PREVENTING DATAMOCRACY: STRATEGIES AGAINST COMPUTER ABUSES AND AN INFORMATION TYRANNY

James W. French

Russell Sage College, Albany, N.Y.; Master of Science Public Service Administration Thesis,; May 1979

ABSTRACT

Section I: Preventing Datamocracy: Strategies Against Computer Abuses and an Information Tyranny

* * * * * * * * * * *

"Datamocracy" is a society in which there are restrictions, or threats of restrictions, on the lives of individuals and society at large resulting from governmental and private interest access, control, use and abuse of data/information file systems and computer resources. Although we have not yet reached a state of datamocracy, current symptoms of this condition can be found in our society (see pages 12-16, 28-31). These symptoms, and the implications they hold for us, and strategies against preventing datamocracy are the subjects of this study.

* * * * * * * * * * *

The advent of the age of computer technology ushered in many benefits FOR from our society. The computer has enabled advances in many fields - education, medicine, public finance, to name a few. However, along with the benefits associated with the use of the technology society has had to experience certain abuses. These abuses run the gamut at one end of which are seemingly minor, unintentional, acts of computer misuse. These concern such matters as unintentional or negligent actions as would be

the case in repeated threats by a utility company to terminate services for failure to pay your bill when you in fact had paid. At the other end of the range are such abuses as: willful, malicious collection or disclosure of information for surveillance, or harassment of citizens; or the commission of crime through the use of computer technology.

Computer expert Donn B. Parker defines computer abuse as any intentional computer related act from which a perpetrator made or could have made a gain and a victim suffered or could have suffered a loss [page 9]. I extend this definition to include all unintentional acts of abuse even when no gain is made, or there was no expectation of gain. This definition includes all unauthorized, thoughtless negligent acts.

Among the most controversial issues relating to the misuse of the technology are abuses of individuals' privacy and computer crimes. Computer crimes include such actions as:

- o business firms swindling other businesses (page 11)
- o government clerks embezzlng public funds (page 11)

Among abuses of citizens privacy are:

- o government agencies empowered to force individuals to supply information (page 12)

- o black lists of businessmen (page 13)
- o rosters of individuals considered to be anti-American from the FBI (page 13)
- o the abuse of individuals' sensitive information in credit reporting and automobile insurance applications (page 13)

At the U.S. Privacy Protection Study Commission held in Washington, D.C. on Aguust 3-5, 1978, Chairman David F. Linowes expressed concern that information collected and disclosed about an individual ranges from minimum identifying data to very sensitive details of personal, physical and behavioral characteristics, and that almost every family can be effected by it. Also, he believes that there is a tendency among consumer-reporting organizaitons toward ever-increasing computerization and centralization of record-keeping operations. This situation could accelerate the incidence and magnify the impact of personal-privacy abuse (page 15).

The use of computers in the federal government has expanded from two (2) machines in 1950 to approximately 11,000 in 1978. In addition to this, there has been increased use of computers in state and local government and in the private sector (page 15). Parallelling this increased use is a growth in the amount and types of sensitive information contained in data systems, hence, greater opportunity and occurrence of abuse (page 16).

There is indication that government is becoming more aware of the extent of the technology's use and abuse, as evidenced by the creation of the National Telecommunciations and Information Administraton (U.S. Department of Commerce). However, my premise is that another ineffective regulatory or advisory agency to regulate computer activity is not needed. Rather, we need an agency that can acocmplish the following:

- eliminate, where possible, existing ineffective agencies that have responsibilities for computer activity, and
- coordiante and be responsible for the operations of remaining agencies; and
- maintain as an overall mission the goal of protecting individuals, and society in general, against computer abuses.

In order to attain these goals a number of strategies are recommended (pages 17-20). Also, in order to prevent the evolution of "another inefficient and ineffective burearucracy" certain questions should be asked. These questions may appear to be obvious, however, the fact that they are seldom adequately answered is often the cause of the phenonema of bureaucracy. The answers to the questions provide the guidelines for the agency's purposeful, directed efforts (page 21-22).

