SOME CAVEATS ON THE CONTRIBUTION OF
TECHNOLOGY TO LAW ENFORCEMENT

Paul Baran

April 1967

FOREWORD

A funny thing happened on the way to the mail box. While the writer was out of town, the attachment to my personal letter was assigned a number and emerged as a formal Paper. While overdignified in form, I hesitate to discard these words in the event they may be of interest to others, and hence: this Paper.

SOME CAVEATS ON THE CONTRIBUTION OF
TECHNOLOGY TO LAW ENFORCEMENT

Paul Baran^{*}

The RAND Corporation, Santa Monica, California

We are witnessing a changing attitude towards the use of technology in law enforcement. For example, the proposed "Crime on the Streets Bill" and the "National Institute of Criminal Justice Bill" are among those submitted to Congress which call for research, development, and the increased use of technology in the fight against crime. In California the new Governor has proposed a new non-profit organization (the California Crime Foundation) to concentrate on the development of technological aids for law enforcement.

As an engineer, I am of course pleased to see what may be the end of the era of obvious under-funding of technological research in the public order field. But, lest the pendulum over-swing, I would like to urge caution. These words are not to dampen enthusiasm, but rather to better direct where we should be going to avoid some possibly dangerous pitfalls.

* Any views expressed in this Paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

These words were written as a personal letter to Professor William H. Hewitt, Chairman, Department of Police Science, State University of New York, Farmingdale, in preparation for a joint meeting with Congressman Scheuer, author of the National Institute of the Criminal Justice Bill.

I have at various times, as an intellectual exercise, toyed with the notion of creating a large set of technologically feasible devices that would be useful in apprehending would-be lawbreakers; and hopefully in the process, deter others. The initial premise was that any device surreptitious in operation would be allowable. (In those naive days I mistakenly thought that there were two classes of citizens: the lawbreakers and the law abiders.) I sought to see where technology could be harnessed to deter "the criminal element" without disrupting the innocent citizen. Devices now in the laboratory stage were considered which could be economically implemented into the field ten to fifteen years hence. In this time period the new computer art would continue to reduce data processing costs. Cheap digital data communications would allow new widespread information systems to be built; integrated miniature electronics would reduce the cost of sophisticated electronic sensing equipment. (I also assumed that in ten to fifteen years the professionalism of the police would have increased to a point where they would be fully capable of dealing with this complex new technology.)

My first thoughts were of organized crime. I started with the question, "Is it possible to work backwards and determine the flow of each piece of printed money or checks involved in all transactions within the country?" With money printed with coded patterns as now used on cigarette coupons, this would be feasible. Each store would run their bills through a small slot and a telephone wire would send the serial numbers as a signal

to a central computer to record the transaction and spot-tainted money.

Then the question, "Would it be possible to determine who spoke to whom throughout the country by long distance telephone?" Here again, the technological answer is "yes." (While we have laws on wire-tapping and revealing contents of letters, we are less prohibited in recording who is sending mail to whom--the common "mail cover.")

New systems that would record the whereabouts of each automobile as it traveled any road, and when, can be envisioned. If drivers licenses were notched plastic cards, which would be a required part of the key system that turns on a car's ignition, we could also transmit probable knowledge of the driver of the vehicle.

I can also envision a family of sensitive chemical detection devices capable of surreptitiously sniffing individuals and even buildings for certain chemicals. (Plant substances such as marijuana should contain distinct volatile oils, each with its own "signature.") It may be possible to detect certain concealed weapons without physically touching the individual. I visualized the growth of a large network of interconnected computers able to recall any selected information on any individual. The computer could perform cross-file examinations, studying, and looking for relationships between individuals suspected of conspiratorial activities. For example, when and where each individual shared any time, place relationship to any suspected member of the "Cosa Nostra."

While many of the techniques which I considered are not economically feasible today, they might be in the

future if we encourage technological development in these directions.

Note that none of these techniques theoretically intrude upon the normal day-to-day life of the "innocent" citizen IF those that control the system are honest and the safeguards adequate. There is the rub. By moving in this direction, we could easily end up with the most effective, oppressive, police states ever created. The old cliché that "knowledge is power" is especially valid in describing a society that holds extensive information about the movements and history of all its citizens. I can think of no organization or government that has proven itself to be sufficiently benevolent to be entrusted with the power that is derived from the volume of information available in such a system.

