a request is authorized by law.
>
> It shall be unlawful for any Federal, provincial or local government institution or the private sector to deny to any individual any right, benefit, or privilege provided by law, because of such individual's refusal to disclose his or her Social Insurance Number, unless such disclosure is required by federal statute.
>
> Any federal government institution which requests an individual to disclose his or her Social Insurance Number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.[22]

3. Exempt Banks

Section 18 of the Privacy Act authorizes the Governor in Council to establish personal data banks to which individuals cannot obtain access under any circumstances. This section stipulates that the information banks in question "contain files all of which consist predominantly of personal information" concerning international affairs, national defence, and law enforcement and investigation, as describeb in sections 21 and 22 of the Privacy Act.[23] Individuals who apply for access to an exempt bank are neither given denial nor confirmation of the existence of information about them. The Privacy Commissioner has an oversight function with respect to these exempt banks and may examine them in detail, except when issues of Cabinet confidence arise.[24]

Until 1986, there were about 20 such "exempt banks" for the entire federal government out of a total of more than 2200 personal information banks. The Treasury Board has informed the Committee that there will now be only 5 exempt banks, as soon as the Order in Council revoling the exempt status of 15 exempt banks has been prepared.[25]

The Committee is impressed by the fact that, after the reduction in the number of exempt banks announced by the Treasury Board in 1986, the following institutions no longer have exempt banks: Canada Employment and Immigration Commission; Canada Post Corporation; Canadian Penitentiary Service; Canadian Security Intelligence Service; and the Department of the Solicitor General.

The status of exempt banks has already been at issue, because of the Ternette decision in 1984.[26] When Mr. Ternette's application for personal information from the RCMP's exempt bank of Security Service records reached the Federal Court of Canada, his lawyer asked the Department of Justice to confirm that all the files in the bank were examined before it was closed, in order to confirm that the bank met the criteria for exemption. Since the response was negative, the Department of Justice subsequently indicated that this bank could no longer be

treated as exempt. The Federal Court also asserted its right to review such files to determine whether or not a file was properly included in an exempt bank. A notice of appeal orginally filed by the Solicitor General was discontinued in November 1984.

Because of the decision in the Ternette case and subsequent developments, the concept of exempt banks has lost much of its rationale and validity. Mr. Justice Strayer of the Federal Court concluded that an order-in-council creating an exempt bank under section 18(1) of the Privacy Act can only be made "where each of the files in the bank consists 'predominantly of personal information described in section 21 or 22. 'This follows from the fact that exemptable banks must contain files 'all of which' consist of such material!"[27] The Privacy Commissioner has conducted a systematic examination of all exempt banks and is treating them as open, if there is evidence that they were improperly constituted.

It would be preferable, in the view of the Committee, to treat all personal data in information banks in the same fashin, thus applying the numerous standard exemptions available under the Privacy Act to all requests by individuals for access to their personal data. As the Privacy Commissioner explained: "Each application will require the institution to examine the file, not to reject the request automatically because of the privileged position of an information bank. Government institutions may regret the loss of an easy denial of access. But applicants for personal information will be assured of receiving individual treatment."[28] The Committee believes that there should be no body of personal information which is entirely exempt from any kind of review and record-by-record examination.[29]

Administrative convenience is the only major argument in favour of exempt banks. It is much simpler for an institution to claim full exemption for an information bank, and it may be less expensive to do so, in terms of workload, than to review every data bank containing information on international affairs, national defence, and law enforcement and investigation. However, the Ternette decision requires a

procedure to ensure that the files in question "consist predominantly of personal information," as required by section 18(1) of the Privacy Act. Thus individual files must now be reviewed for such purposes as a consequence of this judgment. Moreover, sections 4 to 9 of the Act, concerning the collection, retention and disposal of personal information, imply that government departments must have a review mechanism in place to ensure compliance with fair information practices.

In a similar vein, sensitive information of the type intended for exempt banks raises fears in some quarters about what personal data the government is actually collecting. The public should have the assurance that such data are reviewed in detail in order to ensure their conformity with the Privacy Act.

The Privacy Commissioner and the Canadian Bar Association have supported the concept of deleting the provision for exempt banks from the Privacy Act. As the Commissioner stated: "Given my choice, I would not have exempt banks. I think it gives the Privacy Act a bad name... Obviously, some information should be exempted, but I think information ideally should be exempted on a case-try-case basis."[30]

Recommendation:

5.11 The Committee recommends that the concept of exempt banks be removed from the Privacy Act by repealing sections 18 and 36, because there is no compelling need to retain such a concept in light of the other strong exemptions on disclosure that exist in the legislation.

4. The Canadian Police Information Centre

One of the most sensitive data bases is the Canadian Police Information Centre (CPIC). It affects all Canadians, directly or indirectly. CPIC is operated as a centralized, automated index to local police records, by the Royal Canadian Mounted Police, at the expense of the federal government, on behalf of police forces across Canada. CPIC itself contains personal information in a variety of interrelated data

bases, but it is also an index to the original records kept by local police forces. It is the most visible police information system in Canada and illustrates the general problems of implementing good data protection practices in all police data systems. CPIC policy is set by an advisory committee composed of twenty-six senior police officers from across Canada. In practice, it is the RCMP that primarily makes policy for CPIC.[31]

One of the issues that arose at the Committee's hearings is the extent to which CPIC is subject to the Privacy Act and thus to the jurisdiction of the Privacy Commissioner for purposes of auditing and investigating complaints. The Privacy Commissioner and the Solicitor General claimed that CPIC was at least partially exempt from such scrutiny, because certain data in it originated with local and provincial police forces.

A legal opinion from the legal advisor to the Privacy Commissioner, dated November 21, 1986, asserts that "information provided to the Canadian Police Information Centre by police agencies other than the Royal Canadian Mounted Police could not be investigated pursuant to the Privacy Act." The opinion claims that some of the data accessible through CPIC are not in the "control" of the RCMP. In the view of the legal advisor, this jurisdictional problem primarily concerns Investigation Files on persons (covering 1.5 million persons in 1985) and provincial motor vehicle databases (containing 4.4 million registrations in 1985) that are located in provincial computers and accessible through CPIC. There is no jurisdictional problem for the Privacy Commissioner for Investigation Files entered in CPIC by the RCMP acting as a local or provincial police force, or for the major category of Identification Files (containing 2.9 million criminal records in 1985) maintained on CPIC by the RCMP.[32] But a significant percentage of Investigation Files contain information placed in the CPIC system by municipal police agencies across Canada, especially the large metropolitan police forces (excluding Quebec).

The legal advisor to the Privacy Commissioner also expressed the view that amending the Privacy Act to give the Commissioner the right to investigate those parts of the CPIC system which, in his view, are beyond the Privacy Commissioner's jurisdiction, will require consultations with the provinces to resolve potential constitutional problems.

The Committee's view is that the concerns raised about the Privacy Commissioner's jurisdiction over CPIC should not be allowed to impair his oversight role with respect to this sensitive and ubiquitous personal information system. The practical realities are that the RCMP operates the CPIC system and controls policy for its use, and federal taxpayers alone finance its operation. It is arguable that all personal information that enters the CPIC system is under the control of the RCMP for all practical purposes and should thus be regarded as being subject to the Privacy Act.

The Privacy Commissioner expressed the following opinion to the Committee: "If it would give some sense of security that the information in CPIC will not be abused, I think perhaps the Privacy Act could be changed to make specific our involvement, our jurisdiction."[33] The Committee is of the opinion that any ambiguities on this sensitive matter should be clarified by an Amendment to the Act, following negotiations with the appropriate provincial authorities. The Committee also notes that the various exemptions under the Privacy Act, including section 19(1) covering personal information obtained in confidence from the government of a province or an institution thereof and section 22 on law enforcement and investigatory data, would provide the necessary protection of CPIC information.

By noting its concern about CPIC, the Committee does not intend to suggest that it is the only data base of this type which merits attentive and continuing oversight by the Privacy Commissioner. Other relevant systems include the Automated Criminal Intelligence System (ACIIS), the Police Information Retrieval System (PIRS), the Automated Intelligence

Drug System (AIDS), and the Canadian Security Intelligence Service Records.[34] The problem is that the general public knows relatively little about any of these automated systems, and there is no evident external oversight of their operations for purposes of data protection.

Recommendations:

5.17 The Committee recommends that the Privacy Act be amended to specify that all personal data stored in the Canadian Police Information Centre are fully subject to the requirements of the Privacy Act.

5.18 The Committee further recommends that the Privacy Commissioner evaluate and audit the policies and practices of the CPIC system, and other comparable automated data bases, in order to ensure that the privacy interests of individual Canadians are being adequately protected.

5. Electronic Surveillance

One of the newest forms of invasion of personal privacy in the 1980s involves the electronic surveillance of employees by some combination of computers, cameras, and telecommunication devices. The Privacy Commissioner pointed out in his brief to the Committee that "Privacy protection in the workplace is an issue of quickly growing concern, a quintessential issue of the times and technology. Electronic monitoring or surveillance in the federal workplace -- or anywhere else -- poses a challenge to privacy protection beyond the present reach of the Privacy Act."[35]

Since electronic monitoring involves various aspects of personal privacy, it is necessary to distinguish between physical privacy and data protection issues and to tie electronic surveillance to data protection. The Canadian Privacy Act is in fact a data protection statute in the sense that it deals with the challenges posed to individual privacy by the collection, use, storage, and dissemination of personal data. But the law does not, for example, regulate wiretapping or invasion of privacy through the use of cameras or sound recording

devices. At present, section 3 explicitly covers the fingerprints and blood type of an individual. Moreover, the definition of personal information in section 3 of the Privacy Act covers "information about an identifiable individual that is recorded in any form..." Thus it is possible that videotapes, urine specimens, photographs, tape recordings, and electronically-recorded personal data are covered, especially when they are recorded as personal data.

Electronic surveillance, in this context, in fact involves the collection of personal data on employees' use of computers to perform their work and also the use of computers to produce profiles of employees for various purposes. To the extent that electronic surveillance involves the collection and storage of personal data, the problem indeed represents a data protection issue; accordingly, it clearly should be brought under the umbrella of the Privacy Act and should be subject to the investigatory powers of the Privacy Commissioner. With respect to the problem of electronic surveillance, the Commissioner noted that "It is at least an anomaly that someone called the Privacy Commissioner can speak out against one kind of breach of privacy but has no mandate to speak out against, much less prevent, breaches which are different only in method and may in fact be much more insidious."[36] It is apparent to the Committee that clarifications of the Privacy Act are in order.

The best explored examples of electronic surveillance to date concern airline reservations clerks, who work in an environment in which their every activity and conversation at a work station is monitored. At the end of each day, a profile of an individual's productivity is produced and compared to the norm. This technology may illustrate the extent to which innovations of this sort can have both positive and negative consequences.[31] Other sources of monitoring noted by the Privacy Commissioner include the use of telephones, video cameras, security and locator systems, computer terminals, parabolic microphones, and beepers and tonal pagers.[38]

One basic problem is that electronic surveillance or monitoring is often being introduced without consultation with the relevant employee groups and without taking into account the privacy interests of individuals and how these can be best protected in a new technological environment. All employees should have the right to consent to work in a heavily-monitored environment and to be consulted about the uses of data derived from any surveillance process. The discussion should not be what the Privacy Commissioner termed a "one-sided combat" between employer and employee.[39] There will clearly be job conditions in which security needs dictate a high level of monitoring, and others in which electronic surveillance is a dramatic form of overkill in terms of protecting human rights.

Electronic monitoring or surveillance in federal institutions and in the federally-regulated workplace poses a challenge to privacy protection beyond the present reach of the Privacy Act. According to the Privacy Commissioner, the present relationship between the Protection of Privacy Act, (a 1974 law, incorporated in the Criminal Code, designed to control the use of wiretapping), and the Privacy Act is untidy and unsatisfactory. For example, it would obviously be difficult for any person to distinguish between the two statutes by their titles.[40] Privacy protection against electronic monitoring and surveillance is not explicitly contemplated in the Privacy Act.[41]

The Committee wishes to encourage the development of the Privacy Act into a broad-based vehicle for protecting a wide range of privacy rights claimed by residents of this country. No longer should the Act remain solely a data protection statute. Canada is rapidly becoming an Information Society; therefore, it is vital that additional statutory protections for the privacy of Canadians be recognized under the umbrella of the Privacy Act.

Recommendations:

7.1 The Committee recommends that the definition of "personal information" in section 3 of the Privacy Act be broadened to include all

types of electronic surveillance that involve the collection of personal data in any form. To this end, videotapes, urine specimens, photographs, and tape recordings about an identifiable individual should be added explicitly to the list of "personal information" under section 3.

7.2 The Committee recommends that the Privacy Commissioner be explicitly empowered in the Privacy Act to monitor relevant developments in surveillance practices and to investigate complaints about these aspects of electronic monitoring and surveillance in the federal government, crown corporations, and in the federally-regulated workplace.

6. Urinalysis for Drug Testing and the Use of the Polygraph

As noted above in our discussion of electronic surveillance in the federal workplace, many new technological developments result in the collection and storage of personal data pertaining to individuals; therefore, they are subject to the Privacy Act. This is true of the use of polygraphs in employment interviews and security screening and the use of urinalysis as a method for drug testing. Both practices raise fundamental issues for the protection of privacy and for data protection.

Since the Privacy Act is a data protection law, it is appropriate for the use of such novel practices to be subject to the legislation and to the oversight of the Privacy Commissioner through self-initiated investigations and the receipt of complaints from concerned individuals. Scrutiny of proposals to use the polygraph and urinalysis should permit a careful analysis, by informed persons, of the privacy interests that are at stake in specific situations. It is possible that the Commissioner may need to make various recommendations to Parliament to cope with these emerging problems.

There are various proposals to introduce drug testing programs for certain federal employees, such as members of the Armed Forces, inmates in federal prisons, and applicants for employment with Air Canada and Canadian National Railways.[42] The Committee notes that the Department of National Defence and Correctional Services Canada have

plans and programs to conduct widespread compulsory drug testing, relying on the use of urinalysis in particular. It is also aware that a Quebec Superior Court judge ruled against such testing in the Cowansville prison of Correctional Services Canada on August 14, 1986 on the basis of the Canadian Charter of Rights and Freedoms.[43]

The Committee acknowledges as a general matter that some high risk positions may require drug testing as a periodic, and even continuing, part of the employment process. The crucial variable is that such testing has to have some meaningful and reasonable connection to the task or problem in question. The Committee considers it unlikely that uniform, blanket testing of all applicants for employment or all employees would be necessary or desirable.

The Committee recognizes that the results of urinalysis and polygraph tests are already subject to the Privacy Act, if the information is collected by an institution subject to the Act. But these practices pose such fundamental challenges to personal privacy that they merit explicit coverage in the legislation.

Recommendation:

7.3 The Committee recommends that those aspects of the use of the polygraph and of urinalysis that involve the collection and use of personal data be fully subject to the Privacy Act and to the supervisory oversight of the Privacy Commissioner. His jurisdiction should extend to federal government institutions, crown corporations, and the federally-regulated private sector.

Conclusion

The critical point to be derived from the discussion of these specific issues is that privacy and data protection legislation sets the context in which new technologies for criminal justice are introduced.

1. Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs, Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, 97th Congress, 2nd Session, 15-16 December 1982 (Washington, DC: Government Printing Office, 1983), pp. 1-2

2. U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy. Washington, D.C., June, 1986, OTA-CIT-296).

3. Annual Report, Privacy Commissioner 1985-86 (Ottawa, 1986), p. 7. See also Minutes of Proceedings and Evidence of the Standing Committee on Justice and Solicitor General, Issue No. 11 (May 13, 1986): 6-7 (Hereafter cited as Hearings).

4. Ibid., pp. 7-8; see James Richardson and Sons v. Minister of National Revenue, (1984) 1 S.C.R. 614.

5. See Department of Justice, Information Law and Privacy Section, Communiqué, No. 6 (June, 1984), p. 10.

6. Annual Report. Privacy Commissioner 1985-86, p. 7.

7. Treasury Board Canada, "Report on Data-Matching, May 3, 1985." The President of the Treasury Board made this report available during his appearance before the Committee on May 6, 1986.

8. Hearings, 8: 13, 24.

9. This paragraph is based on David H. Flaherty, The Origins and Development of Social Insurance Numbers in Canada (Department of Justice, Ottawa, 1981), chapter 6. This study was prepared for the Privacy Commissioner.

10. Privacy Commissioner, Report of the Privacy Commissioner on the Use of the Social Insurance Number (Department of Justice, Ottawa, 1981).

11. Annual Report, Privacy Commissioner, 1985-86, p. 44.

12. See D.B. Scott, "The Wages of Sin", The Financial Post Magazine, October 1, 1985, pp. 36b-36f.

13. Flaherty, The Origins and Development of Social Insurance Numbers in Canada, p. 182.

14. Annual Report. Privacy Commissioner 1985-86, p. 8.

15. See the list in ibid., p. 8. The inclusion in the list of such diverse activities as race track supervision, student loans, and the Canada Wheat Board suggests that Parliament should also review existing uses.

16. Ibid., pp. 8, 9.

17. U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy, especially pp. 111-12.

18. House of Commons, Bill C-535, An Act to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to government files containing personal information relating to themselves, May 2, 1980, section 9.

19. Bill C-537, An Act respecting the use of Social Insurance Numbers, May 2, 1980 (Hnatshyn); Bill C-586, An Act respecting the use of Social Insurance Numbers, May 2, 1980 (Gamble); Bill C-245, An Act respecting the use of Social Insurance Numbers, June 27, 1985 (Stackhouse); Bill C-236, An Act respecting the use of Social Insurance Numbers, October 21, 1986 (stackhouse). The language of the three bills is identical, except for the addition of section 3(1) to the 1985 bill, prohibiting any "person, organization, group or body that is not a federal body" from requesting any person to disclose his Social Insurance Number.

20. Canadian Bar Association, National (September, 1986), 1986 Annual Meeting, Resolution No. 2.

21. La Ligue des Droits et Libertés, Press Release, Montreal, Dec. 10, 1986.

22. This section is based on section 7 of U.S. Privacy Act of 1974.

23. The concept of exempt banks originated under Part IV of the Canadian Human Rights Act of 1977.

24. One of the ironies of the Privacy Commissioner's systematic examination of all exempt banks is that he is "unable to examine the documents which established the basis upon which the Governor-in-Council closed the banks because these documents are confidences of the Queen's Privy Council." (Annual Report, Privacy Commissioner, 1985-86, p. 23).

25. President of the Treasury Board to the Chairman of the Standing Committee on Justice and Solicitor General, Nov. 6, 1986. The remaining exempt banks are held by National Defence, Privy Council Office, Revenue Canada, and the RCMP.

26. Re Ternette and Solicitor General of Canada, (1984) 10 D.L.R. (4th) 587. Details are from Annual Report, Privacy Commissioner, 1985-86, pp. 21-3, 54.

27. Re Ternette and Solicitor General of Canada, (1984) 10 D.L.R. (4th) 587

28. Annual Report, Privacy Commissioner, 1985–86, p. 23.

29. The U.S. government does allow "exempt" systems to exist under the Privacy Act of 1974, but individuals may seek access to their records in them. Of over 73,000 access requests to exempt systems in 1982, only one percent were totally denied (Oversight of the Privacy Act of 1974, p. 60).

30. Hearings, 11: 30–1; 20: 19.

31. Further details concerning CPIC are available in David H. Flaherty, "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police Information Centre," University of Toronto Law Journal, XXXVI (1986), 116–48.

32. The data on the size of CPIC files is from Flaherty, "Protecting Privacy in Police Information Systems," pp. 146–7.

33. Hearings, 11: 25.

34. See the references to these data bases in Canada, Personal Information Index 1985 (Ottawa, 1985), pp. 27–2. 85–2, and 85–3.

35. Annual Report. Privacy Commissioner 1985–86 (Ottawa, 1986), p. 9.

36. Ibid, p. 10.

37. For details of this practice and expressions of concern by organized labour in southern Alberta, see Peter Lowrey, "Messages give unions Big Brother visions," Calgary Herald, Oct. 20, 1986; and, more generally, Wilfred List, "Electronic monitoring sparks new debate in the workplace," The Globe and Mail, Sept. 22, 1986, p. B4.