The computer technology industry also plays an important role in issues of abuse. Industry must recognize and accept its responsibilities in these areas. No longer can industry be allowed to sit on the side-lines and watch the harm and suffering its products and output causes. In order to accomplish this, strategies for industry to pursue are recommended (page 23-24).

The role of the manager is of critical importance in relation to the abuse of the technology. The strategies provided range from seemingly obvious (but often overlooked) steps that should be taken to more complex methods requiring increased effort (pages 24-28). For example, a strategy that can be easily followed is limiting the amount and kinds of data that is collected and stored to only that which is needed. However, a method that would require additional effort on the managers part would be participation in educational programs to become knowledgeable in such areas as computer technology, its jargon, or applicable legislation pertaining to privacy and security.

In an article in 1971 Jerome B. Wiesner warned of the possibility of becoming an "information-bound" society having the characteristics of a "1984". He believes that this situation could evolve even "without specific overt decision or high-level support, and totally independent of malicious intent..." (pages 28-29). Donn B. Parker, in a 1978 testimony

before the U.S. Senate Committee on the Federal Computer Systems Protection Act of 1977 spoke of future abuse of the technology. He is also concerned that adequate safeguards for computer systems to provide privacy and security protection are not expected for 8 to 10 years. Causing additional alarm is that the present state of computer security is "putting far greater trust in the hands and minds of the few who have sufficient skills and knowledge to compromise the systems" (pages 30-31)

One of the important implications of Wiesner's and Parker's articles is their relaionship to time. The fact that Wiesner stated his concerns in 1971, while Parker voiced his alarm in 1978, is indicative that little has been done to end (or at least minimize) computer abuse since Wiesner warned us. It is time that individuals and society take a stronger stand and demand privacy and security safeguards in computer data/information systems (page 31).

Section II: Issues in Public Administration - A Literary Review

* * * * * * * * * *

Very few individuals in our society remain uneffected from the use of computer technology. Most citizens experience at least some degree of involvement with a computer. The degree of involvement ranges from a remote role (e.g., drivers licenses and automobile registration) to heavy contact on a daily basis (e.g., computer programmers, managers using data processing systems output). The fact that most individuals are affected by the technology is due to the pervasiveness of computers. Every level of government federal, state, local - uses data processing systems. Private business and organizaions (e.g. non-profit) use them. Computers are even available for individuals to purchase for use in their home.

The advances made in computer technology have given us numerous current and potential benefits. However, associated with the use of the technology are many disadvantages. These include such things as:

- computer crime
- abuses of individuals' privacy
- failure to attain optimal computer efficiency (e.g. overspending on equipment, program, personnel)

- viewing the technology in such a perspective that it is feared, idolized, or considered a panacea for all problems.

The benefits of computers may outnumber the disadvantages, but the disadvantages hold severe consequences and implications for society (see pages 9-16, 28-31). Thus, many issues are raised concerning computer technology. Some issues applicable to public managers specifically, while others apply to the general citizenship.

This literacy review explores issues that relate simulataneously to the public administrator and society in general. The areas covered are:

- The need for a new organizational perspective - a "rethinking" of the computers role in relation to the organizational structure in which it operates; currently there are organizational-information system mismatches (in many cases).

- Computerization: is it the answer to managers' operational problems, or, is it the cause of those problems?

- A centralized computer data bank system operated by the Federal Bureau of Investigation making available nation-wide local police hookup through teletype

systems. The "criminal histories" of numerous citizens contained in the files are purported to be incomplete, inaccurate and misleading, yet law enforcement personnel are basing police action decisions on these arrest records.

- Will society control computer technology, or will it be controlled by society? Are we to be computers masters' or mastered by computers?

* * * * * * * * * *

Computer Technology And Public Administration In State Government - The Need For A New Perspective

This article by John A. Worthley and James J. Heaphey concerns the "micro-environment" in which the public administrator functions - the organization. It examines the relationship of computer technology and organizational structure. The authors find that an incompatibility exists between organizational structure and data processing systems.