Thus, while research and development in newer and better techniques for law enforcement is desirable to cope with the increased mobility of the criminal, and with the greater temptation that society places in his path, caution is needed lest we create a Frankensteinian monster.

We should remember that even our police are not above material temptation. There is a rotten apple in every bushel. We should appreciate from the outset that any new device created solely with a legitimate police activity in mind can and will probably be misused. The police community itself is in constant interaction with those that desire to corrupt them. Infiltration is possible. But, probably the greatest long-range danger is the excessive accumulation of power by mere access to information, and the self-intoxicating nature of such power upon mere mortals.

Figure 1 is an advertisement in a widely-mailed catalog of a national chain of radio hobby stores. (There are six branch stores in this chain in the Los Angeles area alone.) Look at the open advertisement of highly sophisticated wire-tapping devices.

While it is easy to pass laws against such devices and their advertising, the information needed to build these devices is too widespread. (Most radio hobbyists could build any of the gadgets shown at perhaps one-tenth the cost of the advertised product.)

My skepticism, and plea for caution is based upon the fear of the misuse of technology. This is not to say that we should impede development of new devices and new techniques for police purposes. Quite the contrary. The high payoff possible by investing more in technological development is so great that it would be shortsighted to outlaw the development of many of these new devices. However, those that are chosen to develop such new devices must be carefully selected to insure that they understand the long-range consequences of their decisions and choices, and that they act in the best interest of society. This means that the new technologists must be men of high ethics. This has never been regarded by my technical colleagues as a necessary prerequisite for those in the trade. (Ignoring perhaps the mixed feelings of guilt of some of the early workers on nuclear weapons.) The mere danger of adverse side effects should not allow us to automatically preclude the prescription of strong medicine. But, we should be sensitive to the possible side effects; to avoid them when possible, and be prepared to take remedial action when

they occur. We should think, as does the military, that technological aids can be expected to fall into the hands of "the enemy." If in those cases where society may have been better off if such devices were never built, an early abort would be a proper policy. Therefore, I believe that any organization developing such new techniques should itself be managed by only extremely prudent individuals, who understand the magnitude of the greater problem to society that misapplication could cause.

But, unfortunately, we live in a commercial world. It is one which creates pressures upon those who develop and manufacture products to claim more good than deserved, and to underplay the dangers of their products.

There is an unmistakable amorality which infects some of my engineering colleagues. That is, whatever we are paid to work on we automatically rationalize to be a blessing to mankind: whether it be rocket ships to the moon or larger engines for automobiles. Too many of my brethren think that merely because something can be built and sold, it should be. Fortunately, there is a growing awareness that it is not always wise to build all that is theoretically possible. In many instances we are better off to carefully pick from among a list of future feasible technical alternatives, looking both at their price and their more subtle unseen consequences.

I believe that the "Crime on the Streets Bill," the National Institute of Criminal Justice Bill, and the non-profit California Crime Foundation would be improved if mechanisms were created that would insure the necessary institutional morality, and balance efficiency of apprehension of the criminals versus the individuals liberties in

light of the longer range goals of an open society. At present, our two key safeguards against misuse of technology are the wisdom of administrative agencies responsible for issuing funds to contractors, and the overview of the legislative branch of government. But these protective safeguards may come into play too late in this fast game. I would prefer to see additional layers of protection allowing a monitoring of all proposed technological innovations in the field of law enforcement and criminal justice by those that hold sufficient understanding of both technology, and those subtle factors of freedom necessary to maintain our form of society. Such persons need a strong voice in what is, and what is not to be done. I would, for example, be reluctant to trust the sole judgment of the police or even the Department of Justice. These are dedicated men who are daily frustrated by watching the obviously guilty escape. I think it may be asking too much for such emotionally involved persons to dispassionately view life from the vantage point of the long-range goals of all society.