38. Annual Report, Privacy Commissioner, 1985–86.

39. Ibid.

40. In a related development, the British Columbia Police Commission, in a report to the provincial Attorney General, has urged the federal government to amend the Protection of Privacy Act to control the use of video surveillance of private conduct by police in Canada (The Globe and Mail, Jan. 14, 1987, p. A4). Earlier in the year, the Deputy Chief of the Niagara Regional Police and the Canadian Civil Liberties Association had lobbied the Solicitor General of Ontario to the same end (ibid., March 7, 1986).

41. For a very timely study of the Protection of Privacy Act, see Law Reform Commission of Canada, Electronic Surveillance (Working Paper 47, Ottawa, 1986).

42. On drug testing by the Armed Forces, see The Globe and Mail, Aug. 18, 1986, p. A3; for Correctional Services Canada, see ibid., Oct. 1, 1986, p. A11; for the CNR, see ibid., Sept. 9, 1986, p. A8. In June, 1986 the Office of the Judge Advocate General, Department of National Defence, submitted an eighteen page document entitled, "Canadian Forces Proposed Urinalysis Programme," to the Standing Joint Committee of the Senate and of the House of Commons on Regulations and Other Statutory Instruments. The Commissioner of Correctional Services Canada had correspondence on the same subject with the same Committee in the spring of 1986.

43. Jean-Pierre Dion v. Attorney General of Canada and Correctional Services Canada, Quebec Superior Court, Aug. 18, 1986, reported at (1986) R.J.Q. (C.S.) 2196.

Droit, procédure pénale et technologie[1]

par

Jean-Paul Brodeur, Ph.D. (Philo)
Professeur
Ecole de criminologie, Université de Montréal

Le thème dont nous devons traiter est celui des répercussions du recours à de nouvelles technologies sur la procédure pénale et sur les droits de la personne. Au lieu de présenter une série de constats, nous avons choisi de soulever un ensemble de questions qui interrogent la nature des transformations qui résulteront de l'introduction de technologies nouvelles dans le champs pénal. Notre exposé comporte trois parties. Nous allons d'abord articuler un paradoxe qui concerne le droit à la vie privée. Ensuite, nous discuterons un effet majeur de l'introduction des nouvelles technologies, à savoir un déclin possible de l'étape proprement judiciaire du processus pénal. Dans une troisième partie, nous aborderons des problèmes spécifiques qui se posent au niveau des opérations policières, à celui de l'imposition des sentences et, finalement, au niveau correctionnel. Nous dirons quelques mots en conclusion de la puissance de la technologie d'engendrer l'illusion d'un progrès dans la résolution des problèmes qui affligent le système pénal, alors qu'en réalité nous progressons peu.

---

(1) Ce texte a été présenté dans le cadre du XXXVIII^{e} Cours international de criminologie, qui s'est donné à Montréal en août 1987. Je n'ai pas tenté de transformer ce qui fut une présentation orale en un article pour une revue scientifique. Les références à la littérature académique sur les matières dont j'ai traité sont donc peu nombreuses, comme c'est habituellement le cas lors d'une intervention verbale.

1. Droit à la vie privée ou droit à la vérité?

Le droit à la vie privée fait en apparence l'objet d'un consensus. En réalité, il fait l'objet de violations si systématiques qu'on peut se demander si la vie privée est autre chose que la vie fictive (voir à cet égard Brodeur, 1983 et 1984; Laudon, 1986 et Marx, 1985). Au cours d'un colloque qui se tint en 1972, M. Claude Forget, qui occupait alors des fonctions de sous-ministre dans le gouvernement du Québec, adopta une position qui ne put manquer d'apparaître provocante. Nous citerons un extrait de son intervention:

> En résumé, le prétendu "droit à la vie privée" est un produit de l'imagination. Nous ne pouvons reconnaître à cette notion aucun titre à nous servir de principe pour normer les relations interpersonnelles ou contractuelles, ou pour régler les relations entre l'individu et l'État. Affirmer cela n'équivaut pas à rejeter le droit de propriété privée ou à prétendre que l'on peut répandre avec impunité des renseignements qui sont faux. Notre affirmation implique cependant que les personnes, les institutions et l'État avec qui nous entrons en relation portent un intérêt vital à notre vie privée et qu'il n'y a en principe aucune raison de bloquer leur accès à l'information qu'ils désirent obtenir. En d'autres mots, et pour dire la chose sous une forme excessive, avant qu'une personne ne soit accusée d'une infraction criminelle et jusqu'à ce qu'elle le soit, cette personne est contrainte de s'incriminer elle-même.
>
> Si l'on est contraint d'autoriser un accès général à des informations personnelles accumulées dans des banques de données, il devient impérieux que les données ainsi accumulées soient un portrait exact de la réalité. Le droit à ce que les renseignements qui nous concernent soient véridiques est dans mon opinion beaucoup plus important que le droit à la vie privée. (Nous traduisons)

La position prise par M. Forget est trop intransigeante pour être, au plan des principes, défendable (Les dossiers médicaux et psychiatriques de tous les patients devraient-ils être publics? Ce n'est là qu'une des multiples questions que soulève la position de M. Forget). Au plan de la réalité, il est cependant possible qu'une grande partie du programme qu'il esquisse soit en fait déjà réalisée. En outre, le problème qu'il soulève est d'une saisissante actualité. En effet, on sait d'une part que toute vérification des renseignements accumulés dans une banque de données judiciaires révèle un taux élevé d'erreurs (ce taux se situe aux États-Unis autour de 50%; voir, Slade et Biddle, 1982). On sait également que plusieurs des technologies utilisées pour effectuer des enquêtes criminelles ne sont pas fiables, le cas le plus notoire étant celui du détecteur de mensonge. Dans la mesure, encore considérable, où une société revendique le droit de ses membres à la vie privée, la cueillette de renseignements personnels rencontre des résistances et elle doit en conséquence souvent s'effectuer sur un mode clandestin. Or, le caractère occulte et détourné de cette pénétration de la vie privée est préjudiciable à l'examen de la véracité des renseignements accumulés par des moyens technologiques et autres. Cette affirmation peut être illustrée par un exemple qui ne relève pas de la technologie proprement dite mais qui s'applique sans difficulté à celle-ci. On soupçonne avec raison qu'une partie importante des renseignements transmis par des informateurs à la solde des services policiers est inexacte ou même carrément fausse. Cependant, comme le travail des sources policières humaines s'effectue sous le couvert d'une impénétrable mascarade de confidentialité, l'évaluation de la véracité des renseignements qui proviennent des indicateurs de police est extrêmement lacunaire. Le même constat s'applique à l'accumulation de renseignements à l'aide de sources techniques, dans la mesure où elle se produit également de manière dissimulée.

Il semble donc que nous soyons conduits au dilemme suivant. Nous pouvons d'une part continuer de résister farouchement à la légalisation de l'infiltration de notre vie non publique (ce dernier terme a une application plus large que la notion de "vie privée", qui connote la "vie intime"), mais c'est au prix d'un refoulement de cette infiltration dans une clandestinité qui fait obstacle à l'exercice d'un contrôle sur la validité des renseignements colligés. D'autre part, nous pouvons choisir de nous donner les moyens d'effectuer ce contrôle, mais ce sera alors au prix d'accorder une sanction légale à l'érosion de notre vie non publique. Jusqu'ici, il semble que les sociétés occidentales aient continûment choisi la première branche de ce dilemme, à savoir la résistance, au nom du droit à la vie privée, à l'invasion technologique de nos activités non publiques. Au regard de l'ascension en fait irrésistible des technologies de surveillance et de renseignement, il serait peut-être opportun de réévaluer nos choix et de nous demander si nous ne nous obstinons pas à défendre un bastion dont les murs depuis longtemps abattus laissent pénétrer parmi nous des intrus dont nous nous gardons à tort de voir le visage.

2. Le judiciaire dans l'étau

Avant d'avancer notre thèse sur les répercussions de la technologie sur la procédure judiciaire, nous proposons d'établir une double distinction, pour ce qui est de la technologie. Première distinction: une technologie peut être polyvalente ou spécifique. L'ordinateur est le prototype de l'instrument technologique polyvalent: il peut être utilisé dans tout domaine où s'effectue du traitement de données. Le polygraphe (ou détecteur de mensonge) est un instrument dont la vocation est plus spécifique et dont usage est fait au cours d'une enquête, le terme d'enquête étant ici pris dans son sens large.

Seconde distinction: une technologie peut être ostensive ou clandestine. Certains systèmes d'alarme constituent de bon exemples d'une technologie ostensible. Loin de dissimuler sa présence, une technologie ostensible s'affiche et produit une partie de ses effets de dissuasion par sa visibilité. C'est ainsi que la porte de plusieurs établissements commerciaux se parent d'une collant qui annonce que l'établissement est protégé par un dispositif d'alarme. Une technologie clandestine opère au contraire de façon dissimulée. Les instruments qui sont utilisés pour intercepter les communications entre des personnes à leur insu appartiennent au champ de la technologie clandestine.

Notre thèse générale sur les répercussions de la technologie s'énonce comme suit: l'effet majeur de l'application de la technologie au domaine du droit criminel sera de restreindre de façon croissante la place et l'importance de la composante judiciaire au sein du système pénal. Cet effet est déjà sensible et tout ce que nous ignorons est l'ampleur qu'il prendra. Il est le produit de deux déplacements.

2.1 Un système qui se développe en ses extrémités

Les technologies qui ont une application spécifique dans le domaine pénal sont en grande partie des technologies de protection, de surveillance et de détection. La cible de ces instruments technologiques est d'une double nature. Cette cible peut d'abord être constituée par le contrevenant potentiel ou encore le contrevenant recherché. Dans ce cas, la technologie spécifiquement pénale est surtout utilisée par la police, lorsqu'elle cherche à prévenir le crime ou à appréhender ceux qui sont présumés être les auteurs de délits. La cible de cette technologie peut ensuite être le contrevenant, après qu'il aura été reconnu coupable et qu'une

sentence lui aura été imposée. L'instrument technologique servira à l'administration de la sentence et il sera utilisé par les services correctionnels.

Cette importation d'instruments technologiques dans les deux extrémités du système n'aura pas seulement pour effet que la masse des opérations du système pénal se concentreront dans les étapes qui précèdent ou qui suivent la phase proprement judiciaire. La signification profonde de ce renforcement technologique des extrémités du système est qu'il constitue un processus d'érosion qui s'approprie progressivement des fonctions traditionnellement dévolues à l'institution judiciaire. Le processus judiciaire comporte en théorie deux phases: la phase adjudicatoire, pendant laquelle le tribunal décide de l'innocence ou de la culpabilité du contrevenant, et la phase sentencielle, au cours de laquelle le tribunal impose une sanction. Or, les moyens technologiques dont dispose la police lui permettent de construire une preuve qui est, à tout le moins en apparence, suffisamment accablante pour que le contrevenant passe aux aveux et dépose un plaidoyer de culpabilité. Certains de ces moyens technologiques, comme l'écoute électronique, peuvent produire des éléments de preuve qui sont sous certaines conditions admissibles devant le tribunal. Certains autres, comme le détecteur de mensonge, ne produisent pas d'éléments admissibles en preuve devant le tribunal. Il n'en reste pas moins que le détecteur de mensonge est utilisé par la police et qu'il produit parfois des effets d'intimidation décisifs à l'égard de la reconnaissance par un suspect de sa culpabilité. La montée toujours croissante du nombre de plaidoyers de culpabilité a diminuée très considérablement l'importance de la phase adjudicatoire (le procès) du processus judiciaire. A toutes fins pratiques, le procès s'effectue avant que le contrevenant ne parvienne devant le tribunal, où son rôle se borne à reconnaître sa culpabilité et à recevoir une sanction. Cette érosion de l'adjudication par le tribunal de la culpabilité ou de l'innocence ne peut être qu'amplifiée par les technologies de surveillance et de détection dont dispose la police.

Subverti par la police dans sa composante adjudicatoire, le processus judiciaire n'est pas moins vulnérable dans sa composante sentencielle. Les avancées de la technologie permettent d'envisager de nouveaux types de sanctions, comme l'assignation à domicile sous surveillance électronique (voir Landreville, 1987), et de nouveaux types d'interventions, comme la lobotomie au rayon laser (voir Vollman, 1987). Il est indéniable que le juge conserve le pouvoir d'imposer ou de s'abstenir d'imposer un type de sanction et qu'il jouit parfois d'un droit de regard sur les interventions qui sont effectuées dans le cadre de l'administration des sentences (ce droit de regard est très limité). Il n'en reste pas moins que le processus sentenciel opère à l'intérieur d'une gamme d'options qui est entièrement déterminée de l'extérieur par les services correctionnels, en fonction de bouleversements technologiques dont la magistrature connaît mal la nature. On pourrait élaborer une fabulation à la Aldous Huxley sur le meilleur des mondes d'une justice pénale qui aurait été amputée de sa composante judiciaire: atterrés par les multiples enregistrements de leurs délits (écoute électronique, films, caméras vidéo, photographies au téléobjectif, tests d'urine, etc.), tous les contrevenants plaideraient coupables et seraient confiés par un ordinateur aux entreprises des services correctionnels.

Nous n'en sommes pas là et il faut souhaiter que nous n'y parvenions pas. Nous terminerons cette description d'un premier déplacement effectué par la technologie par deux brèves remarques. Ce déplacement du poids technologique du système pénal vers les extrémités de ce système est favorisé par deux facteurs. La composante judiciaire du système pénal est la plus ritualisée et elle est dans cette mesure la plus résistante au changement. Il est saisissant de contraster la rapidité avec laquelle les composantes policière et correctionnelle du système pénal se sont appropriées les nouvelles technologies (à commencer par l'ordinateur), à la très lente pénétration de la technologie de pointe dans le monde

judiciaire. L'une des innovations mentionnées par le Ministre de la Justice du Québec, lors de son allocution au XXXVIII^{e} Cours international de criminologie, est l'obtention de mandats d'arrestation par téléphone. On se prend à souhaiter que le monde judiciaire fasse preuve de plus d'audace dans son recours à la technologie et qu'il regarde au-delà du téléphone. Cette timidité trouve peut-être son origine dans la formation qui est donnée aux praticiens du droit. C'est là un second facteur qui favorise les transferts de technologie vers les extrémités du système pénal. Le rapport du Groupe consultatif sur la recherche et les études en droit (1984) a souligné à quel point la formation donnée aux étudiants en droit était étroite et praticienne. Nous avons pu à maintes occasions constater que la simple mention du mot "statistique" offusquait les praticiens du droit. Or une aversion pour la recherche en général et pour la recherche quantitative en particulier n'est pas de nature à nourrir un intérêt pour les développements de pointe en technologie, qui sont la plupart du temps liés de près ou de loin à des progrès dans la recherche mathématisée.

2.2 Un système de justice fracturé

Les remarques que nous avons faites sur la pénétration technologique dans les secteurs policiers et correctionnels s'appliquent également au développement de plus en plus accentué d'un réseau de justice privatisée. En effet, non seulement les agences de sécurité privées et les entreprises qui s'investissent de façon croissante dans la privatisation d'une partie du secteur correctionnel sont-elles voracement consommatrices des nouvelles technologies pénales, mais il faut souligner que la production même de ces instruments technologiques est un monopole de l'entreprise privée. C'est d'ailleurs les employés du secteur privé qui sont habituellement les

premiers cobayes pour la mise à l'essai d'une nouvelle technique, comme les tests d'urine. On constate ensuite que, malgré les déficiences reconnues d'un instrument d'enquête comme le polygraphe, ils continuent d'être massivement utilisés par l'entreprise privée. C'est, croyons-nous, un leurre de penser que nous contrôlons de façon suffisante l'usage des nouvelles technologies pénales. Ce leurre est entretenu en partie par l'expression mystifiante d'instrument technologique que nous utilisons fréquemment pour désigner les technologies pénales. Cette notion d'instrumentalité est propre à engendrer la croyance que nous disposons de la technologie selon notre volonté et nos fins. Or, c'est souvent l'inverse qui est vrai, la technologie provoquant dans un domaine des restructurations qui n'avaient pas été anticipées. Ainsi, pour prendre un exemple banal, la motorisation des services de police publics a complètement transformé le type de relation qui prévalait entre la police et la collectivité. C'est pourquoi on a largement tort de penser qu'être investi par la technologie se réduit à disposer d'un ensemble relativement inerte d'outils et d'instruments. La technologie est par nature un pouvoir et, comme tout pouvoir, elle possède sa dynamique propre. Si cette dynamique se déploie davantage au sein du secteur privé ou privatisé de la justice que dans son secteur public, on peut prévoir que les modes selon lesquels le pouvoir de la technologie s'exerce dans le secteur privé va faire modèle et que les traits de ce dispositif vont éventuellement essaimer dans le secteur public.

Nous n'avons pas le temps de nous attarder longuement sur tous les traits qui définissent l'exercice privé de la justice. Il est néanmoins deux de ces traits, qui ont fait l'objet d'analyses de la part de Shearing et Stenning (1981, 1985 et 1987), et qu'il nous apparaît opportun de discuter. En principe, les pouvoirs des agences de sécurité privées ne sont guère plus étendus que ceux des citoyens ordinaires et sont bien inférieurs à ceux des agents de la paix. En pratique, cependant, le pouvoir des membres de ces agences

s'égalent à ceux des agents de la paix, et leur sont parfois même supérieurs. Comme le remarquent Shearing et Stenning (1981), l'esprit de nos lois consiste à protéger les membres de notre société contre des mesures coercitives, qui leur seraient appliquées en dépit de leur volonté. Cependant, dès lors, qu'une personne donne son consentement à faire l'objet d'une mesure, cette personne renonce en grande partie à la protection de ses droits, qui lui est octroyée par la loi. Ainsi, lorsqu'une personne consent à être interrogée par un enquêteur au service d'une compagnie privée, et même à se soumettre à un test conduit à l'aide d'un détecteur de mensonge, elle répudie de son propre chef la protection apportée par la loi contre les arrestations illégales et contre ce qui est effectué à la suite d'une arrestation illégale. L'exercice privé du contrôle se produit donc sur le mode du consentement, alors que son exercice public est structuré par une relation adversative, dont le symbole le plus visible est l'affrontement entre un représentant du Ministère public et le défenseur de l'accusé au cours de l'étape judiciaire du processus pénal. Dans la foulée de notre hypothèse sur la possibilité que le secteur de la justice privée vienne par suite de son renforcement technologique coloniser le secteur public, on pourrait inférer que le contrôle social trouvera progressivement son assise dans un consentement des membres d'une société à être surveillés et éventuellement sanctionnés, ainsi que dans une cession volontaire, par ces mêmes personnes, de leurs droits. Nous verrons plus loin que cette conclusion n'a rien de spéculatif et que ce que nous désignons comme une inférence logique est déjà largement réalisé dans les faits.

Le second trait du contrôle social, qui est pris en charge par l'entreprise privée, est son caractère purement utilitaire. La meilleure façon d'expliquer ce trait est de l'illustrer par un exemple. Si une banque découvre qu'un de ses employés est coupable d'une fraude et qu'il pourrait éventuellement rembourser les argents détournés en acceptant de les considérer comme un prêt à intérêt

personnel élevé, il est tout à fait possible que cette banque règle l'affaire par le moyen d'un prêt à son employé, plutôt que par la voie d'une dénonciation à la police. Il faut insister sur le fait que l'objectif moral de dénoncer des comportements comme la fraude est écarté au profit de limiter les pertes de l'entreprise (la banque ne profite pas financièrement de l'incarcération de son employé). Le corollaire de cet utilitarisme est l'aspect informel et hautement discrétionnaire de ce mode de règlement d'un ensemble des conflits qui tomberaient normalement sous la juridiction du droit pénal public. Un ouvrage édité par Shearing et Stenning en 1987 a montré l'importance très considérable de ce dispositif privé de régulation sociale. Il en suit d'une part qu'une très grande partie de la délinquance contre les biens échappe à la prise de la justice publique. Il pourrait également en découler que par un processus d'essaimage des traits de la justice privée vers la justice publique, cette dernière se déstructure et que son exercice soit de moins en moins visible. Dans cette mesure, elle pourrait se soustraire efficacement à l'obligation fondamentale de rendre un compte public de son opération.