Although the computer held great promise of increasing the efficiency and effectiveness of the public manager these benefits have failed to materialize. The computer is often keeping the manager from doing his job at all! The problem is not technical in nature. It is an organizational problem (page 33). The organizational problem has evolved because information "technology has changed the organizational environment within

which we mst operate" (page 33), however, the organizational structure has not changed. The failure to attain optimal computer efficiency "lies in a mismatch of information technology and organizational design, information technology has drastically changed while organizational processes have remained the same" (page 34). Historically, organizational processes were designed to organize mechanical work processes - machine technology. These are inadequate today.

In the article the authors discuss many of the problems that are inherent in the "organizational problem". These problems are widespread [41] and include:

- an extensive lack of understanding of computers and their impact, as well as a general mistrust of computer technology.
- although used frequently in routine, process functions, there is little computer use for managerial decision making.

  Lack of oganizaional change in response to computer technology
- managerial involvement in computer usage has been token.

"In practice the use of computer technology in government has often produced and aggravated rather than resolved the

decision making problems of public administration" [41]. To correct this situation, Worthley and Heaphey suggest that there is a "need for a new organizational perspective in view of the fact of modern information technology". Because there is little experience in implementing such a new perspective, the authors are not claiming that any easy answers exist. However, as a beginning, they recommend: increased managerial knowledge; increased user involvement; and organizaitonal adaptation (pages 35-40).

THE NATIONAL CRIME INFORMATION CENTER (NCIC) OF THE FBI:
DO WE WANT IT?

Stanley Robinson's article expresses alarm over the NCIC system. NCIC is a nationwide "criminal history" information system: Teletypes connected by telephone lines to state police computer centers are installed at local police stations. The state police computers are connected to a central computer in Washington, D.C. operated by the Federal Bureau of Investigation, the central computer stores and searches arrest records on-line with state and federal computers. The system is designed to provide wide-ranging informaion of a criminal justice nature. Robinson believes that these services currently hold great potential for abuse, however, he is alarmed over what the future implications of the system are for citizens.

The future of NCIC is feared by the author because of the great amount of uncertainty revolving around the system.

The uncertainty involves such issues as:

- future plans are in a state of flux
- there is a degree of secrecy about the system among planning officials
- there is variation of NCIC concepts among different sources he consulted (page 41)

The article gives other reasons and explanations why NCIC should be a "growing source of alarm for all of us who are concerned with human rights especially the rights of those who are black, poor, or politically unpopular" (page 42). These reasons for alarm revolve around the following issues:

- o the number of records, their content and quality
- o plea bargaining
- o suggested policies to safeguard privacy, ethics, and civil liberties, are weak
- o the very basic premise of NCIC that police need arrest records, and can use them safely, may lead to possible other misuse of the system against citizens.
- o the methods of funding and "selling" the system
- o the system contains the ingredients of a "police state" (page 42)

Robinson is not optimistic that NCIC can be prevented from occurring, however, he does suggest that the system should be challenged. By challenging NCIC, he believes that this data bank and those individuals who gather, communicate, control and use its information can be made more responsible - held accountable for any abuses. The strategy for challenging this data bank is used on the local governmental level.

Through town and city meetings citizens could vote that police departments be required to provide and make public certain statistical information concerning their use of NCIC. The author gives the example of such an occurrence in Wayland, Massachusetts. At a town meeting Robinson was able to get a majority vote of citizens (present at the meeting) that requires the police department to include in the town's Annual Report statistical tabulation of the following:

- o number of inquiries by type of inquiry and reasons for them
- o results of inquiries, including arrests and known convictions
- o a similar summary "entered" by Wayland police
- o trouble encountered (down-time of system, false arrest, invasion of rights, etc.) (page 27)

Through citizens' local challenges of NCIC the author believes that measures will be gained to aid in safeguarding individuals' privacy and civil liberties. This will be accomplished by forcing responsibility and accountability. Responsibility and accountability will be gained through citizens' impacts on the NCIC system. For instance, on of these impacts is the deterring of "questionable operations by the police by requiring an accounting of such operations (thereby opening them to criticism and veto)" (page 28).