I would be inclined to place tight restrictions both upon those that develop new equipments under this program and upon the distribution of their products. In particular, I would do everything possible to prevent this equipment and this technology from misuse by the private detective community. One must appreciate that policemen, FBI men, National Security Agency men, and Central Intelligence Agency men are all human (and become old and retire). Yet, in most instances, retirement from government occurs at a sufficiently early age to encourage entering a new career. These new careers are often based

upon knowledge gained in one's former environment. Therefore let us not kid ourselves into believing that information developed solely for the police can be maintained within the police community. Retired policemen and FBI agents have been known and will continue to use their old connections to obtain information from files for their new employers--almost anyone with a buck in his pocket and an axe to grind. Even that relatively small handful of men who dishonor the police service by being corruptible constitute a danger completely out of proportion to their limited numbers. If, for example, even one percent of an organization can be corrupted, this would allow infiltration of some highly centralized information systems and wreck their usefulness for police intelligence purposes.

I did not intend to dwell solely upon the problems and the necessity of the safeguards. I would most like to focus upon the positive aspects of suggesting a few of the foreseeable developments that appear to have fewer and less serious undesirable side effects. For example, very much better command and control systems, such as used by the military, are both possible and economically feasible at an early date. The present shortage of police frequencies is primarily a tribute to the legal viewpoint of treating the radio spectrum as land, and the issuance of title in fee simple to the land. Police frequency spectrum congestion, I believe, can be solved by better management of the electromagnetic spectrum and choice of modulation schemes. (On a statistical basis, 99.99+ percent of the spectrum is used to transmit silence. Better use of statistics would allow better use of the

spectrum. We could free sufficient bandwidth to permit new police communications services. It is technically feasible to provide a person calling the police with instantaneous communication to the policemen directed to the scene. Of course, cryptographic protection to the channels will be necessary to prevent the criminal from listening to the conversation. But, I think such equipment can be technically developed at a tolerable price.

The payoff for such developments would be high. We could sufficiently speed and augment the flow of information to the policeman, so that when he arrives at the scene of a crime he would be fully briefed as to what has transpired without broadcasting this information "in the clear" to the criminal.* If a policeman has a question, he can get firsthand information by speaking directly to the person that called in the complaint. This could drastically reduce the time between placing a call and the arrival of a fully-briefed policeman at the scene. He would arrive with the latest of information and know exactly where to go and what to do without wasting time. The policeman could even carry a tiny short-range transmitter/receiver that relays his voice through his car transmitter/receiver to the police station. He would never need to be out of communication with the police station, and could be allowed the option of leaving his microphone open and having his entire conversation with suspect monitored and recorded in its entirety. This

* Cheap, tiny transistor radios that cover the VHF police band are selling like hot cakes at 25 dollars apiece. No burglar in his right mind is without one.

protect the policeman from complaints of rudeness or brutality and offer him an extra measure of protection. It could also aid in the evaluation and training of the new policeman. (For practical purposes, the policeman should retain control of his own microphone switch so that he himself not fall victim to the "big brother is always watching" danger that concerns us all.)

At a later date we could build devices to display both the location of the calling number of the complainant and the police car on a map display in the police car. A microfilm file system in the police car could even display specified large-scale maps of houses, yards, fences, etc. (even the layout of apartments). Alternatively, map generation could be performed by a central information center and transmitted to facsimile receivers in police cars.

Search warrants could also be transmitted electrically by facsimile when haste is desirable. This could eliminate some of the unhappiness by the police to recent court decisions on the right-to-search without a warrant.

No longer can the policeman know his large beat. But a computer could have the record of information pertinent to the policeman's possible choice of action. Central information files could supply the policeman with a history of previous police activities at the address, or of the participants involved in a telephoned-in complaint. The policeman would know, for example, whether there were any firearms registered to an individual in a house in which he is entering to break up a domestic dispute. But now we are getting into a field where extreme precautions must be

exercised in the design of such a system because of the danger to civil liberties. As an example of how new systems could improve one's right to privacy, we note that minor modifications to the telephone system could permit verification of the origin of telephone calls by the police station allowing anonymous calls to be instantaneously traced.

Clearly then, there is both good and evil in the new police technology. Wisdom is needed to separate the safe paths from the treacherous. Possibly above all, institutional safeguards are needed to insure that haste is not confused with progress.