Avant d'aborder la troisième partie de ce texte, nous formulerons brièvement la conclusion des analyses auxquelles nous venons de nous livrer. L'introduction croissante d'une technologie spécifiquement pénale risque de produire deux grands déplacements. D'une part la masse des opérations et des décisions qui sont effectuées dans le système de la justice pénale sera repoussée dans les deux composantes les moins procédurales du système pénal, à savoir les composantes policière et correctionnelle; d'autre part, l'innovation technologique va accentuer le poids des réseaux privés dans l'exercice du contrôle social. Ces deux déplacements, dont les effets sont déjà sensibles, vont accélérer le rétrécissement et l'obsolescence de la procédure judiciaire et des droits qu'elle est censée garantir.

3. Technologie pénale et effets localisés

Nous aborderons dans cette troisième partie la description d'effets plus localisés dans les trois principales composantes du système pénal, soient la police, les tribunaux et les services correctionnels. Nous ne nous étendrons que sur les effets qui concernent de façon plus particulière la police et les tribunaux.

3.1 Le contrôle judiciaire de la surveillance électronique exercée par la police

La surveillance électronique est sans doute l'aspect de la technologie pénale qui a le plus impressionné l'opinion publique et qui suscite les plus grands apeurements. Depuis 1974, l'écoute électronique est soumise au contrôle de la magistrature au Canada. Un agent de la paix qui se propose d'intercepter les communications verbales entre deux ou plusieurs personnes doit obtenir l'autorisation légale d'effectuer cette interception. Cette autorisation prend la forme d'un mandat décerné par un juge. Initialement, les membres du Service de sécurité de la Gendarmerie Royale du Canada étaient soustraits à l'obligation d'obtenir un mandat pour intercepter des communications préjudiciables à la sécurité nationale du Canada. Depuis la création en 1984 du Service canadien du renseignement de sécurité (SCRS), l'interception des communications aux fins de protéger la sécurité nationale est également soumise à un contrôle judiciaire.

Ce contrôle est-il efficace et est-il suffisant pour protéger les citoyens d'une intrusion policière indue dans leur vie personnelle? Nous pensons qu'il faut répondre par la négative à ces deux questions. Nous justifierons brièvement notre opinion.

3.1.1 La saturation de l'espace sensoriel

Il importe de souligner que la loi de 1974 qui est censée protéger la vie privée du citoyen n'est relative qu'à l'écoute électronique. Perpétuant un retard du droit sur le développement de la technologie, un document de travail sur l'écoute électronique, publié en 1986 par la Commission de réforme du droit du Canada, n'a pas jugé opportun de soumettre la surveillance électronique de nature vidéographique au contrôle de la loi. La fixation législative sur les techniques d'interception acoustiques est complètement désuète. On peut affirmer sans risque d'erreur que c'est maintenant tout l'espace sensoriel qui est quadrillé par la technologie de surveillance. Non seulement sommes-nous écoutés et observés, mais il existe maintenant des moyens techniques de surveillance et d'enquête, qui sont le prolongement de nos autres canaux sensoriels. Le détecteur de mensonge, qui vérifie la tension artérielle, le degré de sudation et le rythme des battements du coeur, est un mode d'auscultation qui se situe dans le prolongement du sens du toucher. Il existe également des modes de détection qui sont de nature olfactive (par exemple, des animaux dressés pour dépister diverses substances, comme de la drogue). Toute cette technologie opère dans un vide juridique, en dépit de "bavures" qui ont fait l'objet de maintes dénonciations (par exemple, l'installation de caméras dans les toilettes publiques). Pour l'essentiel, ces modes de surveillance opèrent sous le couvert de notre ignorance — lorsqu'il s'agit de technologie clandestine — ou avec notre consentement. Nous avons de cette façon consenti à la multiplication des points de surveillance vidéographique, sans prendre une conscience claire de ses conséquences au niveau de la protection des droits de notre assentiment à être surveillés.

3.1.2 L'autorisation mécanique

Dans un article publié en 1984, nous avons présenté le résultat de notre dépouillement des données relatives à l'écoute électronique au Canada, depuis la secode moitié de 1974 jusqu'en 1982. Pendant cette période, la police a présenté 5 239 demandes d'autorisation de se livrer à l'écoute électronique et n'a essuyé que 10 refus; elle a également demandé que les autorisations originelles soient prolongées dans 3 259 cas et n'a reçu que quatre refus. Nous avons vérifié si cette libéralité des magistrats contrôleurs s'était poursuivi après 1982. Elle s'est en vérité accentuée: les magistrats ne refusent les demandes qu'à titre tout à fait exceptionnel. De 1983 à 1986 seulement 3 demandes d'autorisation ont été refusées. Les juges exercent leur contrôle en ajoutant au mandat d'autorisation quelques conditions que la police doit respecter. Ces conditions sont pour l'essentiel relatives au respect de la confidentialité des communications entre un prévenu et son avocat. On retrouve la même tendance du côté des juges de la Cour fédérale qui ont juridiction en matière d'interception des communications — au sens large du terme, qui recouvre à la fois l'écoute électronique, l'ouverture du courrier et des perquisitions clandestines — par le SCRS. D'après les rapports annuels du Comité de surveillance des activités de renseignement de sécurité (CSARS), les magistrats de la Cour fédérale n'ont refusé aucune des demandes du SCRS, depuis sa création en 1984.

3.1.3 Le cas Atwal

Une explication qui est souvent apportée de l'acceptation sans faille par la magistrature des demandes de la police est que celles-ci ont fait l'objet d'une sélection préalable par les cadres

policiers. D'après cette interprétation, les cadres policiers rejettent eux-mêmes les requêtes déraisonnables ou mal fondées, de telle sorte que seules les demandes légitimes parviennent aux magistrats. Jusqu'à récemment, on ne pouvait se prononcer sur la justesse de cette explication, par manque complet d'informations pour l'évaluer. Le cas Atwal est venu jeter une lumière crue sur la procédure suivie par la police — en l'occurrence, le SCRS — pour obtenir l'autorisation d'intercepter des communications privées.

L'affaire Atwal fut révélée à l'opinion publique canadienne en janvier 1987 (voir The Globe and Mail, 8 janvier 1987). Voici brièvement l'histoire de cette cause maintenant célèbre. Par suite de l'explosion en vol en 1985 d'un avion d'Air India qui avait décollé d'un aéroport canadien, cette explosion extraînant la mort de plus de 300 personnes, les services policiers canadiens se sont livrés à une enquête pour découvrir les auteurs de cet attentat. Dans le cadre de cette enquête, le juge Heald de la Cour fédérale du Canada a accordé l'une des plus vastes autorisations pour intercepter les communications privées qui aient été octroyées au Canada depuis 1974. En conformité avec le mandat octroyé par le juge Heald, le SCRS a eu pouvoir d'installer un dispositif d'écoute électronique dans tous les locaux fréquentés par M. Atwal, de juillet 1985 à juillet 1986, y compris des édifices publics. Les communications entre M. Atwal et son avocat, Me David Gibbons, ont de cette façon été interceptées. Me Gibbons a appris qu'il était soumis à l'écoute électronique et il a entrepris de contester devant la Cour fédérale du Canada la légalité de l'autorisation conférée par le juge impliqué dans cette procédure. Il s'est trouvé que le magistrat devant lequel Me Gibbons a effectué sa contestation était celui-là même qui avait initialement autorisé l'interception de toutes les communications de M. Atwal, à savoir le juge Heald. De façon prévisible le juge Heald se donna raison contre les allégations de Me Gibbons et celui-ci fut débouté par la Cour, qui rendit sa décision dans un jugement longuement justifié.

Cette affaire connut son épilogue au mois de septembre 1987. Il fut alors révélé devant le tribunal que l'affidavit, dans lequel s'énonçait les motifs du SCRS pour soumettre M. Atwal à l'écoute électronique, était fondé sur des informations que le service de renseignement savait être fausses. Le procureur de la Couronne a alors retiré ses accusations contre M. Atwal.

Il faut noter que dans cette affaire toutes les instances de contrôle ont failli. Non seulement le juge a-t-il été la dupe d'agents du SCRC, mais même le CSARS déclarait dans son rapport annuel de 1986-1987 que:

> "Par suite de rapports dans les médias (notamment dans le Globe and Mail, Toronto, 8 janvier 1987), nous avons enquêté sur un cas particulier où les communications entre un avocat et son client avaient été interceptées. Nous sommes convaincu que, dans cette affaire, l'interception était justifiée pour des motifs de sécurité valables. Nous avons également noté que l'information acquise n'a été transmise à aucun autre organisme."

En dépit de ce que déclare le CSARS, qui s'accorde avec la décision du juge Heald, les "motifs de sécurité" sur lesquels s'appuyait la demande du SCRS pour intercepter les communications de M. Atwal n'étaient pas véridiques, et l'interception de ses communications avec son avocat n'étaient pas justifiées. Il est toutefois difficile de reprocher au juge Heald et au CSARS d'être parvenus à de mauvaises conclusions. Une conclusion obtenue à partir de prémisses délibérément faussées par des agents du SCRS pouvait difficilement être adéquate. On ne peut, sur la base de ce seul exemple, affirmer que la police extorque des mandats aux juges en leur présentant de fausses justifications. Nous estimons toutefois qu'il serait naïf de croire que le cas Atwal constitue la proverbiale bavure "isolée".

Il n'est pas en soi de relation de principe entre le recours à une technologie de surveillance et la présentation de fausses justifications pour obtenir l'autorisation d'utiliser une telle technologie. On peut aussi bien mentir pour obtenir un mandat d'arrestation que pour recevoir une autorisation de se livrer à l'écoute électronique. Le développement de la technologie va toutefois multiplier les occasions où les services policiers voudront se servir des nouveaux moyens technologiques. Si l'on persiste à soumettre l'utilisation de ces moyens à une procédure d'autorisation par la magistrature, les situations favorisant la transmission d'informations incorrectes se multiplieront également. À une procédure d'autorisation qui est déjà mécanique correspondra alors un contrôle tout à fait fictif.

3.2 Informatique et sentencing

Nous quitterons le domaine des relations entre la police et l'instance judiciaire pour ne traiter maintenant que des tribunaux en eux-mêmes. Il est possible qu'à brève échéance, les tribunaux soient le théâtre (ou la proie) de la télédiffusion de leurs séances. Il est un grand nombre d'autres applications de la technologie audiovisuelle dans l'opération des tribunaux, comme par exemple, le déroulement de procédures alors que les diverses parties impliquées (le juge, l'accusé et les témoins) sont dans des lieux différents.

Nous aimerions toutefois très brièvement traiter de deux applications de l'informatique au travail des tribunaux. La première de ces applications est déjà réalisée, à tout le moins dans le district judiciaire de Montréal. Il suffit de posséder le nom et la date de naissance d'une personne pour obtenir, au Greffe du Palais de justice de Montréal, tous les renseignements relatifs à

ses antécédents judiciaires. Ceux-ci font partie d'une banque de données à laquelle les citoyens ont juscu'ici un accès libre. Nous ne nous prononcerons pas sur l'opportunité de laisser un accès libre aux antécédents judiciaires des contrevenants. Il importe toutefois de souligner que cet accès libre à des informations qui peuvent avoir des conséquences préjudiciables à la capacité d'une personne d'occuper un emploi met en lumière l'impérieuse nécessité de s'assurer que les renseignements contenus dans ces banques de données sont exacts et n'attribuent pas à des personnes des antécédents judiciaires qui sont fictifs.

Il est une seconde application de l'informatique qui se révélera à long terme plus lourde de conséquences. Il n'existe, à l'heure actuelle, aucun programme de collecte systématique de données au Canada sur la nature des sentences imposées par les juges. Ces programmes sont en application dans plusieurs juridictions des États-Unis et il est probable qu'à la suite des recommandations de la Commission canadienne sur la détermination de la peine, de tels programmes soient implantés au Canada. Voici quel est l'enjeu de ces programmes. On sais qu'à peu près tous les pays occidentaux sont affligés d'un problème de surpopulation des prisons. Le but premier des programmes informatisés de cueillette de données sur les pratiques sentencielles n'est pas d'accumuler des statistiques qui décrivent la pratique des juges, mais d'établir un lien entre les pratiques sentencielles et la capacité d'accueil des établissements carcéraux. Lorsque l'on dispose de données fiables sur le nombre de sentences carcérales imposées par les juges et sur leur durée, il est relativement facile de programmer un ordinateur de manière à faire des projections sur le taux d'occupation des prisons dans le futur. Si ces projections révèlent que les tendances actuelles dans les pratiques sentencielles vont résulter dans une aggravation inacceptable du problème de la surpopulation des prisons, il est possible d'effectuer des exercices de simulation à partir de modèles hypothétiques qui intègrent diverses modifications aux pratiques courantes en matière de détermination des sentences.

L'établissement d'une mesure systématique des conséquences des sentences imposées par les tribunaux sur le volume des populations carcérales est non seulement inévitable en ces temps de contraintes budgétaires mais elle est également souhaitable. Le système pénal doit mettre un terme à son aveuglement sur les conséquences de son opération. L'utilisation des études projectives que nous venons d'esquisser soulève des questions qui ne manqueront pas d'être controversées et dont la solution pourrait entraîner des modifications considérables dans le processus de détermination des sentences. La question cruciale est de savoir quelle importance accorder à la disponibilité des ressources carcérales dans la détermination des sentences.

Les juges sont d'une part trop souvent insensibles à la carence des ressources carcérales et s'indignent à tort que les personnes qu'ils envoient en prison en ressortent par la porte arrière peu de temps après leur arrivée. La cause de ces remises en liberté qui sont parfois massives tient au problème de la surpopulation carcérale, dont, encore une fois, beaucoup de juges tiennent un compte insuffisant. Il convient d'autre part de signaler qu'asservir complètement la détermination des sentences à l'espace carcéral disponible équivaudrait à donner priorité à l'intendance sur la justice, ce qui est inacceptable. On devra trouver dans un futur très prochain un équilibre entre ces deux positions également excessives.

3.3 L'assignation à domicile sous surveillance électronique

L'une des prétendues solutions de rechange à l'incarcération qui est le plus souvent discutée de nos jours est l'assignation à domicile sous surveillance électronique. Cette mesure fait l'objet d'une discussion approfondie par Landreville (1987). Pierre Landreville a

en outre repris cette question lors du XXXVIII^{e} Cours international de criminologie. Nous n'en dirons nous-mêmes quelques mots que dans la mesure où nos remarques sur cette question serviront d'introduction à notre conclusion.

L'assignation à domicile sous surveillance électronique est considérée par plusieurs de ses défenseurs comme une façon de résoudre le problème de la surpopulation carcérale. Cet optimisme nous semble injustifié. Un examen de l'histoire de la pénologie depuis le XIX^{e} siècle nous enseigne que les solutions de rechange à l'incarcération n'ont pas été véritablement substituées à l'incarcération mais ont été utilisées pour produire une escalade répressive dans le champ des sanctions non carcérales. Il est donc prévisible que l'assignation à domicile remplacera plutôt des sentences de probation que des sentences d'incarcération.

On sait en second lieu que la surpopulation carcérale est attribuable à deux facteurs, soit le nombre de personnes incarcérées et la durée de leur incarcération. D'après le Rapport du Comité d'études sur les solutions de rechange à l'incarcération, le second facteur (la durée) est le facteur le plus déterminant dans la genèse du problème de la surpopulation carcérale. Or, l'assignation à domicile ne peut être imposée pour une période de temps substantielle (plusieurs années) et elle ne saurait être substituée à une longue période d'incarcération (plus de deux ans). Il est donc extrêmement douteux que son utilisation produise une décroissance sensible dans la population carcérale.

Ces remarques ne sont pas inattendues et plusieurs chercheurs les ont faites. D'où vient que l'assignation à domicile sous surveillance électronique suscite un tel engouement pour réduire le recours à l'incarcération? On pourrait en première part affirmer que le désarroi des administrateurs du système pénal les conduit à s'agripper à tout ce qui paraît flotter. Il est une autre réponse, que nous soumettrons en conclusion.

4. La puissance des illusions

Il existe une nouvelle technique pour découvrir si une personne a consommé de la drogue. Il s'agit de l'analyse d'urine, dont on fait maintenant un usage abusif. Cette technique est moins sûre qu'on le croit, mais elle produit des résultats qui sont plus fiables que les procédés antérieurs. Ce point n'intéressant pas le coeur de l'argument que nous voulons présenter, admettons provisoirement à titre d'hypothèse servant les fins de cette discussion, que l'analyse d'urine produit des résultats infaillibles et qu'elle évite complètement le problème des faux positifs.

Lors du XXXVIII^{e} Cours international de criminologie, un chercheur a présenté les résultats de tests d'urine effectués sur des contrevenants après qu'ils eurent été arrêtés par la police. Ces tests ont révélé qu'un pourcentage important de ces contrevenants avaient consommé de la drogue. Le chercheur concluait à l'existence d'une relation causale entre la consommation de drogue et la criminalité.

Imaginons qu'on intervienne au cours d'une "jam session" réunissant des musiciens rock et des musiciens de jazz, et qu'on les soumette à des tests d'urine. On peut raisonnablement prédire que les analyses d'urine vont révéler qu'un nombre élevé de ces musiciens ont consommé de la drogue, à tout le moins si l'on s'en remet au stéréotype populaire, qu'on peut également admettre à titre d'hypothèse. Même si le stéréotype populaire se trouvait confirmé par des analyses d'urine, se trouverait-il un chercheur pour affirmer de façon crédible que la consommation de drogue développe le talent musical? Une telle conclusion ne manquerait pas d'apparaître facétieuse.

Pourquoi établit-on alors sans autre explication une relation causale entre la consommation de drogue et la genèse de la délinquance? Non seulement cette assimilation entre une relation de co-occurence et une relation d'influence orientée dans un sens déterminée — c'est la drogue qui conduit à la délinquance et pas l'inverse — apparaît-elle gratuite quand on tente de l'établir dans d'autres champs que celui de l'explication de la criminalité, mais cette assimilation constitue une erreur méthodologique contre laquelle nous préviennent les manuels les plus élémentaires sur les procédures à suivre dans les recherches sur la délinquance. D'où vient que le chercheur qui utilise des tests d'urine est soudainement frappé d'amnésie par rapport à l'une des requêtes les plus élémentaires de la méthodologie?

Il est difficile de répondre à cette question en se limitant à déconstruire le processus rationnel d'inférence suivi par le chercheur. Il nous semble que d'autres facteurs que la rationalité interviennent pour produire ce type d'interprétation des résultats que révèlent les tests d'urine. Tout se passe en effet comme si la sûreté de la technologie utilisée pour déceler la consommation de stupédiants se propageait par irradiation. Au cours de cette bizarre pentecôte pour âmes crédules, les langues de feu voltigent de l'urinoir à la tête du chercheur et confèrent une mythique validité aux conclusions les plus arbitraires. De la même façon, la fascination exercée par les diverses panacées issues de la technologie est tellement puissante qu'elle paraît inhiber toute lucidité par rapport aux conséquences d'un recours systématique à ces expédients et produire l'illusion d'une avancée là où il n'y a qu'un recul.

RÉFÉRENCES

BRODEUR, J.-P. (1983).
High policing and low policing: remarks about the policing of political activities. Social Problems, Vol. 30, no. 5, June, p. 507-520.

BRODEUR, J.-P. (1984).
Policing: beyond 1984. Cahiers canadiens de sociologie, Vol. 9, no. 2, Printemps, p. 195-207.

CANADA (1986).
La surveillance électronique. Commission de réforme du droit du Canada, Document de travail 47. Ottawa: Commission de réforme du droit du Canada.

CANADA (1987).
Rapport de la Commission canadienne sur la détermination de la peine. Ottawa: Ministre des Approvisionnements et Services Canada.

COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT DE SÉCURITÉ (1986).
Rapport annuel: 1985-1986. Ottawa: Ministre des Approvisionnements et Services Canada.

COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT DE SÉCURITÉ (1987).
Rapport annuel: 1986-1987. Ottawa: Ministre des Approvisionnements et Services Canada.

GROUPE CONSULTATIF SUR LA RECHERCHE ET LES ÉTUDES EN DROIT (1984).
Le droit et le savoir. Rapport au Conseil de recherches en sciences humaines du Canada. Ottawa: Ministre des Approvisionnements et Services Canada.