COMPUTERIZATION: PANCACEA, OR PART OF THE PROBLEM?

Computerizing municipal functions is the subject of this article by Richard E. Anderson. The article examines problems encountered in installing and operating computer driven Integrated Management Information Systems (IMMIS) in city government. the author contends that managers "are in trouble and do not even know how to find out how much". The reason for this is that "managers have accepted and are perpetuating an extraordinary number of myths about computerization". Numerous examples are provided. Take, for instance, the myths that:

- "computerization simultaneously reduces the workload of operating departments, the number of employees, and expenditure levels
- computer salesmen can best determine what equipment is needed" (page 32)

Anderson discusses the many problesm associated witht he myths and how they formulate into the basic overall problem relative to an IMMIS. The basic aggregate problem is: public managers do not really understand how a city functions in terms of data generalization and flow. These functions have not (or at least have not sufficiently) been examined from these particular perspectives (page 35). As a consequence, managers allow themselves to be led by myths regarding computers.

The intent of this article is to get managers to stop, look, and think about their present situation. By doing so, managers can begin to recognize problem areas. Anderson advises against expecting immediate solutions. He states that "developing a truly integrated system will cost about twice as much and will take about three times as long as the most liberal estimate" (page 36).

Among the author's recommendations to aid in solving the problem of computerization are:

- heavy user involvement in the design and implementation stages of installing a system; this is especially important when using consultants
- closing the communication gap between data processing personnel and managers
- justification for installing the system: managers should be challenged, or challenge installation, on a cost/benefit basis (page 36-40)

Anderson believes that attaining an IMMIS is not only possible, but critical to maintaining municipal services in the future. Public managers can no longer afford to accept and perpetuate myths surrounding computerization (page 40).

MASTERED OR MASTER?

Erwin D. Canham's article states, in effect, that our society faces a critical decision regarding the use of computer technology. The alternatives are: Will we let computers control soceity, or will society control computers? Does the appropriate choice seem obvious? Canham fears that the wrong choice will be made. His concern has a historical basis.

The challenge and threat do not lie in computer technology. They lie in the use or abuse to which society puts the technology. Canham states: "Mankind has faced this problem before... He has not done too well in avoiding the hazards. He has learned to control the machines better than he has learned to control himself" (page 43). Thus we have the "threat". The challenge is: Will we allow the computer to take the place of conscience and humanitarian considerations in the decision-making processes?

In certain decisions (e.g., war) certain considerations which could not possibly be physically programmed must be included in the decision-making processes. The author believes that moral, ethical and spiritual considerations must play a role. Also, "the possibility of error must be rigorously surveyed and prevented" (page 44).

Canham advocates a thorough awareness of the implications of computer technology for society. Those in control of, or having

access to the technology must recognize the potentially far reaching consequences of their use or abuse of it.

Men and computers must remain close partners, but men must always have the upper hand they must remain in control. It must always be kept in mind that the computer is the "product of intelligence, not the creator of intelligence" (page 47).

INTRODUCTION

This study is divided into two parts. Section I concerns the issues involved in a "datamocracy". It discusses the potential threat of datamocracy and provides strategies that will help in preventing computer abuses and an information tyranny. Included in this section are:

- Computer technological benefits for society in the areas of education, medicine and public finance (pages 1-8)
- Computer abuses - computer crimes, abuses of privacy (pages 9-16)
- Strategies for a regulatory agency to follow to monitor and prevent abuses (pages 16-22)
- The role that the computer industry can play in preventing a datamocracy (pages 23-24).
- The role of the manager-strategies are suggested that act as guidelines; the manager is a very important actor in controlling abuses (pages 24-28)

- The "Conclusion" of this section discusses the present situation that we face. It tells how little has been done to prevent datamocracy. Also, there is little hope that more effective safeguards against abuses will be available in the immediate future (pages 28-31)

Section II consists of a literary review of four articles concerning issues in public administration. Worthley's and Heaphy's article (page 32) and Anderson's article (page 54) view issues on an organizational level. Robinson's article (page 41) and Canham's (page 60) have a broader perspective. They are geared to society in general. However, as explained at the end of these two articles, both are directly applicable to managers' functions on an organizational level.