LANDREVILLE, Pierre (1987).
Surveiller et prévenir. L'assignation à domicile sous surveillance électronique. Déviance et société, Vol. 11, no. 3, septembre, p. 253-269.

LAUDON, Kenneth (1986).
Dossier Society. Value Choices in the Design of National Information Systems. New York: Columbia University Press.

MARX, Gary (1985).
I'll be watching you. Reflections on the new surveillance. Dissent, Winter, p. 26-34.

QUÉBEC (1985).
Rapport du Comité d'étude sur les solutions de rechange à l'incarcération. Québec: Gouvernement du Québec, Ministère du Solliciteur général.

SHEARING, Clifford D., STENNING, Philip (1981).
Private security in Canada: some questions and answers, in W.T. McGrath et M. Mitchell (Ed.): The Police Function in Canada, p. 53-76. Toronto: Methuen. Traduit par J.-P. Brodeur. Criminologie, Vol. 17, no. 1, p. 59-89.

SHEARING, Clifford D., STENNING, Philip (1985).
From the Panopticon to Disneyworld: the development of discipline, in A.N. Doob et E.L. Greenspan (Ed.): Perspectives in Criminal Law: Essays in Honour of LL. J. Edwards, p. 335-348. Aurora, Ontario: Canadoan Law Books Ins. Traduit dans Actes, été 1987, no. 60, p. 27-33.

SHEARING, Clifford D., STENNING, Philip (Ed.) (1987).
Private Policing. Newbury Park, California: Sage Publ. Co.

SLADE, Margot, BIDDLE, Wayne (1982).
Is Big Brother prone to error?. New York Times, October 31st, section E, p. 7.

VOLLMAN, John J. (1987).
Neutering homicidal recidivists in juridictions without capital punishment. Unpublished paper presented during the 1987 conference of the American Society of Criminology, Montreal, November 1987.

LES PROBLEMES ETHIQUES ET DEONTOLOGIQUES DES NOUVELLES TECHNOLOGIES GENETIQUES. PERCEPTION SOCIALE ET PERCEPTIONS NORMATIVES DANS UNE PERSPECTIVE EUROPEENNE!

par

Giacomo Canepa
Directeur de l'Institut de Médecine Légale et
du Centre International de Criminologie Clinique
de l'Université de Genes, Italie.
Président de la Société Internationale de Criminologie,
Paris, France

Marco Lagazzi
Médecin Chercheur de l'Institut de Criminologie et Psychiatrie
Légale et du Centre International de Criminologie Clinique
de l'Université de Genes, Italie

1- Les récents développements de la technologie bio-médicale ont donné aux chercheurs et aux cliniciens la chance de modifier le patrimoine génétique et les processus de conception et de gestation de l'homme, à travers des modalités que l'opinion publique souvent n'arrive pas à comprendre et qui demandent à la médecine légale, à la déontologie, au droit et à la criminologie l'élaboration de réflexions nouvelles, dans un contexte extrêmement délicat et complexe.

Face à ces innovations, la réaction de l'opinion publique semble osciller entre l'attente vers les progrès de la science et la peur de son développement incontrolable, dans un cadre d'émotivité et d'incertitude collectives, qui pose des problèmes inquiétants, en partie encore sans réponse.

Face à un thème si complexe, la prescription normative paraît riche de lacunes ou insuffisante, et parfois conditionnée par les exigences opposées de l'opinion publique, de l'industrie et de la recherche scientifique.

Les nouvelles technologies génétiques et d'insémination artificielle, même si elles représentent un important progrès pour la science médicale et pour la biologie, peuvent aussi permettre, dans un contexte de perception sociale déformée et de carence normative,

plusieurs activités illicites ou franchement criminelles. Il peut donc être opportun de vérifier synthétiquement quelques caractéristiques des problèmes provoqués par ces nouvelles technologies dans la réalité sociale et normative européenne.

Il faut donc affronter ces problèmes sur la base d'une préliminaire réflexion déontologique, en considérant que la culture européenne pose la déontologie médicale entre les prémisses doctrinales fondamentales de la médecine légale.

Suivant cette perspective la déontologie étudie les devoirs, les pouvoirs et les droits du médecin qui, dans son activité, doit respecter des règles morales, sociales et juridiques (Canepa, 1983).

Il est évident que la base doctrinale de telles normes dérive de l'éthique ou philosophie morale (Puccini, 1984). Les normes de conduite établies par l'éthique, ou philosophie morale, ont un caractère général, et concernent n'importe quelle activité humaine, professionnelle ou non (et pas seulement l'activité du médecin).

Par conséquent n'est pas l'éthique qui se qualifie au niveau des différentes professions (et pour cette raison parler de "biothique" ou de "éthique médicale" représente une erreur).

Cette qualification se produit au niveau de la déontologie, en tant que application des normes morales et juridiques aux règles de conduite à suivre dans le domaine des différentes professions.

La déontologie qui nous intéresse, dans le contexte des nouvelles technologies d'importance juridique, et notamment pénale, est donc celle concernant les comportements des personnes qui exercent une activité médico-biologique, soit au niveau pratique, c'est-à-dire des professions, soit dans le domaine scientifique, c'est-à-dire de la recherche.

Le grand développement de ces technologies nouvelles dans le domaine professionnel (par exemple l'insémination artificielle avec ses différentes modalités) représente aussi la conséquence de la planification pratique de telles activités selon des critères , dans une perspective de profit et de productivité. Il s'agit de critères et de perspectives purement économiques, souvent réalisées sans aucune considération pour les aspects moraux.

Par conséquent ces activités, qui se développent en désaccord avec les normes légales et morales (où elles existent), n'intéressent pas seulement la déontologie médico-légale, mais aussi la criminologie (Canepa, 1986).

A cet égard, on a récemment signalé l'exigence de promouvoir des systèmes de protection et de moralisation renovés dans le domaine de la criminalité économique, de mettre en garde les citoyens contre les abus des moyens de communication de masse et les falsifications d'une publicité mensongère, de protéger le patrimoine naturel des effets nuisibles d'un développement technologique et industriel prodigieux et incontrolé (Ancel, 1985).

2- L'ingénierie génétique représente un important progrès dans le domaine médical, surtout pour la production d'hormones et d'anticorps monoclonales par la re-combinaison du ADN d'espèces bactériennes, pour la prévention des maladies héréditaires et, dans le domaine de l'agriculture et de la zootechnie, pour l'amélioration des espèces animales et végétales d'intérêt économique (Parisi et Spalla, 1985; Buvoli et Sqaramella, 1986).

Sa complexité et la difficulté d'en prévenir un emploi incorrect (création d'hybrides entre homme et animaux, manipulations à fins militaires de bactéries pathogènes, etc.) ont toutefois déterminé dans l'opinion publique un état d'appréhension, pour lequel l'image du chercheur médecin - biologiste est parfois assimilée à celle du "savant fou", capable de créer des montres ou de conduire des études contre

l'humanité, comme on peut déduire de l'opinion répandue sur la genèse de laboratoire du virus de la S.I.D.A. (Bologna, 1986; Spinsanti, 1987).

Les valences dirigées vers les nouvelles technologies de fécondation artificielle sont au contraire marquées par des éléments différents, relatifs au bruit provoqué par la nouvelle des premières naissances déterminées à travers une fécondation de ce type et à la nécessité conséquente de redéfinir, aussi sur le plan moral et social, la notion de paternité et de maternité.

Les récentes innovations bio-technologiques ont créé un état d'attente et d'inquiétude dans l'opinion publique, augmenté par les nouvelles de phénomènes qui ne peuvent que susciter de la perplexité, comme le commerce d'embryons, la création de marchés illégaux d'organes à transplanter, et la tendance à l'emploi commercial de ces technologies, qui peuvent provoquer des doutes et des conflits dans la collectivité, et solliciter la médecine légale, la déontologie, et aussi la criminologie, à s'interroger sur les possibles violations des droits de l'homme et sur les délits que telles innovations peuvent favoriser (Svennson, 1985).

A cet égard on peut citer les infractions, d'ordre déontologique et légal, liées à l'expérimentation sur des embryons et des foetus vivants, destinés à l'avortement, et le commerce des produits de conception ou des annexes embryonnaires destinés aux activités expérimentales ou industrielles (Dell'Osso et de Palma, 1983; Parodi et coll., 1984), ainsi que la découverte récente, mentionnée par la presse, d'un trafic d'organes, prélevés d'enfants kidnappés et tués en Amérique Centrale, et destinés à des greffes réalisées dans un milieu médical illégal.

Des réactions analogues peuvent être provoquées par la pratique de l'expérimentation de moyens diagnostiques et thérapeutiques sur la femme enceinte et sur l'embryon, réalisée au dehors des paramètres nécessaires du consentement et de la légitimation normative (Mantovani, 1986; Agazzi, 1987).

Il s'agit donc d'un domaine en évolution tumultueuse, où les droits des parties intéressées, et surtout les droits de l'enfant qui va naître, ne semblent pas sauvegarder d'une manière adéquate, dans le contexte d'une pression scientifique, industrielle et commerciale face à laquelle la promulgation normative et la réflexion éthico-déontologique sont souvent dépassées, et parfois seulement substituées, d'une façon partielle, par des meta - disciplines, comme la soi-disante "bio-éthique", dont la crédibilité est encore à évaluer (Gillon, 1986; Lagazzi, 1987).

Dans le contexte européen, dans une culture plus traditionnelle que celle américaine, l'opinion publique semble s'interroger sur les valeurs et les risques liés aux nouvelles bio-technologies, et sur leur caractère légal, avec un débat articulé et riche de contrastes, où a récemment pris position aussi l'Eglise catholique, en soulignant les risques moraux dûs au défaut du respect pour les droits de l'homme, du dommage à la vie embryonnaire, et à la violation des modalités naturelles de conception et de gestation (Johannes Paulus II, 1983).

Cette attitude restrictive, qui exclut toute possibilité d'interruption volontaire de la grossesse, considère en outre "illicite et immorale" l'insémination artificielle hétérologue, et toute autre activité analogue réalisée en-dehors du mariage, comme la pratique de prélever le sperme du donneur avec masturbation, et la création des "banques du sperme", qui permettent la donation aussi par des personnes qui sont en-dehors du lien du mariage (Sgreccia, 1986).

Dans le contexte européen, ce débat a contribué à l'élaboration de plusieurs recommandations déontologiques et projets de loi, qui représentent une médiation difficile entre les préoccupations de l'opinion publique et les exigences de développement d'un secteur de recherche et d'expérimentation complexe et en évolution rapide.

3- Comme souligne Chiarelli (1984), le développement des bio-technologies impose à l'homme moderne une liaison plus forte entre les disciplines humanistes et celles scientifiques, pour réconsidérer son rapport avec la nature, avec la science et avec soi-même.

Dans le domaine sanitaire, cette liaison est réalisée par la déontologie, discipline médico-légale que nait de l'interaction entre les valeurs anciennes, comme le Serment d'Hyppocrate, et la réflexion éthique sur les différentes problématiques posées par la moderne activité médico-biologique (Franchini, 1985).

A cet égard la réflexion de la classe médicale mondiale, codifiée par la Déclaration sur les recherches bio-médicales, approuvée en 1964, et mise à jour en 1975 et 1983, éclaircit d'une manière adéquate comment le chercheur doit sauvegarder le consentement et les droits du patient, en se posant comme seul but sa santé, valeur non soumissible aux intérêts de la société et du soi-disant "progrès scientifique".

Reste toujours ouvert le problème du caractère licite de l'intervention du médecin face à la demande du patient de jouir de techniques d'insémination artificielle ou de "embryo-transfert", dont on devrait en tout cas évaluer l'opportunité, en rapport à la sauvegarde des droits de toutes les parties intéressées, et en-dehors d'intérêts économiques qui les impliquent.

En effet sous le profil déontologique, il est bien différent de garantir le droit d'un couple à avoir des fils avec la crio - conservation du sperme destiné à la stérilité parce qu'atteint d'une tumeur testiculaire ou de la maladie de Hodgkin (Scammell et coll., 1985), ou transplanter un embryon fécondé dans l'utérus d'une "mère à louer". Telle action peut en effet être identifiée comme une forme "rémunérée" de violence sur la femme, qui n'a pas la disponibilité de parties de son propre corps à des fins commerciales. En effet cette disponibilité, pour la normative juridique et la déontologie européennes, est de toute façon illicite.

Aussi la crio-conservation du sperme pose quand même quelques problèmes délicats, inhérents à la reconnaissance de la paternité pour un nouveau-né qui soit conçu en conditions de stérilité actuelle du père génétique, ou même après sa mort.

Egalement douteuse semble, comme souligne Santuososso (1984), la question de l'insémination artificielle réalisée sur des femmes seules, sur des couples homosexuels, ou dans d'autres situations qui peuvent ne garantir pas à l'enfant une famille bien constituée (même si à ce propos on devrait d'abord donner une solution aux problèmes de la protection de la maternité et de l'enfance "naturelle", qui souvent offre au mineur des garanties encore plus réduites).

De telles pratiques posent aussi de graves problèmes par rapport aux concept de droit à la procréation, à l'identification des parents, à la reconnaissance du nouveau-né, au status des fils conçus par insémination artificielle homologue ou hétérologue, à leur position dans la puissance paternelle et dans les droits héréditaires, et à leur droit d'être informés, ou non, de leur origine (Alpa et coll., 1984).

Restent enfin complètement à élaborer les paramètres psycho-physiques qui permettent à un couple, ou à d'autres personnes, de jouir de l'insémination artificielle, en-dehors d'éventuelles demandes non motivées, d'intérêts économiques ou d'autres facteurs capables d'influencer négativement le développement du nouveau-né et sa jouissance des droits civils.

Pour ce qui concerne l'ingénierie génétique, au-delà des plus extrêmes hypothèses concernants son emploi dans l'hybridation d'espèces animales et dans la guerre bactériologique, ou au-delà du dommage à l'environnement dû à des espèces végétales ou animales altérées à fins commerciales, se pose le problème du caractère licite de la manipulation des gènes humains, par rapport au but que telle action se propose.

C'est en effet évident qu'aucune altération volontaire du patrimoine génétique humain, même si directe à fins préventives et thérapeutiques, peut être réalisée en-dehors du consentement des parties intéressées, ou sans avoir examiné déontologiquement et normativement telle action, et ses motivations, techniques et fins.

On peut finalement citer le problème du diagnostic précoce par prélèvement de liquide amniotique, qui pourrait causer des demandes en-dehors des exigences thérapeutiques, comme la demande d'interrompre la grossesse après l'identification d'un embryon viable, qui présente un sexe non accepté par la femme ou par sa famille (Fletcher, 1980).

Du point de vue de la médecine légale les problèmes posés par les technologies bio-médicales et par l'insémination artificielle donc ne peuvent pas être codifiés en normatives spécifiques, parce que la même conduite peut être déontologiquement et cliniquement correcte dans un cas, mais illicite ou non adéquate dans un autre cas.

La fonction de la médecine légale, dans ce domaine, doit être orientée à la comparaison entre la réalité casuistique et les supérieurs préceptes de la déontologie et des droits des parties intéressées, dans le respect de la normative existante (Barni, 1985).

Il faut toutefois encore définir quelle soit cette normative et à quelles fins elle soit adressée.

4- Comme souligne Vacca (1987), l'intervention du droit dans le domaine de l'expérimentation médico-biologique peut être finalisée à la limitation de l'acquisition de connaissances, ou bien à la réglementation de leur emploi pratique.

Le choix du niveau d'interprétation dérive d'une évaluation probabiliste des dommages éventuels, causés par les recherches actuelles ou futures. Par conséquent, suivant la tradition, une autonomie plus grande est accordée à la recherche qu'à ses applications opératives. Mais dans ce domaine c'est la recherche même qui a posé de nombreux

doutes sur son caractère licite, en déférant au droit la tâche de définir le seuil au-delà duquel l'augmentation des connaissances scientifiques devient violation des droits de l'homme.

Dans ce contexte, il faut aussi définir les délicats problèmes, moraux et juridiques, inhérents au status d'être vivant du produit de la conception, au caractère licite de l'expérimentation sur lui et de sa suppression éventuelle et, d'une manière plus générale, à la définition de ses droits civils, par rapport aux droits des autres parties intéressées au problème (Alpa, 1985; Lanzillo, 1984; Kaufman et Weekes, 1986).

Aussi dans des systèmes juridiques avancés, comme le système allemand, la normative actuelle est toutefois adressée surtout vers la réglementation d'activités déjà acquises dans la pratique médicale, comme l'expérimentation et l'emploi de médicaments et de radiations, alors que semblent encore partielles, et donc insuffisantes, les normes directes vers la réglementation de la recherche génétique, surtout sous le profil de la sauvegarde des droits des intéressés et de l'admissibilité de l'expérimentation dans ce domaine (Esser, 1986).

Actuellement, dans le contexte italien, il n'existe aucune normative à ce propos, malgré la riche moisson de propositions de loi présentées dans les derniers dix ans, et malgré la querelle, désormais séculaire, entre les partisans de l'insémination artificielle et l'Eglise catholique.

La condamnation prononcée par l'Eglise moderne contre ces pratiques qui remontent en 1897, se basait en effet sur les mêmes raisons restrictives présentées dans ses orientations récentes (Pius XII, 1949, 1951, 1956) et actuelles, inhérentes à la sauvegarde de l'Institution de la famille et au refus des voies de fécondation "innaturelles", ou réalisées en-dehors du mariage (Sgreccia, 1986).

Ces orientations furent accueillies aussi dans la jurisprudence des années cinquante, et reprises par quelques unes des premières propositions de loi sur cette matière, qui tendaient à incriminer la fécondation hétérologue comme délit contre la famille.

Dans les années suivantes, on a présenté au Parlement italien plusieurs propositions de loi sur ce sujet, essentiellement concordantes sur la possibilité de réaliser les différentes modalités de insémination artificielle (à l'exception de la plus controversée fécondation hétérologue), même en-dehors du mariage, à condition que tout soit réalisé dans un contexte médical, avec le consentement des parties intéressées, l'exclusion de tout intérêt économique, et la plus grande garantie des droits de l'enfant qui va naître (entre les autres, on peut citer pour leur caractère exausthif la P.d.l. n. 2543 du 1981, la P.d.l. n. 2467 du 1981, la P.d.l. n. 2231 du 1984, et la P.d.l. n. 2260 du 1985).

Etant donné la fin anticipée des législatures, au cours desquelles furent présentées, aucune de ces propositions s'est traduite en Italie n'existe donc encore aucune normative en matière, ni existent des normes inhérentes au domaine de la manipulation génétique.

C'est en tous cas intéressant de noter comme l'élaboration normative allemande et celle italienne se soient directement rapportées aux règles minimales proposées le 5 mars 1979 par le Conseil de l'Europe, reprises ensuite par le Décret n. 4776 de 1981, qui après un large débat a entendu donner au législateur européen une référence unitaire, avec la proposition d'un "décalogue de recommandations", auquel devraient se référer les normatives en matière des Etats membres (Santuososso, 1984):

1) Défense de pratiques génétiques et d'ingénérie biologique;

2) Identification de la responsabilité du médecin en telles activités;

3) Gratuité de la donation du sperme;

4) Nécessité du consentement de la femme et, si mariée, du mari, pour n'importe quelle forme de fécondation artificielle;

5 Respect des garanties sanitaires dans le traitement de la conservation du sperme;

6) Garantie du secret pour toutes les activités à l'insémination;

7) Admissibilité de la fécondation homologue et hétérologue, sur une femme mariée, ou non mariée;

8) Définition de spécifiques modalités et garanties pour l'insémination post-mortem;

9) Légitimité de l'affiliation par le mari qui consent l'insémination artificielle;

10) Défense du rapport entre le donateur et le fils dans l'insémination hétérologue.

L'orientation du Conseil de l'Europe est donc directe à l'admissibilité de la fécondation artificielle, à condition qu'elle arrive dans le contexte de la pratique médicale, sous le contrôle de la loi et en-dehors de tout intérêt économique.