Worthley and Heaphey believe there is a need for a new organizational perspective concerning the relationship between modern information technology and organizational structure. They feel that current organizational structure is incompatible with modern information systems.

Robinson's article expresses alarm over the National Crime Information Center operated by the Federal Bureau of Investigation. He believes that this centralized data bank containing inaccurate, incomplete and misleading arrest records on millions of individuals will be to oppress citizens' privacy and civil liberties.

Anderson examines the problems that public managers face when trying to install computerized information systems in city governments. Although his article relates to organizations within cities his premise is applicable to other public organizations. He believes that the reason there are few examples of successful applications of computerized integrated information systems is because managers have accepted and perpetuate a number of myths.

Canham asks society: Mastered or Master? He fears that we will be mastered by computer technology. He bases this opion on mankind's historical performance with new technology. He states, in effect, that men have learned to control machines, but have not learned to control themselves. We have to make a choice: Will computers control society, or will society control computers?

TABLE OF CONTENTS

SECTION II: ISSUES IN PUBLIC ADMINISTRATION - A LITERARY REVIEW

SECTION I

PREVENTING DATAMOCRACY

SOCIETAL BENEFITS OF COMPUTER TECHNOLOGY

Examples of the benefits given to society as a result of computer technology are plentiful, with much exposure in the media and much attention paid to the positive impact of computer usage. Almost daily we learn of new achievements in the technology that we find astounding and dazzling. Take for example, the fields of education, medicine and public finance:

Education

- Through the use of computers 9 year old Lana is being taught a form of modified English. Lana is a chimpanzee who since 1972 has been learning to communicate with humans. the project at the Yerkes Regional Primate Research Center of Emory University in Atlanta, Georgia is expected to continue until 1980.[1] It involves a teaching system that is based on a computer that Lana can operate at will by operating large keys on a console. There are different geometric forms on each of the variously colored keys that when pressed in proper sequence form sentences and communicates the chimps desires (e.g., "Please machine give juice..."). When testing Lana's potential for learning to read

her tutors tried confusing her. They first flashed parts of sentences on the computer screen ("Please machine give..."), and Lana almost always pressed the keys for a correct completion. "When the researchers tried to trick her with jumbled syntax - like "Please make machine..." - Lana usually wiped out the sentence by indignantly punching the period key which cleared the computer and the screen". [2]

Beside the possibility of opening a new channel of communication between man and animal, the techniques being developed at Yerkes are being used to determine whether speechless children can learn language by flashing symbols and simple push buttons. Computer technology and the Yerkes techniques offer hope for the "thousands of children who fail to develop any language at all" [3].

- Pocket calculators are actually mini-computers. With their advent into the field of education they were at first "condemned as crutches by those who feared that the ease with which they came up with the answers would create a generation of numerical

illiterates. However, the National Council of Teachers of Mathematics has firmly endorsed their use" [4]. After students learn the basic functions of math calculators cut down the time needed to perform dull, repetitive tasks. According to council member Prof. J. Fey of the University of Maryland: "You see kids fascinated by calculators who would never think of sitting down with paper and pencil to do a little arithmetic for fun". [5].

Medicine

- The use of computer technology in health care has saved lives, time, money and increases the availability of more sophisticated medical services and consultation. Computers are performing a wide-ranging variety of functions in medical science from diagnosis, monitoring and treatment of illnesses to preventive medicine:

- Dr. John W. Kirklin, surgical chief at the University of Alabama Hospital (Birmingham) created computer programs for patients experiencing open-heart operations. Dr. Kirklin estimates that since the system was started in 1966 the lives of 300 critically ill patients have been saved because the computer can "monitor every sign that the surgeon orders, forgets nothing, never gets tired and makes no mistakes" [6].