Ces recommandations, déjà acceptées par l'élaboration normative européenne, semblent donc répondre à plusieurs des problèmes posés par cette technologie, et offrent aussi une indication en matière de manipulation génétique sur l'homme, comme indiqué par les suivantes prescriptions discutées au mois de mars et septembre 1986, et synthétisées dans la Recommandation 1046 du 24.9.1986 (Recommandation relative à l'utilisation d'embryons et foetus humains à des fins diagnostiques, thérapeutiques, scientifiques, industrielles et commerciales), qui invite les gouvernements des Etats membres du Conseil de l'Europe à:

- procéder à des enquêtes au sujet des nouvelles concernant le commerce d'embryons et de foetus morts, et à en publier les résultats;

- limiter l'utilisation industrielle des embryons et des foetus humains, ainsi que de leurs produits et tissus, à des fins strictement thérapeutiques;

- interdire toute création d'embryons humains par fécondation in vitro à fins de recherche de leur vivant ou après leur mort;

- interdire tout ce qu'on pourrait définir comme des manipulations ou des déviations non désirables de ces techniques, entre autres:

  - la création d'êtres humains identiques par clonage ou par d'autres méthodes, à des fins de sélection de la race, ou non;

  - l'implantation d'un embryon humain dans l'utérus d'une autre espèce, ou l'opération inverse;

  - la fusion de gamètes humains avec ceux d'une autre espèce;

  - la création d'embryons avec du sperme d'individus différents;

  - la fusion d'embryons ou toute autre opération susceptible de réaliser des chimères;

  - l'ectogénèse, ou production d'un être humain en laboratoire, en-dehors de l'utérus d'une femme;

  - le choix du sexe à fins non thérapeutiques;

  - la création de jumeaux identiques;

- la recherche sur des embryons humains viables;

- l'expérimentation sur des embryons vivants, viables ou non;

- le maintien des embryons in vitro au-delà du 14ème jour après la fécondation;

— assurer l'application de ces règles; élaborer un registre national des centres autorisés à ce type de recherche; encourager la création de comités multidisciplinaires de surveillance.

Dans la même Recommandation on énumère aussi une série de normatives à respecter dans le prélèvement et dans l'utilisation de tissus d'embryons ou foetus humains à des fins diagnostiques ou thérapeutiques qui, ensemble aux normes citées, rendent le document du Conseil de l'Europe extrêmement détaillé, et tel à constituer une référence pour les gouvernements des Etats membres.

Face aux aspects d'émotivité de l'opinion publique, et à la commercialisation des pratiques fécondatives, l'élaboration normative actuelle semble donc orientée d'une façon réaliste, avec une extensive acception de l'admissibilité de ces pratiques, à condition qu'elles soient actuées dans un contexte adéquat sous les profiles juridique, éthique et sanitaire.

Toutefois, puisque dans plusieurs Etats, comme en Italie, telles normes n'ont pas encore été traduites en loi, le domaine de la fécondation artificielle et de l'ingénierie génétique restent encore ouvert pour des initiatives légalement et moralement illicites, face auxquelles il faut réaliser une forme particulièrement stricte de controle social, attentif aux progrès constants de la technologie du secteur.

5— Il est évident que le contrôle des activités d'ingénierie génétique et de fécondation artificielle doit s'exercer en premier lieu à travers une règlementation de leurs différentes modalités applicatives, qui en assure la correction et en réduise l'actuation conduite en dehors des nécessaires paramètres déontologiques, légales et sociales.

L'émanation d'une normative autant délicate et complexe, toutefois, demande une longue période de débat parlementaire et social, et autant de temps est nécessaire pour la mettre à jour par rapport aux innovations technologiques du secteur, soit dans le domaine de la fécondation, soit dans le domaine de l'ingénierie génétique, la réglementation de la quelle est genée aussi par sa intrinsèque complexité, qui peut échapper d'une normative non détaillée d'une manière adéquate (Koch, 1985)..

Dans toutes les deux activités, reste donc encore ouverte la voie pour la réalisation de comportements illicites, la sanction desquels semble difficile, aussi par rapport à leur caractère privé, qui arrive à l'attention publique seulement suite à la violation d'un contrat entre les parties intéressées à un acte de fécondation, ou pour la dénonciation d'activités de manipulation génétique par des techniques ou par des citoyens engagées vers ce problème.

Face à ces activités, comme souligne Eaton (1985), n'est toutefois utile adopter d'une façon extensive une normative pénale, parce que, sauf les effectifs délits contre la personne (comme le prélèvement illégal d'organes du vivant, ou l'expérimenation non autorisée sur la femme et l'embryon), déjà prévus par la loi pénale, elles intéressent le domaine du privé, de pure pertinence civilistique.

La réponse juridique devrait aussi être internationnalement cohérente, pour prévenir la création de "zones de tolérance" vers des pratiques ailleurs interdites, l'actuation desquelles pourrait intéresser les citoyens d'autres nations ou, dans le cas de l'ingénierie technique, l'humanité entière.

Le contrôle vers telles activités ne peut donc être limité à l'intervention normative, inévitablement arriéré en rapport à la réalité, mais doit s'exprimer par l'augmentation de la fonction du contrôle informel, exercé grâce à la prise de conscience, de la part de la collectivité, des avantages et des risques liés aux bio-technologies.

Ca comporte d'abord un travail d'information et de "demythisation" de la matière, qui ne doit plus être cause de craintes archaiques, ou représenter une res incognita dans laquelle coexistent des chercheurs qualifiés et des "commerçants" de la reproduction et de la génétique.

La réglementation et le respect des droits des parties intéressées devraient donc d'abord se baser sur une oeuvre d'information de la collectivité, oeuvre qui considère les récentes innovations de la technologie bio-médicale comme un des aspects actuels les plus importants du progrès médico-biologique, à comprendre en tant que tel, et à surveiller pour sa correcte application.

Comme pour d'autres problèmes posés par la technologie moderne (emploi de l'énergie atomique, appauvrissement de l'environnement, etc.) le centre de la question n'est en effet représenté par la technologie en soi même, mais par son application non correcte, qui n'est presque jamais accidentelle, mais est due à des précis buts économiques, politiques ou militaires; la règlementation normative ne doit donc être directe vers la recherche en tant que telle, mais vers ses spécifiques applications, et vers les personnes et les institutions responsables.

A cet égard, il ne semble pas correct proposer une approche normative trop restrictive, qui comprime le droit des chercheurs de réaliser des études directes à améliorer le bien-être de l'humanité, et le droit des individus d'avoir des fils, d'autre façon impossible.

Il semble plus correct réaliser, dans le contexte d'une surveillance attentive des éventuelles distorsions applicatives de telles technologies, une évaluation spécifique des problème liés à chacune des interventions; évaluation qui devrait être formulée soit au niveau éthico-déontologique, soit au niveau clinique et social.

Les sciences médico-légales viennent donc chargées d'une oeuvre qui ne doit pas être seulement évaluative, mais aussi et surtout préventive, parce que seulement le médecin légiste a les connaissances et la culture inter-disciplinaire capables de comprendre les possibles altérations actuelles ou futures liées à telles innovations technologiques.

Sur le plan social, il faut enfin considérer la nécessité d'éviter la mise au point de l'attention publique, et de la normative, sur les aspects les plus évidents, comme l'"embrio-transfert" ou le mythe de la création de chimères, en négligeant la plus silencieuse ouvre d'exploitation des technologies génétiques dans le contexte biologique, agricule et zoo - technique, avec des dommages à l'homme et à l'environnement qui peuvent représenter une des formes les plus graves de white collar crime de l'avenir.

Dans ce domaine aussi, comme a signalé Zincani (1984), il est donc arrivé qu'une société de consommation a posé le bien - être matériel et l'argent à la sommet des valeurs; raison pour laquelle le délit même a assumé un caractère essentiellement économique.

L'absence de mobilisation morale de la société face au délit a plusieurs explications, pour lesquelles il faut surtout considérer l'attribution à l'argent de la signification de valeur primaire.

Bibliographie

Agazzi, E. ; Problemi morali della ricerca bio-medica. Liguria Medica, 12, 12, 1987.

Alpa, G. e coll.: La famiglia nel nuovo diritto. Zanichelli, Milano, 1984.

Alpa, G.: Appunti sulla inseminazione artificiale. Riv. Critica del Diritto Privato, 3, 333, 1985.

A.M.M.: Dichiarazione sulle ricerche biomediche. Riv. Ital. Med. Leg., 6, 458, 1984.

Ancel, M.: La défense Sociale. Presses Universitaires de France, Collection Enciclopédique "Que sais-je?". Paris, 1985.

Anonimo: Commissione d'indagine sull'impiego dei feti umani nella produzione di cosmetici. in: Riv. Ital. Med. Leg., 6, 1173, 1984.

Barni, M.: Sessualita e medicina legale. Relazione presentata all'VIII Seminario per Professori di discipline criminologiche. Siracusa, 22 - 25 Maggio 1985 (in corso di stampa).

Bologna, G.: La prossima catastrofe nascerà da una provetta? La Nuova Ecologia, 5, 80, 1986.

Buvoli, M., Sgaramella V.: Ingegneria genetica. Stato attuale e prospettive future. Federazione Medica, 39, 600, 1986.

Canepa, G.: Note introduttive allo studio della responsabilita professionale dello psichiatra in ambito ospedaliero. Riv. Ital. Med. Leg., 5, 19, 1983.

Canepa, G.: Criminologie et nouvelles formes de criminalité organisée: aspects cliniques et éthiques. in: "Rapport du Ministère de la Justice d'Italie, Centro Nazionale di Prevenzione e Difesa Sociale". XI Congrès International de Défense Sociale, Buenos-Ayres, 27 octobre - 1er novembre 1986.

Chiarrelli, B.: Storia naturale del concetto di etica e le sue implicazioni per gli equilibri naturali attuali. Federazione Medica, 37, 543, 1984.

Consiglio d'Europa: Rapporto sull' inseminazione artificiale umana. Strasbourg, 18.1.1981 (4776).

Consiglio d'Europa: Principes provisoires sur les techniques de procréation artificielle humaine et sur certains procédés appliqués aux embryons en liaison avec ces techniques. Strasbourg, 5.3.1986 (CAHBI/INF 86 1).

Consiglio d'Europa: Recommendation 1046 (1986) relative à l'utilisation d'embryons et foetus humains à des fins diagnostiques, thérapeutiques, scientifiques, industrielles et commerciales. Strasbourg, 24.9.1986 (1046).

Dell'Osso G., de Palma T.: Il distacco di parti da soggeto vivente nei suoi riflessi medico - legali. Riv. Ital. Med. Leg., 5, 76. 1983.

Eaton, T.: Sperimentazione di Biomedica e di Bioingegneria. L'ambito del controllo sociale. Relazione presentata al IX Seminario di Studi I.S.I.S.C. Siracusa, 9 - 12 Dicembre 1985 (non pubblicato).

Eser, A.: La genetica umana alla luce del diritto tedesco. Riv. ital. Med. Leg., 8, 19, 1986.

Fletcher, J.: Ethics and Amniocentesis for Fetal Sex Identification Hastings Center Report, 10, 15, 1980.

Franchini, A.: Medicina Legale. CEDAM, Padova, 1985.

Gillon, R.: Un' introduzione all' etica medica filosofica: il caso Arthur. Brit. Med. Journ. (ed. ital.), 4, 187, 1986.

Johannes Paulus II: Discorso tenuto ai membri della Associazione Medica Mondiale. Roma, 29.10.1983. in: Riv. Ital. Med. Leg., 6, 159, 1984.

Kaufman, K., Weekes, M.: Juvenile Law and the Viable Fetus: Clinical Perspectives and Legal Intervention. Internat. Journ. of Law and Psychiatry, 8, 471, 1986.

Koch, H.: Sperimentazione di Biomedica e di Bioingegneria. L'ambito del controllo sociale. Relazione presentata al IX Seminario di Studi I.S.I. SC. Siracusa, 9 - 12 Dicembre 1985 (non publicato).

Lagazzi, M.: Il dialogo ambiguo. Riflessioni sull' "eutanasia" del paziente terminale. Rassegna di Criminologia, 13, 191, 1987.

Lanzillo, R.: Fecondazione artificiale, locazione di utero, diritti dell'embrione. Corriere giuridico, 6, 635, 1984.

Mantovani, F.: Aspetti giuridico - normativi della sperimentazione in ambito ospedaliero e profili generali di responsabilità dell'Ente. Relazione presentata al Convegno: "La sperimentazione in ambito ospedaliero". Pavia, 2.10.1986 (non pubblicato).

Parodi, E. e coll.: Raccomandazione al Parlamento Europeo sul commercio ed impiego sperimentale di embrioni e feti umani. in: Riv. Ital. Med. Leg., 6, 1174, 1984.

Parisi, F., Spalla, C.: La rivoluzione biotecnologica: processi, prodotti e promesse. Mondadori, Milano, 1985.

Pius XII: Allocuzione ai partecipanti al IV Congresso Internazionale dei Medici Cattolici, 29.9.1949.

Pius XII: Allocuzione ai partecipanti al Convegno della Unione Cattolica delle Ostetriche, 29.10.1951. A.A.S., 850, 1951.

Pius XII: Allocuzione ai partecipanti al II Congresso Mondiale della Fertilita e Sterilita, 19.5.1956.

Proposta di Legge n.2467 del 24.3.1981 (Teodori, De Cataldo, e a.). in: Riv. Ital. Med. Leg., 5, 268, 1983.

Proposta di Legge n.2543 del 15.4.1981 (Giudice, Rizzo). in: Riv. Ital. Med. Leg., 5, 274, 1983.

Proposta di Legge n.2231 del 6.11.1984 (Rizzo). in: Atto Parlamentari, 9, 1, 1984.

Proposta di Legge n.2660 del 12.3.1985 (Teodori). in: Riv. Ital. Med. Leg., 7, 668, 1985.

Puccini, C.: Istituzioni di Medicina Legale (p. 543-556). II ed. Ed. Ambrosiana, Milano, 1984.

Santuososso, F.: La fecondazione artificiale umana. Giuffré, Milano, 1984.

Scammell, G. e coll.: Crioconservazione dello sperma di uomini con tumore testicolare o con morbo di Hodgkin: risultati della inseminazione artificiale delle loro partners. The Lancet (ed. ital.), 2, 62, 1985.

Sgreccia E.: Bioetica: manuale per medici e biologi. Vita Pensiero, Milano, 1986.

Spinsanti, S.: Etica biomedica. Edizioni Paoline, Roma, 1987.

Svensson, B.: Crime prevention and the new technologies. Relationze presentata al IX Seminario di Studi I.S.I. SC. Siracusa, 9-12 Dicembre 1985 (non publicato).

Vacca, R.: Il diritto e la sperimentazione. Relazione presentata al Seminario "La giustizia penale e la fluidità del sapere: ragionamento sul metodo. Siracusa, 19 - 21 Marzo 1987 (non publicato).

Zincani V.: Criminalità e rapporti economici. in: "La nuova criminalità" (textes réunis par A. Balloni et P. Bellasi) p. 27-46. CLUEB, Bologna, 1984.

New technologies in the criminal procedure and the protection of human rights /On the basis of the Hungarian legal system/

By

Dr. Imre Kertesz
Institute for Forensic Sciences
Hongrie

1. Introduction

1.1. It is a fundamental human right to live in security. Life, physical safety, property and human dignity should not be offended. All that is only possible if persons having commited crime are properly punished and, at the same time, innocent persons are not convicted.

The validation of human rights in the criminal procedure is closely related to one of the main goals of the procedure: to the implementation of finding the truth.

The access to learning the truth in a case is the basic precondition to the due operation of jurisdiction. Fair justice can be done only on realistically stated facts.

The citizen who sustained injury can rightly demand that the state should do all that can be done to find the truth using all legal means and also the achievements of modern technics. If an innocent

As a consequence of all mentioned above, making use of tested, truly reliable technical means and technologics in the criminal procedure is fundamentally in accordance with protecting human rights, and it facilitates their realization.

1.2 In respect of protecting human rights it is not only the result of finding the truth that has significance but also the way to it. The principle of "the end justifies the means" is incompatible with a democratic legal way of thinking. During the criminal procedure the realization of all the principles must be guaranted that are provided in the "International Covenant on Civil and Political Rights" of 1966. The regulations like the guarantee to a fair hearing, the right to an independent and impartial tribunal, the presumption of innocence also belong here together with other important regulations guaranteeing the realization of the rights of the suspects. Of these, concerning the application of modern technics, the protection against torture or cruel, inhuman or degrading treatment and the right to respect for privacy, home and correspondance are particularly important.

The Hungarian People's Republic has granted probate of the document of the International Covenant on Civil and Political Rights, and on the basis of its 2nd part, article 2, Hungary is under the obligation, fitting with the Agreement, to provide for legal measures that are needed for the predominance of the rights claimed in the covenant. In accordance with this the Penal Procedure Law of the Hungarian People's Republic / 1973. Law 1/ regards safeguarding personal freedom and other rights of the citizens as well as the presumption of innocence as the basic principles of procedure law.

There is no doubt that it is inadmissible to use evidence, obtained by violating human rights, even if there are some differences in the position of some authors. But they all agree that obtaining evidence, by violating human rights can be prevented better by inadmissibility, than by disciplinary, administrative or legal impeachment of officials violating the law. That is why, among others, the 12th international congress of the International Association of Penal

Law /Hamburg, 1979/ passed the resolution that "Evidence obtained directly or indirectly by means which constitute violation of human rights such as torture or cruel, inhuman and degrading treatment shall be inadmissible". Fully agreeing with that, I would like to complete the position with the following thought. The prevention of obtaining evidence by means which violate human rights can effectively be contributed if law enforcement officials are trained in criminalistics on a high level, if they know how to use legal means effectively, if they have an access to learn the truth, and to prove it, they can make use of the achievements of science and technics, and among them first of all, expert institutions with modern equipments, and if they can make use of the technical means facilitating finding and recording evidence, and if they can use the data of registers facilitating the success of the procedure.

2. The role of experts

2.1 Experts who join the most recent achievements of science and technics to the criminal procedure are playing an increasingly greater role. The achievements of scientific research in the recent years have turned a lot of physical evidence into sources of important information the examination of which – not so long ago – could not even be considered.

Identification technics developed extremely rapidly in three particular areas:

– The development of image analysers enabled the transformation of analogous signs into digital signs and their examination by pattern recognition. Thus the procedure came to be apt, to help by solving criminalistic tasks like for instance examinations of handwriting or carriing out, ballistic examinations – where the essence is the development and comparison of visual information.

– More and more modern equipments, computers and softwares are applied in chemical analytical examinations widening their possibilities in solving criminalistic tasks.

– The latest methods of the examination of different biological materials / Blood, hair, saliva, semen / open up new potentialities to more reliable, quicker and automated examinations; and can help to enlarge the circle of verifiable typs that brings closer the possibility to prove their derivation from one single person.

2.2 The better possibilities expert examinations have, the larger is the experts responsibility in the criminal procedure. Expert institutions do their best to check the reliability of examinations by quality assurance, and by elaborating and introducing control programs which guarantee the reliability of expert reports, and law defines and details who can be an expert and what his rights and obligations are.

The theory of evidences in criminal procedure law rightly points out the importance of measuring methods by carrying out expert investigations, but it has failed to set the problems arising from it in their true light. While the quality assurance of the measurings and to reduce accidental errors in it to a minimum are technical tasks, the evaluation of uncertainty elements arising from the errors of measuring in the evaluation of evidence is a legal problem that affects finding the truth and the predominance of the rights of the defendant.

Just a simple example: blood alcohol level measurings are done three times with a specific method in each specimen which are independent from each othet /3 parallel measurings on gas chromatographs/. Let us suppose that the findings of the three measurings are within the permitted deviation /m 5%/ and their middle value is 0.8%. (This is the dividing line in Hungary of the criminal offence of driving intoxicated/. It would not be right to give out this result because it would not take in consideration standard deviation and the principle of "in dubio pro reo", that is, that uncertainty can be interpreted only in favour of the defendant. So standard deviation in this case must be taken into account, in fact so, that its value /starting from mathematical-statistical assumptions threefold of it /is reduced from the average measured. So instead of the 0.8%. value above – in case of 1% standard deviation – experts report 0.78%. of blood

alcohol level. So the level of blood alcohol reaches the dividing line of criminal offence undoubtedly if the average of the values measured is 0.825 or above, practically 0.83%.

In cases of criminalistic material examinations this problem is more complex because usually many more series of examinations are carried out there. That is, in these cases the sets of features of the samples found at the scene of the crime and those of the control materials must be separately detected and then compared.

The sensitivity, the precision and the capacity of the equipments used in expert activity is growing and unfortunately so do their prices. Similarly, the requirements concerning the qualifications of experts are also higher. All these show that it is not enough to declare the right to legal experts, it is also necessary to secure the required staff, organization and equipments. With these considerations in mind we have brought about a system of well equipped legal expert institutions where highly qualified, independent, constant experts do their work.

The high quality of the reports of experts is guaranteed by the requirements concerning the qualification of the experts, and their skills in a given field are supervised by the judiciary.

Like it is provided in many countries /FRG e.g./, we have officially appointed institutions that are apt to exercise expert activity, and similarly to the provisions of several countries, /like "durably appointed" experts in Switzerland, "permanent" experts in Yugoslavia/ the Ministry of Justice appoints national "legal" experts, and county courts appoint experts for the country who are primarily to be applied to.

These experts are inaugurated by the judiciary or other legal organs of the county concerned, and it is done so in the Hungarian legal system too. This way they are not to be instructed in their rights and obligations in every single case.

The Hungarian law has strict provisions to secure the impartiality of the experts and their independence from the parties.

Expert institutions in Hungary are financed from national budget. Law determines the cases when experts must be excluded, and the state secures the independence of the experts by paying their fees in advance - among the costs of the criminal procedure. Expert institutions and their employees are commissioned and paid not by the parties but by the courts according to their participation and costs in the criminal procedure.

Our legal system does not know the notion of expert of the prosecution or expert of the defence, an expert must have the goal of stating the truth from scientific point of view and not from the point of the prosecution of the defence. This also means that the activity of our expert institutions and the content of the experts reports cannot be influenced by the financial conditions of the defendent or by this social position, the expert is not limited by the expenditure of the examinations. He needn't consider weather the party that has applied for it has the means to finance it or not.

Our system of expert institutions makes it possible that a report can be supervised by other experts, or even by high level scientific organs of the most important special fields.

At the same time citizens are entitled to apply for private expert examinations.

Reports obtained in this way can be accepted as evidence in the criminal procedure later on.

It is well known that in Anglosaxon legal system it is the duty of the parties to prove guilty or innocence, so experts are usually involved into the procedure by the parties although the court may also initiate appointments of experts /US. Supreme Court, Rules of Evidence November, 20, 1972, Rule 705./. The lack of independence and impartiality of experts representing the parties can be counterpointed

partly by the right of the opposite party to call his expert, and by his right to crossexamine the expert. As it can be seen from the mentioned, above, different legal systems are trying to make expert examinations serve jurisdiction in different ways.

2.3 Expert examinations and the application of new technical means may directly touch upon human rights in physical examinations when taking specimens of human blood, saliva or any secretion. The Hungarian criminal procedure law provides that "both the defendant and the plaintiff are obliged to undergo expert examination, except an operation or an examination qualified as an operation, and tolerate the strictly, necessary examination by the expert." It is generally accepted that these examinations may not violate the inegrity of the human body, human dignity, if they imply stripping certain parts of the body, the participants there – except for doctors and medical staff - must be of the same sex with the person being examined. Operation or any intervention painful or hazardous to health may not be carried out for the success of the criminal procedure, it must only medically be indicated. In the Hungarian legal system – like in several countries – taking blood is not considered to be an intervention violating the integrity of human body.

The examination of the human body and the problem of protecting human rights give rise to the question whether having to be examined is not against the right to be silent, the right which gives the privilege against self-incrimination. Hungarian criminal procedure law provides that "anyone may refuse to give testimony who, in this way would charge himself or his relative with committing crime in the case concerned", and also provides that "the defendant has the right to refuse to give testimony". In the opinion of the Hungarian lawyers and the position is also reflected in judicial practice, evidence obtained by the examination of the defendant or that of his blood, hair etc. in chemical or biological way is not testimonial and thus it does not violate the right of the defendant to refuse to give testimony. The criminal procedure law of the Finnish Republic even provides that the privilege against self-incrimination does not affect the duty to exhibit oneself for identification, to give handwriting specimens or to tolerate physical search, blood tests tc.

The United States Federal law distinguishes between communicative or testimonial, and physical or real evidence, and considers that evidence obtained by forensic technics except the one obtained by the use of polygraph, is not testimonial but real evidence, and so it does not violate the privilege laid down in the Fifth Ammendment of the Constitution. It is known that the law of some states of the United States does not dissociate according to testimonial and real evidence, but e.g. the Supreme Court of Georgia, dissociates in privilege against self-incrimination by testimony according to the degree of the defendant's activity, that is, it considers the evidence inacceptible - irrespective of its real or verbal character - if obtaining it requires the active participation of the defendant.

The theory of the Hungarian criminal procedure distinguishes personal and physical evidence, according to how they reflect the relevant phenomenon, event, the personal ones as reflected in the human mind, the physical ones as to the physical, chemical and mechanical changes. The traces on a human body, the particles taken from there, secretions, certainly cannot be counted to personal evidence as defined above, so their examination does not violate the right to refuse self-incrimination.

2.4 Courts are not obliged to accept expert reports, those are valued together with full set of the evidence. But experts are particularly responsible because behind their reports there are more and more sophisticated measurements and calculations and that is why it is difficult for the judges and assessors to check and value them. And in addition, parts of trace evidence may be destroyed during the examination, even if it is most carefully done.

Our criminal procedure law has detailed rules which regulate how physical evidences must be distrained, sent to an expert examination and how it must be expertized. It also decides the ways of supplementing, checking and supervision of expert reports. The supervisory expert involved in the case can value the examinations carried out by the previous expert, the justness of his calculations and his conclusions.

But we cannot conceal that a very important link, on which the rightness of the whole job depends, cannot be checked. It e.g. the coat of a hit and run case victim is brought in for examination with the car of the suspect, then, from a single chip of paint found in the clothing, the expert can identify the car. In this case one can check that when and were the coat was distrained, how the car got to the investigating authority, a new expert involved in the case can reexamine the specimens taken from the chip of paint and the comparative ones, the photographs taken from them, the spectrograms, but the most important element cannot be checked, namely whether the expert has found the chip of paint in the coat of the victim indeed, or not. This is a fact the reality of which is guaranteed only by the authenticity of the expert. And such facts can be found not only in the expert examination that was mentioned above.

This shows that forensic experts must be not only highly qualified but they must meet high moral requirements, too. And this also shows that new technical equipments may facilitate to find the trouth in criminal procedure, the defence of human right, but also create the possibility of the violation of rights

3- Video-and audio recording

3.1 Another important direction of modern technical development is in connection with electronic audio and video recording and with wired and wireless transmission of voice and image. The professional and legal use of these equipments may well facilitate the success of the preliminary investigation. This in itself is important considering the defence of human rights, but this is also speeds up the procedure. The right to speedy trial is a basic principle of criminal proceeding. In accordance with this, the laws of most countries and Hungary is among them draw deadline for certain deprivations and for finishing the investigation and the procedure. The proper use of technical equipments contributes to putting these provisions into practice. Just an example to illustrate this: simultaneously with the crime scene investigation the computered registration gets and identifies the fingerprint found there, and the result is immediately fed back to the investigating officer.

3.2 The legally recorded video and audio materials may have important role in recording certain actions of the procedure. The Hungarian Penal Procedure law rules that "authorities may prescribe recording procedural actions by stenography, tape recorder or other equipment." Recorded testimony is a true reflection of the process of the hearing and provides an opportunity to see the respect of the rights of the defendant. The law rules that a copy of the tape must be handed over, if requested by the defendant or the counsel for the defence. It also contains a lot of legal provisions which make it possible - when listening to the tape - the realization of such rights of the defendant, as the right not to incriminate himself, to refuse to make a confession, to be silent.

Recording testimony on tape usually does not substitute taking minutes. Tapes are usually supplements to the minutes. Unlike the penal procedure code of several countries the Hungarian law knows exceptions from this general rule in certain cases.

3.3 The use of video and audio recording devices for electronic devices and hidden cameras may directly jeopardize human rights, may violate the right to privacy, home and correspondence.

The Hungarian penal procedure code provides for the seizure of mail and telegram and telex undelivered yet, and it can be done only by the rule of the prosecutor or the court. To interpret similar legal regulation it was suggested in Poland that a tape of wire-tapping should be considered a sort of mail, and regulations concerning mail should be applied. Hungarian courts firmly refuse to interpret law extensively and to accept such evidence.

Yet it seems that, in proper framework, we might find the way how to make use of technical possibilities without violating human rights. Thus, e.g., the Austrian penal code allows wire-tapping and recordings of conversations if a crime is being investigated and it is, liable to at least a year of imprisonment, if the owner of the telephone can be profoundly suspected of committing the crime, or it may well be suspected that such a person is staying with the owner, or if the owner

of the telephone has agreed to wire-tapping. After finishing the wire-tapping the owner and the suspect must be notified, and they must be given the possibility to listen to the tapes. If the court rules that the provision for the wire-tapping is out of effect, the tape must be destroyed.

The regulations of the issue are similar in Sweedish law, too, where crimes, with two years imprisonment liability allow telephone surveillance. According to Sweedish law, court permits telephone surveillance only for one week, but by serious criminal offences the permission can be given for a month and even this period can be prolonged.

The use of hidden camera and the use of the film made by the camera as evidence could be regulated in a similar way but with further reservations. Such further reservation would be e.g. that a hidden camera cannot be placed in a flat or in a room serving as a flat /hotel room/ etc.

However, I must emphasize that such a procedure is not accepted by Hungarian law, and evidence cannot be obtained in this way and cannot be attached to the case.

4- Registration

4.1 The present forms of crime can only be faced successfully through the channels of a well coordinated system of exchange of information.

At present criminals and groups of criminals commit their actions not in the vicinity of their homes but mostly in the territory of a country or sometimes in several countries. Consequently the investigation organ of any country may need the information recived by any other investigation organ. So, e.g. for a police organ investigating the case of a burglary, it may be important to know when and where similar crimes where committed in the country and to know what information the local organs have in the case. And at the same time they need the data kept in the central register: who committed similar crimes

before, the committer's description, his fingerprints, whether he is in a penal institution, how many times and why he was punished etc. And in addition, preliminary investigation needs information on cars, weather conditions and a number of other circumstances which cannot be found in police registers, but elsewhere.

All this shows that organizing exchange of information between police organs is a much more complicated task than those of average hierarchical organs either in the field of jurisdiction, industry or commerce. In all these fields the necessary information can be determined in advance, the upper levels ask only for selected or global information instead of a detailed one, and there is little exchange of information between the levels, etc. The solution of the task is further impeded by the short deadlines of the procedure and because of the limited number of persons available for the task, the system of information should be completed with certain automation which would provide not only for the automatic storage of the necessary information / for instance of the record of a hearing / and the automatic production of the information where they are just needed, on the other hand.

It is obvious, that building up a system of information like this can be done only with a computerised background of criminal information in Hungary, we have begun to build it up, but a lot is still lacking for its complection.

Criminal information systems can work with the help of proper data-bases and records, which have a long tradition in every country. But nowadays when the data can easily be handled by computers, they can be stored in their memory units and can be transmitted to the user by distance data service, the question raises, who can have an access to any data, and how the system can be controled so that it should not jeopordize personal rights.

4.2 In the Hungarian People's Republic "the registration of the data of the citizens can be provided only by law, by an executive order* or by a cabinat order", and "the data of the registration and the documents on which the data are based can be given to organs and persons defined by the rule". /Law I. 1981, 53. /

Criminal registration is done in Hungary by the police. According to the 29th of executive order No 5/1979, the following persons must be registered:

a) anybody who has been sentenced or against whom measures have been taken;

b) anybody who committed an offence that can be liable to imprisonment, and anybody sentenced for breaking the customs and foreign exchange regulations;

c) anybody who is officially declaired standing on police surveillance;

d) anybody on search warrants;

e) anybody taken into custody;

f) anybody given procedural pardon.

The executive order clearly defines who of the persons in the categories above and how long they must be registered, that registration data are official secret, that the data can be given only to the authorities acting in the criminal procedure, and that the data can be given to official authorities in a limited circle, to members of the Council of Ministers, to the president of the capital's council, and county councils.

---

* An executive order is a provision of law enacted by the Presidium of the People's Republic. The Presidium substitutes the Parliament between the sessions. The executive order must be approved by Parliament in its subsequent session.

Considering the realization of human rights it is important that citizens, in this way, know, what data can be found in criminal registration, and who can have access to them. Our law facilitates that anybody can learn the data concerning his previous conviction and can apply for corrections, if he considers then wrong.

Certain important and confidential jobs can be occupied in Hungary if a clean record is certified. Such a certificate can be given to anybody, and only final judicial judgement can be indicated in it. If there is no judgement, the words "he/she has no criminal record" are put down in the certificate.

4.3 The most important personal data of the Hungarian citizens and foreigners having permanent residence in the territory of the Hungarian People's Republic are kept in the national demography registration system directed by the Central Office of Statistics. The executive order, No. 8/1974.1. , provides that it is one of the goals of demography registration to defend personal rights and 8. says that giving out and making use of the data of the national demography registration may not violate personal rights.

Every citizen has the right to ask for information concerning his own data. Any citizen may ask for the address of any other person /It is compulsory to register addresses in Hungary /. A citizen may ask for the personal data of any other person if he certifies his right or legal interest to do so. If someone finds any difference in the given data from reality, the mistake must be examined, the properly verified, correct data must be registered.

The system of national demography registration facilitates attending to the problems of the citizens, it gives useful contribution to reaching the goals of criminal procedures and at the same time the provisions of the law secure the defence of personal rights, too.

To sum up, it can be stated that modern technologies in the criminal procedure -- like in other fields of life - serve people, but this service can be used for good and bad purposes. The guarantees which exclude the use of technics for anti-human purposes must be built up both in international law and the laws of the nations. This is an important task of criminal procedure law, too. We, Hungarian lawyers do our best in our field to face the challenges of rapid technical development.

THE PSYCHOLOGICAL AND PSYCHOSOCIAL ASPECTS OF TECHNIZISED CONTROL AND SURVEILLANCE SYSTEMS

By

Detlef NOGALA, Univesity of Hamburg

The controversy over the use of modern technologies for control aims arose in West-Germany in the mid-70s. The employment of technology as a means of control by the state, particularly through police forces, led to vehement public disputes. Data-security became a durable topic.

In the meantime the use of advanced technology for control aims has increased and developed: Since April of this year every german citizen gets a machine-readable identity card, which is the key to several data banks. Legislative hindrances against collection and use of personal data are being abolished. Recommended by the one party as an effectualization of police work and feared by the other party as "big brother", the controversy about the development and employment of advanced technology for control aims has become a standard topic of public discussion in West-Germany.

At this conference we have seen how advanced technology can be used effectively as a means of identification, control and surveillance. In my view it is the task of social scientists to analyze the structure of the employment of technology in the social frame of society and examine its social and psychological significance. My questions are therefore: what does it mean to control people via technological systems? How does this circumstance influence their thoughts, feelings, and actions? Can we anticipate possible effects reliably or state them empirically at all? And if so, how do we evaluate them?

The narrow frame of my contribution to this conference allows only a roughly outlined discussion of these questions. First I will briefly illustrate my central conceptions and promises. Subsiquently I will expound my assessment of the social meaning of the use of technological control systems.

This is the basis for my reflections on the psychological aspects. Finally I want to consider the prospects of fighting crime with technizised control systems.

Starting positions: Terms, premises, approach

I think, there are three aspects to our subject: a) the relation between the individual and society; b) technology (as a socially formed ans socially forming force); and c) control (as a conflict-induced process in a concrete context of social power and rule). The multiple and dialectical connections and interferences between these categories can't be treated here in details; however, for better understanding I want to outline my approach briefly.

a) Traditionally Psychology views the individual independent of the genesis of modern subjectivity in the historical process and independent of its concrete social context: Posivistic psychology blends out internal processes usually, while idealistic directions of psychology often neglect the importance of social and structural factors. I believe that a psychoanalysis, enlighted by social sciences (as it was developed in the continuation of the Frankfurter Schule), is suited best for an adequate understanding and formulation of the reciprocal dependence and shaping of individual subjektivity and social organization (e.g. R. Jacoby 1978; K. Horn 1976; A. Lorenzer 1976 u.a.).

Individuality and subjectivity diclose their character only after we have a substantial understanding of social relations and vice versa.

Whatever the evaluation, no social scientist will deny that modern societies are typified by very complex rule- and power-relations, and it seems, that these elements have a major impact on the individual psyche, depending on the individual' social position.

b) An increasingly determinating element of society has become technology. If we consider technology the totality of objectivated skills and abilities of a society, through which it rules over the natural forces, necessary for its own existence, then the same is true about human nature. The degree of availabiltiy and the spreading of technology have a direct impact on social relations, and particularly on the circumstances of (industrial) production. In my opinion the example of the automobile illustrates very well, how the availability and the use of technology have immediate consequences on everyone's life and society at large.

But ahead of any application of technology there is a development and decision-process, which determine the If, the How and the extent of its real implementation. But this process may not be public nor democratic or deliberate.

Technology is in my eyes a socially formed and socially forming factor. The philosopher G. Anders, living in Vienna, even claims: "And its finally true, that we are formed by every device we use, no matter what we intend to use it for or believe to be using it for, no matter within which political-economical system we are using it, it influences us, because it always presuposses a certain relation between us and our fellow-men, between us and things, between the things and us" (Anders 1984, 217). Such a view of technology certainly rejects the idea of its social and moral neutrality. Technology is understood rather as an essence of social interaction but since technology is integrated in a certain social context of power. We cannot discuss it neutrally, especially since the availability of technology itself has become a significant social power-factor.

c) Control in the context of social sciences has to be considered as a type of interaction in a social relationship. Described in abstract terminology it is the relation between the (controlling) subject, that has the power of definition and sanction and is able to set the aim of the process, and the (controlled) object, whose behavior is scrutinized suspiciously. If this relation is durably asymmetrical, we can approach it as a power-relationship (1). At that moment in which this relationship is actualized, it aims at the adjustment of the control-object's behavior or attitude to the intentions or ends of the control-subject, who can threaten to punish disregard with sanctions.
The organized and institutionalized form of control can be called control-system: "A control-system is a synthesis of single control-phases, in which certain control-agents (with a specific control-behavior) control objects; this happens in certain control-cases, at certain control-times and with concrete methods of control" (Thieme 1982, S.34). Technizised controlsystems are such arrangements, in which control is established technically or with technical devices that occupy a dominant function. If a control-system isn't limited in time or place, we can speak of a surveillance-system.

In my view there is a reciprocal interaction between the individual, society and technology in which the three factors stipulate each other, without completely dissolving in each other.

The application of advanced technology in the area of the criminal justice system: Rationalization and Industrialization of Social control

If we talk about the application of advanced technology within the criminal justice system and its possible consequences, then we do this on the background of an enormous and advanced social level of control over natural forces on the one hand, and on the other the problem, that our societies have failed to create conditions for socially satisfying relations between their members, which would abolish crime and oppression.

Obviously the idea to compensate its social inability with

technological command appeals to our society. Additionally we should realize that 1) the use of computers for control aims is only one, but an important possibility within the wide range of application of advanced technology, and 2) by that the use of them within the criminal justice system is only one part in the field of control using. Especially production-processes have increasingly become the object of control via technical advices, where the surveillance of discipline and achievement is the matter of interest as even in the educational system. Therefore the employment of advanced technology as a means of social control has to be considered part of an universal technologization of society, which is supposed to eliminate real or supposed deficiencies.

As far as early societies were structured heirakially in history, certain ways of behavior or thinking were labeled as criminal by the ruling class and the attempt was made to eliminate them through sanctions. But rule was dependent on the instrument of personal power, i.e. control on individuals and groups could only be exercised by the engagement of loyal individuals or groups. If we consider control as a process of information it becomes evident, that man as an information-processing creature takes on a central role: the fixing of the nominal value bu those in power according to their interests, or its acceptance through agents (supplied with certain privileges); the comparison of nominal and actual value through perception and thinking; the deduction and initiation of a correction if necessary.

As the first advanced attempt to substitute technical organization for human power of control, we can classify the Panopticon of Bentham dating back to the 18th century. This disciplination-institution was organized along the principle of the division between seeing and beeing seen: from a central tower the inmates could be observed in their cells at any time, without them knowing if or whe they were observed. The principle of the panopticon demonstrates the prototype of a techizised control device: a many can be observed by few; as isolated beings they are at the mercy of the central power. The inmate is subjected to the normset by a central authority and becomes a pure control-object: "He is seen without beeing able to see, he is an object of information, never a subject in communication process" (Foucault 1977, 257).

G. Ortmann has pointed out that the modern personell-information-systems in industrial plants and offices follow the same logic (S. Ortmann 1984). And I maintain that police data banks operate after the same principle: informaion about the person is collected, checked on its "normality", and behavior-accounts are opened, which can be combined and used without the knowledge and the influence of the person concerned (2).

Modern control-technologies presented at this Course can be reduced to three major function: the obtaining of information, the identification and processing of information (opening the possibility of control).

Therein lies the attraction and usefulness of advanced technology for control agents. Computers are so well suited for control aims, because, they have made information-processing so much faster, they are able to process huge data quantities economically and store them systemtically over a long time with little need of space. Microelectronic devices like buggs and video cameras (on the other hand) are new and significant agents in the extension of gaining data for a controlsystem (3). With reference to Foucault we can identify this as the historical rationlization-process of power and discipline:

a) Rationalization in the sense of a de-moralisation and de-emotionalisation of control in favor of a functional perspective (4);

b) Rationalization in the sense of a more economical use of control-ressources;

c) In the sense of an intensivation and expansion of control power; and at last

d) In the sense of an elimination of the often unreliable and irrational factor man.

Technology tends to be substituted for human control-power: some technizised control-systems make man superfluos, others complete his skills to perfection by improving his accuracy and reach. Others yet permit an insight into certain situations and disclose knowledge that was hidden or unaccessible till now. Like any human controller, technized control-systems are to trace conspicuousness and deviance. It is their task to discover and to identify: a hidden behavior, an unknown characteristic or a wanted person.

In a structural view we can observe replacement of human memory with mechanical memory, human perception with automatic perception, human attention with mechanical and smoothly running processes, human initiative with the algorithm of technology. But most important: technizised control-systems overcome the drawbacks of the human control-agent: his inattention, his tiredness, his limited perception and memory capacity, his avertiveness, his corruptability, his capriciousness, his psychological vulnerability but also his capability of feeling indulgence, empathy and solidarity - shortly everything, that determines human subjectivity. Technizised control-systems cannot be easily deceived and one cannot argue with them. In my view shows how the "objectivation" of control via technical devices leads to a specific form of alienation: To a policeman one can talk, one may even try to fool him or make a deal, he has a motivation of his own and his own range of judgement.

A technizised surveillance-system cannot be questionned about its purpose - it will silently produce his control-knowledge and encounter the individual as an external, alien power. The control-subject, using technology, shifts into the background, without actually being absent - it profits from the ends of control. Such systems turn simple information-data into priviliged knowledge, and this knowledge becomes power, given the opportunity to sanction. I will not ignore that control-systems can work well even without technology, driven only by human working power. But it is the very characteristic of technology that it renders this process more efficient and potent.

But if it is justified to consider this a process of rationalization of control (which is always a sort or rule), we may even take one further step and ask, if we aren't facing the industrialization of the norming-process. Let me draw a comparison: In an organized form, technology has made natural forces easily available for the industrial production process. Analogue to this procedure human nature will be adjusted to given social norms via technological processes. Both the shaping of conformity and the surveillance of norm-keeping are organized industrially with the aid of (control) machines. This could mean a huge quantity in the production of conformity, but also a severe loss of social vitality and development (S. Greenwald, cit., in Burnham 1983, 47)(5).

The objection may be made, that my considerations tend to be an exaggeration, as we are just at the beginning of this process and there are some other factors to consider: protecting laws, responsible governments, and others. But we can see the slow development, that technology tends to be employed in areas in which traditional norm-controlling factors (the parents, the church, the school, social authorities in general) don't work well any more and loss their function.

From the control-agents point of view, this development can only be wellcomed as it seems to make their work more successful. Therefore Stanley Cohen is correct in pointing out that in connection with the increasingly technologization of control-systems, a renaissance of behaviorism imagineable - prevention of the act of crime by the direct control of whole populations, categories and spaces." (Cohen 1985, 147).

But from the point of view of a criminology, which investigates the norms of a society critically and points out their changebility according to social interests, it is to be feared that there are undesirable and unforseen side-effects or that social development to more autonomy and freedom will be hindered. To imagine what the Gestapo would have done with the modern possibilities of controlling people or social groups is not very pleasant. Of course this doesn't imply, that our Western societies are totalitarian; but we have to realize that the

employment of technology for control-purposes contains a totalitarian potential (s.G.T. Marx 1984). The philosopher G. Anders put it this way: "If men are fundamentally controlable and if they can be put at the mercy of their fellows or another power, or if they are considered or treated as beings that may be put at anybody's mercy and should they live as potentially controlable beings at the mercy of others or be in effect controlled or at the mercy of others, then this determines - no matter who is at another person's mercy or why, no matter in which political system - a certain mode of existence, an unfree existence..." (Anders 1984, 218). I have exposed these ideas, to point out the background, to which a psychological analysis should refer.

Discussion of possible psychic, psycho-social and socio-psychological effects

In his book "On the process of civilisation" the social scientist Norbert Elias has described, how the historical changes of economy and the resulting modifications of social relations have slowly created something like the self-control of individuals, since this proved to be advantageous for individuals as well as groups. Let me cite one very informative statement from Elias' book: "The control - and surveillance apparatus of the society has its equivalent in the control apparatus, which develop in the mind-economy of the individual" (Elias 1979, 327 - 328). This statement is important to my considerations. If we talk of control, we can distinguish psychologically between foreign-control and self-control. The first term describes an external relationship in which the individual is the object of control-aims. This relationship is characterized by differing sanction-possibilities. The purposes of the control-subject has not yet been internalized by the individual. The tension between foreign and the individual's own intentions is latent and can lead to conflict. We can speak of self-control, if the individual has internalized common norms during the process of socialisation and the conformity to them needs no permanent support from the social outside. Conformity will be kept even against dislike through internal psychological processes. Psychoanalysis calls this internal mediator, which guarantees the self-control, the super-ego.

Depending on the permissiveness of the ego there is still the possibility to articulate demands, whose successful realization depends on the correct evaluation of the situation. If the pressive to follow the norm is very strong, there is the danger of "self-repression", which means that internal opposition is directed against the self.

Of what meaning is in this context Elias'statement? We can assume, that the social technologization of control-systems will form the individuals in a way, that foreign-control will be transformed into adjusted self-control. As soon as a person recognizes, that he is the object of control in a given system of sanctions, he has to control himself preventively in order to avoid severe disadvantages. If he anticipates that he cannot prevail his contradictive intentions, he will have to succumb to the foreign will in his own interest. The technologization of control-systems increases the disciplination-effect, since the myth of their objectivity and perfection seems to make any deviant thought hopeless. In this way controlling power slowly seeps into the individual, the formerly external conflict is internalized. But it has to be underlined that the intervening technology disquises the social character of the conflict: it just seems to be an adjustment to a "normal" social demand, objectivated and legitimated by technology. This will cause a certain kind of alienation: the individual concerned cannot easily realize that technology is merely the mediator of social rule. On the other hand it will be forced to repress the consciousness of its own oppression. The inferiority of the individual to technically perfect control-systems and its alienation from the social backgrounds may lead to a serious loss of personality, as the ethno-psychoanalyst Mario Erdheim has claimed for oppresive power in general,: "The aggression against those in power increases in a way that the effort to repress it, is no longer sufficient. Everything urges the individual to act, but the fear is so strong, that it cannot do anything. One way out of this dilema is offered by regression. Thus it comes to a conversion of the aggression, which allow more accessable modes of satisfaction, but this advantage is "paid" for with a reduction of ego-structures and the according environmental relations" (Erdheim 1984, 427 - 428). The consequence could be apathy, depression or even psychosis.

The controversy over the use of technology for control - and surveillance - purposes often shows vehement affections. One example is perhaps the worldwide success of Orwell's "1984". Obviously fears and emotions are awaked, which perhaps we all experienced during our early socialisation, when we were more or less at the mercy of our educaters' power of control and sanction. These fears were certainly reinforced by the idea of a "dear Lord" who supposedly saw everything we did, especially the forbidden things. The autonomy and self-determination, the average adult usually gains is now threatened by the new technologies of control, which attack them sometimes loudless and surprissingly. To me this seems to be a realistic reason for the emotional aversion against this kind of control. Psychologically a conflict-induced control seems to concern the struggle over the degree of self-determination and liberty of action, which remains for a person. Nobody will submit to a restriction of his liberties for a long time without opposition, if that results in permanent aversion. The possibility of imagining oneself as a self-determined and free creature within the frame of a satisfying social order is not accidentally the ideal of Western philosophical tradition.

Technizised control-systems will increasingly become a part of the social and objective environment, and, as Environmental-psychology points out, suggest certain behavior and thinking patterns and prevent others. In this sense technological progress may be psychological regress, as the environmental-psychologist Lenelis Kruse claims (s.Kruse 1981, 75). The control and restriction of behavior via technological control-systems undermine the awareness on the variety of current action-possibilities and the social genesis and initiation of norms. This loss of control over individual action can in the long run lead to stress and serious disease symptoms (6). It is even unimportant, wether these systems are actually installated and well functioning; the hunch or the fear of their reality alone creates the desired effect (7).

As me know from the privacy research, to a satisfying identity belongs the control over one's own image, that one represents to the public. Goffman has called this impression management. Naturally this

includes the possibility of deception and manipulation; police could tell a tale or two about that. But faced with such a powerful control-institution as the state, this preventive should not vanish, if we don't want to be at the mercy of the world, as G. Anders put it. The situation gets particularly dangerous when computers allow it the controllers, to know more about us than we ourselves do. "In this case the specific loss of control means, that we no longer know, what the others, if they wanted to, could do with me "(Kruse 1981, 79).

For the users and agents of technizised control-systems some specific psychological reactions can be described too.

For them the aversion against their surveillance-systems often serves as evidence for deviant purposes, respectively latent crime. Everyone who refuses "technocontrol" is suspected to be aiding crime in general.

This attitude can be interpreted as a generalized distrust, which results from a deep shaking of security- and harmony-needs. Out of the fear of being socially and personally overwhelmed by crime and violence growns the strategy to illuminate reality as far as possible, to perceive danger early on and to intervene preventivly. But beyond this legitimate need for security a delusion is developing, that wants to shape society and individuals conformingly by technical aids; this means: the will, the aims and the intention of all potential control-objects will be torn out of their social context and will also be deprived of their potential legitimate contradictibility. By that I claim, that technizised control-systems effect not only the control-objects psychologically, but also the controllers themselves.

So far I have discussed the psychological aspects of technizised control-systems under the assumption of a more or less forced acceptance. But as german experiences show, the implementation of such systems cause public protest and resistance. The theory of reactance of J. Brehm and others defines reactance as the psychological condition, in which people are motivated to defend their freedom or fight to win it back. Under the assumption, that a person is aware of behavior

alternatives, he will strive to ensure his action-scope and will encounter a threat with resistant behavior. But it was also shown in experiments, that severe repression leads to a vent-effect: resistance expresses itself in "covered" actions (s. Wicklung, 1978). I want to emphasize, that these statements about the psychological relevance of new technologies for the criminal justice system are provisional and incomplete, but they are enough for now.

Technology for law and order?

I am aware of the fact, that my notions aren't very useful for practitians. Perhaps they are seven angry about the fact, that I mentionned their concern about crime in society in connection with intentions to assume power. As an excuse I could only mention that even as a critic of such control I am interested in a society with no or little crime. But I have doubts that the problem of crime can be solved with a "technological attack" on deviant behavior, as i happening in large parts of society, without at the same time damaging constitutional fundaments of a free society of self-determined and autonomous individuals.

Provided that all new technologies will work in practise, succeed politically and were accepted by the people: will there be no more crime, because potential delinquents could be sure to be detected and are therefore detered? My opinion is that, as long as structural factors of the social phenomena "crime" are not cleared up and changed under consens, the technologisation of control-systems will only help to manage deviant behavior more economically but not abolish it. Deviant behavior will be tranferred into fields, which cannot be controlled formally (8). And what if with the assistance of technology all deviance is detected, and it is demonstrated that most of us are some kind of a crook anyhow, as some criminologists claim? Perhaps the "preventive effect of non-knowledge" (Popitz 1968) belongs to a pleasant and practicable way of life. Thank for your attention.

Notes

(1) The dynamic and dialectic of these topics can not be discussed here. See therefore Kelvin 1973 and Ullrich 1979.

(2) The use of advanced technology in German police forces is described in Busch et al. 1985).

(3) The potential of this technology was recognized early on:
In 1947 Konrad Kuse, one of the inventors of the computer, suggested the employment of his invention as a controlling agent of access-authorization and work achievment (s. Personal informations system 1986).

(4) See the argumentation of Ingraham and Smith 1972)

(5) In addition to this we will get the old problem of "wild" industrialization: How things are produced is determined by technology, what is being produced is no question of democratic social consideration, perhaps there remains the debate over the what for, i.e. which social demands should be satisfied. Problems resulting of this unconsious process are well known: satisfied. Problems resulting of this unconsious process are well known: 1. The chance to participate in and to influence the social normprocess will depend on the command or not-command over technological forces. This has to be considered unfavorable for a democratic creation of society.
2. The intercepting technology disguises the social balance of power: control-subject and control-object are objectively alienated. The actual social process (which is always subject to a social and historical dynamic and changeability) will be superimposed by the efficiency and the impartiality of technology and is objectivated in the material sense of the word.

(6) According to Kruse the competence of (self) determination is founded upon transparence, predictability and the ability to take influence on the environment (Kruse 1980)

(7) What G.T. Marx designates as the myth of surveillance (Marx 1984, 18).

(8) In addition: new technologies have already become a new instrument for crime itself. We can expect an increase of crimes by the powerful, who will use the potentials of these systems unscrupulously.

Abstract

This contribution deals with the psychological effects possibly caused by the implemantation of new technologies for control aims. Proceeding from a dialectical relation between the individual, society and technology the use of advanced technology in controlsystems is viewed as a process of rationalization and industrialization of social control. The change of the relationship between foreign-and self-control is discussed on the background of psychological theories. Finally there is a brief comment on the prospect of using new technologies for criminal justice aims.

Literatur

Anders, G. (1984). Die Sntiquiertheit des Menschen Ed. 2 (Ueber die Zerstoerung des Lebens im Zeitalter der dritten industriellen Revolution). Muenchen: Beck. (3. Aufl.)

Burnham, D. (1983). The rise of the computer state. New York: Random.

Busch, H., Funk, A., Kauss, U., Narr, W.D., Werkentin, F. (1985). Die Polizei in der Bundesrepublik. Frankfurt/M./New York.

Cohen, S. (1985). Visions of Social Control (Crime, Punishment and Classification). Cambridge: Policy Press.

Elias, N. (1979). Ueber den Prozess der Zivilisation (2. Bd.: Wandlungen der Gesellschaft. Entwurf zu einer Theorie der Zivilisation). Frankfurt/M.: Suhrkamp.

Eerdheim, M. (1984). Die gesellschaftliche Produktion von Unbewusstheit (Eine Einfuehrung in den psychoanalytischen Prozess). Frankfurt/M.: Suhrkamp.

Foucault, M. (1977). Ueberwachen und Strafen (Die Geburt des Gefaengnisses). Frankfurt/M.: Suhrkamp.

Horn, K. (1976). Schwerpunkt: Politische Psychologie. Leviathan, 4, 1 -13.

Ingraham, B.L., Smith, G.W. (1972). The use of Electronics in the Observation and Control of Human Behavior and its possible use in Rehabilitation and Corrections (2). Issues in Criminology, 7(2), 35-53.

Jacoby, R. (1978). Soziale Amnesie (Eine Kritik der Konformistischen Psychologie von Adler bis Laing). Frankfurt/ M.: suhrkamp.

Kelvin, P. (1973). A social-psychological examination of privacy. British Journal of Social and Clinical Psychology, 12, 246 - 261.

Kruse, L. (1980). Privatheit als Problem und Gegenstand der Psychologie. Bern u.a.O.:Huber.

Kruse, L. (1981). Psychologische Aspekte des technischen Fortschritts. In: Ropohl, G. (Hg.): Interdisziplinaere Technikforschung, Berlin, 71-81.

Lorenzer, A. (1974). Die Wahrheit der psychoanalytischen Erkenntnis (Ein historisch - materialistischer Entwurf). Frankfurt/M.: suhrkamp.

Marx, G.T. (1984). The iron Fist in the Velvet Glove: totalitarian potentials within democratic structures. Manuskript. (Orwell Kolloquium Council of Europe, Strassburg)

Marx, G.T., Reichman, N. (1984). Routinizing the Discovery of Secrets: Computers as Informants. Manuskript. (s.a. American Behavioral Scientist, Maerz 1984).

Ortmann, G. (1984). Der zwingende Blick (Personalinformationssystem - Architektur der Diziplin). Frankfurt/M. /New York: Campus.

Personalinformationssysteme a'la Zuse (28) 1986. Wechselwirkung, 8 (28).

Popitz, H. (1968). Ueber die praeventivwirkung des Nichtwissens (Mohr, Tuebingen). Recht und Staat, Heft 350 (Mohr, Tuebingen).

Spitzer, S. (1979). The rationalization of crime control in capitalist society. Contemporary Crises, 3, 187 - 206.

Thieme, H.R. (1982). Verhaltensbeeinflussung durch Kontrolle. Darmstadt: E. Schmidt.

Ullrich, O. (1979). Technik und Herrschaft (Vom Handwerk zur verdinglichten Blockstruktur industrieller Produktion). Frankfurt/M.: Suhrkamp.

Wicklung, R. (1978). Was verboten ist, macht uns erst scharf (5). Psychologie heute, 5(5), 15-19.

CONCLUSION

CONCLUSIONS

Denis Szabo
Centre international de criminologie comparée
Ecole de criminologie
Université de Montréal

Vingt ans après le 17e Cours international de criminologie qui s'est tenu à l'Université de Montréal, en 1967, dans l'année de l'Exposition universelle, notre Université accueille le 38e Cours, organisé sous les auspices de la Société internationale de criminologie, par le C.I.C.C. et l'Ecole de criminologie. Il y a vingt ans, c'est la "Criminologie en action" qui fut le thème du Cours: on examinait l'impact de cette discipline dans ses grands domaines d'application: sur l'Homme d'abord, sur la société ensuite, sur l'administration de la justice enfin. L'apport des sciences de l'homme et de la société à l'étude du comportement et de la personnalité criminelle, sur les groupes, les milieux sociaux, des cultures et de sous-cultures, sur les institutions qui constituent la Justice -la police, les tribunaux, les systèmes correctionnels-, soulignait le caractère interdisciplinaire de la criminologie. Il indiquait aussi la prééminence de la multi-causalité si bien illustrée par les travaux de Gluecks, de Pinatel, de Ohlin, de Wolfgang, par exemple, par rapport aux tentations du monisme, fort présent encore dans la criminologie de la première partie du XXe siècle. On révélait également le rôle crucial du système d'administration de la justice, traducteur incontournable du droit pénal dans la définition et la gestion des questions et des problèmes criminels. Etiologie, évaluation des services, peines et prévention: voici les mots-clefs des années soixante.

Si nous regardons l'évolution du champ criminologique, celle de la théorie comme celle de la pratique, nous sommes frappés par la justesse des diagnostics et des pronostics émise lors de ce Cours. Le thème choisi vingt ans après se révèlera-t-il de la même importance stratégique? Anticipant le jugement de l'histoire, il me semble que la réponse est affirmative. En effet, le développement technologique façonne, d'une manière décisive, l'organisation et les pratiques sociales. Il pose des défis au pouvoir tant législatif qu'exécutif et judiciaire. Il affecte la définition même des objets d'étude, influence décisivement les priorités de recherche, transforme notablement notre approche aux phénomènes étudiés. Le progrès technologique en médecine, dans l'astrophysique, dans l'intelligence artificielle, en biologie moléculaire ont profondément influencé les théories, les concepts scientifiques au cours des dernières décennies. Il était donc raisonnable de présumer que le champ de la justice pénale, de la prévention du crime et le traitement des délinquants ne fera pas d'exception. Là aussi, les transformations spectaculaires sont à prévoir dans des délais relativement brefs.

Si l'on veut dater le début de l'intérêt de la technologie pour notre champ d'étude, c'est bien l'annexe "Science and Technology" du rapport de la Commission Katzenbach, rédigé par Al Blumstein, qui en marque la naissance. Marginal en face des études étiologiques et longitudinales qui dominaient à l'époque des sciences criminologiques, Blumstein est devenu depuis lors une personnalité centrale de notre discipline. La preuve, c'est qu'il fut honoré par le Prix Sutherland lors du congrès américain de criminologie qui s'est tenu en novembre 1987 à Montréal, distinction la plus importante dans notre discipline en Amérique du Nord.

Les travaux du Cours examinent les nouvelles techniques dans l'ordre des applications "micro" et "macro". Les sciences "forensic" sont d'une façon éminente affectées, car leurs liens avec les sciences de la nature sont immédiates. On relève des progrès spectaculaires dans les domaines de l'identification, de l'empreinte digitale, l'identification

précise et rapide des diverses substances. La marge d'erreur se réduit dramatiquement, l'efficacité des services s'en accroit d'autant. L'obstacle pour la généralisation du progrès c'est la qualité des informations, des données. La quantité et la qualité du personnel professionnel est en relation directe avec la quatité et la qualité des informations recueillies. Ce goulot d'étranglement se résorbe lentement: le Congrès de la Société américaine de criminologie, qui se tenait à Montréal au début des années soixante comptait une centaine de participants. Ce même congrès réunissait, dans la même ville, en 1987, plus de 1000 participants. Le nombre des universités investissant dans la recherche et la formation criminologique a spectaculairement augmenté durant cette même période. La traduction de ces chiffres dans la pratique professionnelle devrait résoudre progressivement les questions liées à la qualité des informations qui augmenteront alors la qualité des techniques d'analyses et d'exploitation déjà disponibles.

Les craintes légitimes se manifestent devant la puissance de ces technologies nouvelles. La responsabilité des divers acteurs du champ pénal, les agresseurs et les contrôleurs, ceux qui sont chargés de la prévention ou de traitement, n'auront-ils pas une tentation orwellienne de toute puissance? La lecture de nos textes est rassurante à cet égard: le danger est permanent comme sont disponibles des antidotes. Les limites de la responsabilité reculent grâce ou à cause de l'introduction des nouvelles technologies. Le principe de la liberté, toujours menacé, peut et doit être préservé dans la pratique.

Dans l'ordre "macro", il s'agit du perfectionnement du système de justice pénale. Un gravissime problème se pose ici car, contrairement à l'ordre "micro" où la déontologie individuelle joue un rôle décisif, ici c'est la puissance de l'Etat qui est confrontée. Certes, il faut assurer la sécurité des citoyens, mais quel en est le prix? Le respect des droits de l'homme se pose quotidiennement à la discrétion des grands services policiers, judiciaires et correctionnels. Comment être efficace sans être oppressif? Comment faire respecter les droits individuels sans freiner redoutablement les actions qui découlent du devoir de l'Etat à assurer l'ordre et la sécurité publics?

La question de l'ordre social juste se pose ici incontestablement. Elle se pose sans égard aux régimes politiques, dans les pays socialistes aussi bien que dans les pays de la démocratie libérale. Nos travaux ont bien montré que les différences entre les régimes politiques existent au niveau ontologique. Elles sont absentes au niveau du vécu. Infliger une peine physique ou morale injuste est ressentie de la même manière sous toutes les latitudes. Les criminologues de l'Est et de l'Ouest, du Nord ou du Sud sont engagés, comme disait le slogan, "dans le même combat". La police a décuplé son efficacité grâce au recours et à l'exploitation des empreintes digitales. Le parquet a fait la même chose en ciblant mieux les cas traités. Les tribunaux aussi en réduisant considérablement les délais de justice. La diversification des techniques de surveillance en pénologie diversifie la rispote pénale etc. etc. La digestion d'une grande quantité d'information dans un délai court: voici le défi qui est posé aux professionnels du champ pénal, aux criminologues des prochaines décennies. En médecine, en économie sans parler des sciences militaires, de semblables défis se posent depuis longtemps déjà.

Le panorama dressé pour le lecteur par les diverses contributions n'évoque pas le pessimisme orwellien devant l'accroissement de la puissance de l'homme sur l'homme grâce au progrès de la technologie. On ne sent pas la logique implacable d'une société totalitaire qui se profilera derrière celui-ci. La maîtrise comme la responsabilité demeurent entre les mains des hommes (garanties déontologiques) et de l'Etat (garanties démocratiques et parlementaires). C'est là où se situe le combat permanent toujours actuel, toujours à recommencer, pour la liberté et la responsabilité de l'homme.

Une dernière question: où allons-nous, vers où nous conduit le progrès technologique? La réponse qui se dégage pour moi est double. D'abord vers la modernisation du système de justice criminel. Ce processus est inéluctable. Ses dangers ne sont pas différents que ceux qu'affrontent les hommes de notre génération dans d'autres champs

scientifiques et sociaux. On doit cependant se préparer à affronter les questions que nous effleurions sur ce qui précède. Des expériences partielles, contrôlées et évaluées, doivent précéder chaque généralisation de recours à de nouvelles technologies. Des services de recherches doivent se multiplier; les sommes consacrées au "R.&D." doivent être très rapidement augmenter pour atteindre la proportion qui leur est consacrée dans les autres champs scientifiques et sociaux. Quant aux résultats, on doit se méfier d'un optimisme béat: la recherche spatiale est là pour nous enseigner des leçons magistrales de modestie!

Le processus de la modernisation est inséparable de l'évaluation constante des critères de la modernité. Ceux-ci sont liés à des valeurs et des normes qui changent dans nos socités. La plupart du temps lentement, mais parfois subitement et brutalement. Il doit y avoir des forums de discussion, d'échanges qui assurent une confrontation permanente d'idées. On doit se prémunir de l'introduction subreptice de valeurs sous prétexte de la modernité (par le truchement de la technologie bien souvent), sans examiner les conséquences ou les préalables touchant aux valeurs.

Ensuite, nous allons vers une plus grande responsabilisation des individus et des services (accountability). La pression vers une plus grande efficacité va s'accroître à la fois pour des raisons fiscales que pour des raisons qui tiennent à la peur des citoyens pour leur sécurité. Cette peur, qui est selon Hobbes le ressort principal de l'âme humaine et la raison principale de la soumission des hommes à la puissance publique, étatique, doit être maîtrisée. Une vigilance permanente est dans l'ordre tant au niveau des citoyens qu'au niveau des institutions publiques, scientifiques et culturelles, qui doivent en débattre, se donner des cadres pour analyser ce phénomène d'une manière constante. Le contrôle de la peur -phénomène normal mais amplifié par l'accélération du processus de la modernité-, me paraît une démarche stratégiquement parmi les plus importantes lorsqu'on réfléchit sur l'impact des nouvelles technologies sur la justice pénale. La peur des individus prédateurs, des minorités menaçant le confort du statu-quo de l'ordre social, soit les sources principales des anxiétés. Celles-ci

font courir une menace aux libertés et à la démocratie. Le progrès spectaculaire -et répétons-le inévitable et souhaitable- des technologies nouvelles peut s'il n'est pas contrôlé, jouer un rôle néfaste.

Finalement, tout au long de ce Cours, nous avons réalisé le rôle capital et irremplaçable de l'Université, à la fois dans la production des nouvelles technologies comme dans la production des critères à proposer pour en limiter l'usage. C'est la déontologie qui précise notre responsabilité dans la protection des libertés. C'est la justice sociale qui précise les limites de notre aspiration vers l'efficacité. Nos universités, nos enseignements criminologiques, doivent être des lieux privilégiés pour ces réflexions et ces débats. Le succès de ce Cours est une invitation à tous pour y participer à l'avenir.

LISTE DES PARTICIPANTS

LISTE DES PARTICIPANTS

ARCAND, J.	Journaliste - Radio-Canada 1400 Dorchester Est Montréal - P.Q.
ARNOLD, J.	Public Security Program Conseil National de recherche Division de génie électrique Ottawa, Canada K1A OR8
AUCOIN, J.	Service correctionnel du Canada Approvisionnements et Services Canada Centre de production Région de la Capitale nationale 350, avenue King Edward Ottawa, Ontario K1A OS5 (613) 995-5356
BEAUCAGE, J.	(Sûreté du Québec à Montréal) Capitaine Chef du Service des Supports techniques 1701 Parthenais - Mtl, H2L 4K7
BEGIN, S.	Directeur de la Coordination Service de police de la Communauté Urbaine de Montréal 750, rue Bonsecours Montréal - P.Q. H2Y 3C7
BERGER, A.	Co-organisateur du XXXVIIIe Cours
BERGERON, M.	Bell Canada
BLAIS, B.	Institut de Police du Québec 350 rue d'Youville, C.P. 1120 Nicolet, Qué. JOG 1EO
BLUMSTEIN, A.	Dean Carnegie-Mellon University School of Urban and Public Affairs Office of Dean Pittsburgh, Pennsylvania 15213

BOLDUC, R.	Policier Sûreté du Québec 1252 rue Jumièges Boucherville J4B 7E8
BONIN, J.P.	Palais de Justice 1 Notre-Dame Est suite 4.26 Montréal - P.Q.
BORDEN, A.	Computer Security Western Comsec 3244 Camino Diablo Lafayette, CA 94549, U.S.A.
BOULERICE, B.	A/Senior Project Manager Custody & Control - Correctional Service Canada 340 Laurier Ouest, Ottawa K1A OP9
BRODEUR, J.P.	Professeur titulaire Ecole de Criminologie Université de Montréal
BROWN, C.	(remplaçante de James Roberts) A/Senior Project Manager, Custody and Control - Correctional Service Canada, 340 Laurier Ouest Ottawa, Ontario K1A OP9
BUMSTED, K.	Director, Administration and Technical Services National Center for States Courts 300 Newport Avenue Williamsburg Virginia 23187
CANEPA, G.	Directeur Institut de médecine légale Université de Gênes Via de Toni, 12 16132, Gênes, Italie
CARDENAS GONZALEZ, O.	(Cuba)
CARSON, A.	Director Tennessee Bureau of Investigation P.O. Box 100940 Nashville, Tenn. 37210

CARTER, W.	Service Correctionel du Canada Evaluation and Research Corporate Policy and Planning Sector 340, avenue Laurier Ouest Ottawa, Ontario K1A OP9
CASTELLANOS SOTO, J.	(Cuba)
CHAPDELAINE, B.	Journaliste Service Hebdo-Science 2730 Côte Ste-Catherine Montréal, Qué. H3T 1B7
CHEVRIER, P.	50 Bvd. Hauts Bois Ste-Julie, P.Q. JOL 2SO
CLERMONT, H.	Etudiant en administration 5251, boul. Lévesque St-Vincent-de-Paul, Laval H7C 1N5
CLERMONT, Y.	Co-organisateur du XXXVIIIe Cours
CORBETT, N.	Director General, Systems Branch Correctional Service of Canada, 340 Laurier Ouest Ottawa, Ontario K1A OP9
CORDEAU, G.	Co-organisateur du XXXVIIIe Cours
COUTURE, P.	3984 Ontario Est Montréal, Qué. H1W 1S9
CUNNINGHAM, W.C.	President Hall crest Systems Incorporated 7316 Hooking Road, McLean Virginia 22101
DALLAIRE, R.	Ministère du Solliciteur Général du Québec Institut de police du Québec 350 rue d'Youville, C.P. 1120 Nicolet, Qué. JOG 1EO

DAVID, J.J.	Directeur de Laboratoire Laboratoire international de police scientifique, 40 rue Marius Berliet-69371 Lyon Cedex 08
DELAGRAVE, C.	Co-organisateur du XXXVIIIe Cours
DE STEPHANO, F.	Instituto di Criminologia and Psichiatria Forense Universita di Genova Via de Toni, 12 16132, Genova, Italia
DEPUE, R.	Behavioral Science Instruction and Research Unit FBI Academy Quantico, Va 22135
DOUYON, E.	Professeur Ecole de criminologie Université de Montréal
DOZOIS, J.	Professeur Ecole de criminologie Université de Montréal
DUNBERRY, O.	Solliciteur général du Canada Centre de consultation - Région du Québec, Montréal (283-7362)
ELIE, D.	Professeur Ecole de criminologie Université de Montréal
FLAHERTY, B.H.	Center for American Studies University of Western London, Ontario
FORTIN, R.	(Agent sécuritéPréventive Drummondville) Etablissement Drummond 2025 Jean Brébeuf Drummondville - P.Q. H2B 7Z6
FRIEL, C.	Dean and Director Criminal Justice Center College of Criminal Justice Sam Houston State University Huntsville, Texas

GAUDETTE, D.	800 Alain # 704 Ste-Foy, Qué. J1X 4E7
GODIN, S.	Co-organisateur du XXXVIIIe Cours
GOUGEON, G.	85 De Martigny Ouest St-Jérôme, P.Q. J7Y 3RE
GRANT, A.	Professor of Law Osgoode Hall Law School York University 4700 Keele St. Downsview, Ontario M3J 1P3
GRAY, S.	(Probation Officer Valparaiso, Indiana) Adult. Prob. Officer County Porter Courthouse - Room 412 16 East Lincolnway Valparaiso, IN 46383
GREENWALD, F.	Director Foundation for Development Int'l Probation and Parole Practice 2005 Virginia Lame Norristown, Pennsylvania 19403, U.S.A.
GUAY, D.	1200 route de l'Eglise Ste-Foy, Qué. G1V 4M1
HERREEA GONZALEZ, Y.E.	(Cuba)
HOLLIEN, H.	Professor and Founding Director Institute for Advanced Study of the Communication Processes (IASCP) Main Office: 63 ASB University of Florida, Gainesville, Florida 32611
HUGHES, T.	Executive Assistant to Regional Director Ministry of Correctional Services Eastern Region - 1055 Princess St. Ste 404, Kinsgton, Ontario K7K 1H3

ICOVE, D.	F.B.I. Academy Behavioral Science Investigative Support Unit Quantico, Virginia 22135
IONESCU, L.	Chef adjoint du Laboratoire Ministerul Justitiei Laboratorul Central de Experitze Criminalistice Bucuresti Bd. Gheorghe Gheorghiu Dej 33 - 35 Roumanie
JAYET, M.C.	(INRETS France)
JULIEN, M.L.	3984 Ontario Est Montréal - P.Q.
KERTESZ, I.	Director, Institute for Forensic Sciences H-1903 Budapest P.O. Box 314/4 Hongrie
KOLMETZ, P.	Division Director, Division of Information Systems & Technology Department of Criminal Justice Services - 805 East Broad Street Richmond, Virginia 23219
LAGAZZI, M.	Instituto di Criminologia and Psichiatria Forense Universita di Genova Via de Toni, 12 16132, Genova, Italia
LANDREVILLE, P.	Directeur Ecole de criminologie Université de Montréal
LAPOINTE, J.M.	10 est St-Antoine # 12.5 Montréal - P.Q.
LARIVIERE, G.	Service Correctionel du Canada 5550 Bvd. Lévesque St-Vincent Paul - Laval
LAUZON, D.	Directeur de la formation Police Communauté Urbaine de Montréal, 750, rue Bonsecours Montréal - H2Y 3C7

LAWLESS, E.W.	Midwest Research Institute 425 Volker Bvd. Kansas City MO 64110
LEBLANC, M.	Professeur titulaire Ecole de criminologie, Université de Montréal Directeur du XXXVIIIe Cours International de criminologie
LEGER, G.	Chief Causes and Prevention Sir Wilfried Laurier Building 340 Laurier Avenue Ouest Ottawa, Ontario K1A 0P8
LEGUERRIER, Y.	Co-organisateur du XXXVIIIe Cours
LEMAITRE, A.	Service de Criminologie Université de Liège Bâtiment B 31 - B 4000 Liège Belgique
LYKKEN, D.T.	Professor of Psychiatry and Psychology University of Minnesota Department of Psychiatry, Research Unit Medical School Box 392 Mayo Memorial Building 420 Delaware Street S.E. Minneapolis, Minnesota 55455
MANGANAS, A.	3076 Ed. Montpetit # 6 Outremont, Qué. H2V 2Z9
MARX, G.	Professor Department of Urban Studies and Planning - Room 9-515 Massachusetts Institute of Technology Cambridge, Mass. 02139
MASTROFSKI, S.	(University Park Pennsylvania) Assistant Professor The Pennsylvania State University S-159 Henderson Building University Park, Pennsylvania 16802
McDUFF, P.	Co-organisateur du XXXVIIIe Cours
MOKE, M.	(Zaire)

MOORE, R.	(remplaçant de Don Head) Project Manager, Offender Management - Correctional Service Canada, 340 Laurier Ouest, Ottawa, K1A 0P9
MURBACH, R.	Département de Sciences juridiques UQAM C.P. 8888 Succ. A Montréal, Québec
NOGALA, D.	Nationale du Canada Universitat Hamburg Gemeinsame Kommission fur das aufbau- und Kontaktstudium Kriminologie Jungiusstrasse 6, 2000 Hamburg 36 R.F.A.
NORMANDEAU, A.	Co-organisateur du XXXVIIIe Cours
PATIN, H.	
PETITCLERC, D.	2471 Letondal Laval, P.Q. H7T 2B2
PICCA, G.	Secrétaire général Société internationale de criminologie 4, rue de Mondovi - 75001 Paris - France
PIGEON, E.	Policier SÛreté du Québec 1700, rue Parthenais H2L 4K7 (598-4736)
PLANTE, C.	3933, Drolet Montréal - P.Q. H2V 3L3
POPLINGER, C.	Office of Inspector General Office of Investigations Chambre 7620 U.S.A. Dept. of Commerce 14th and Constitution Avenue Washington, D.C. 20230

PORPORINO, F.	Service Correctionel du Canada Evaluation and Research Corporate Policy and Planning Sector 340, avenue Laurier Ouest Ottawa, Ontario K1A 0P9
PRATHER, J.	Senior Research Analyst Office of Security Technology US Directio of Prisons 320 first street Northwest, Washington DC 20534
PREVOST, L.	Cegep de Sherbrooke
ROBERTS, D.J.	Director Research and Statistics Programs The National Consortium for Justice Information and Statistics 925 Secret River Drive, suite H Sacramento, California 95831
SABEC, F.A.	Directeur de Centre d'information de l'organisation
SCHMIDT, A.K.	Annesley K. Schmidt National Institute of Justice 633 Indiana Ave. N.O. Washington, D.C. 20531
SHUTLER, G.	Centra Forensic Laboratory R.C.M.P.
ST-ONGE, L.	917 Poirier Mc Masterville, P.Q.
STIGLIC, J.	La Gazette 250, rue St-Antoine Ouest Montréal, Québec
STRATHMAN, G.J.	Director, Information and Analysis Division 300 Bigelow Building 450 Syndicate Street St-Paul - Minnesota 55104
SURETTE, R.	School of Public Affairs & Services Criminal Justice Department Florida International University Bay Vista Campus at North Miami North Miami, Florida 33181

SWEET, R.	Professor, Criminal Justice California State University 6000 J. Street, Sacramento CA 95819
SZABO, D.	Professeur titulaire Ecole de criminologie Université de Montréal
TEPPER, S.	Co-organisatrice du XXXVIIIe Cours
TIEN, J.	Acting Dept. Head Engineering Center Rensselaer Polytechnic Institute Troy, New York 12180-3590
TREMBLAY, P.	Professeur adjoint Département de sociologie Université McGill Chercheur associé C.I.C.C., Université de Montréal
TREPANIER, J.	Professeur, Ecole de criminologie Université de Montréal
WILLIAMS, R.E.	National Research Council Canada Division of Biological Sciences Ottawa, Canada K1A OR6
WILSON, T.F.	Search Group The National Consortium for Justice Information and Statistics 925 Secret River Drive, suite H Sacramento, Ca. 95831
WISH, E.D.	National Institute of Justice 554 College Parway Rochville - Maryland 20850 USA
ZYLWITIS, F.	(Criminal Justice Administrator, Anne Arundel County, U.S.A. P.O. Box 1831 Annapolis, Maryland 21404 U.S.A.