The University Hospital serves as the open-heart surgery referral center for the Southeast states, a region with a shortage of skilled technicians and nurses. In order to meet the increasing demand for open-heart operations the hospital would have needed additional intensive care space and personnel that were not available. Because of the computer the hospital has increased its heart operations from 150 to 1000 a year with no increase in the size of the Intensive Care Unit (ICU). Under the manual care system patients spent 3 to 5

days in ICU; with the assistance of the computer patients usually spend 16-24 hours. While the computerized ICU care cost around $50 extra per day it saves the patient about $450 (1974 prices) by eliminating about four days of intensive care. [7]

- A group of specialists in pediatrics programmed a computer to assist in diagnosing over 3000 important childhood ailments. This will aid doctors in reassuring a complete diagnosis and furnish information about unfamiliar diseases. Because any physician can consult the computer by dialing the nearest hospital that has a teletypewriter the program can be especially useful to isolated doctors and hospitals without expert consultants [8].

- A computer at the University of Wisconsin's Center for Health Sciences allows direct dialogue between it and patients. It calculates their chances for good health and long life (and how

to improve those odds) after analyzing patients answers to its quesitons. Dr. Norman Jensen, director of adult medicine at the university's hospitals and co-developer of the program sees it as an inexpensive alternative to costly physical exams for persons under 40 who need to be warned of bad health habits that could lead to medical problems (although they show no signs of current illness). Thus the computer is an aid in preventive medicine [9].

Public finance

- The examples shown below demonstrate how computer technology was used in New York City to save taxpayer's dollars [10].

  - In two years 15,000 ineligible people have been removed from the welfare rolls. Computer searches that match names on welfare rosters with those on city and state payrolls have removed these ineligibles and reduced payments for thousands more, thus saving nearly 60 million dollars.

- A new computer-match program will result in the closing of an estimated 3,150 cases and a savings of 11.4 million dollars through comparison of Social Security payroll information with welfare lists.

- The computer matching programs of the Internal Revenue Service will provide more than a quarter-billion dollars in additional revenue from added taxes collected in 1978 while an additional 50 million dollars will be paid out to people who overpaid their taxes [11].

- When the IRS reaches the level of matching 100 percent of information documents with individual tax returns it is expected that an additional half-billion dollars will be collected annually from 4.8 million people who do not report their full income or fail to file any tax return [12].

We must not let ourselves be dazzled by the direct effects of the state of the art to the extent that we are blinded to the indirect effects of the technology - computer abuses. This paper throws light on the issues of privacy and security as they relate to the abuses that society has experienced as a result of

computer technology. No matter how great or how extensive the positive impact is, this offers no justification or rationalization for the harm and suffering that have occurred and the potential disasters that may occur from the evolution of a "datamocracy". Datamocracy is a society in which there are restrictrions, or threats of restrictions on the lives of individuals and society at large resulting from governmental and private interest access, control, use and abuse of data/information file systems and computer resources. The focus of this paper is primarily on the controlling of computer abuses in the areas of the privacy and security of the data/information itself and the abuses of computer hardware/software and will present examples of this. However, the subject of physical security (e.g. bombing of computer facilities) is only touched upon in the recommended strategies for defense.

Because computers have the ability of processing vast amounts of data involving large numbers of individuals, businesses, etc., any abuse of the technology - whether intentional or otherwise has the potential of harming and causing suffering to huge numbers of indivdiuals and our society as a whole. Consequently, it is essential that proper light be shed upon such abuses in order to tone down the dazzling effects of the technology so we may see the crisis in its true light.

Computer Abuses

Computer technology expert Donn B. Parker named five categories of computer abuses [13]: 1) the computer as an object of an abusive act (e.g., physical damage). 2) the computer as the basis for a unique environment in which an act occurs, or the source for unique forms of assets (e.g., theft of hardware/software). 3) use of a computer to commit an act of abuse (e.g., stealing data, theft of funds). 4) claiming available computer equipment and facilities for prestige in order to intimidate or deceive (e.g., falsely claiming ownership of computer facilities) heretofore undiscovered new methods of abuse. He further defines computer abuses as "all intentional computer-related acts in which perpetrators made or could have made gain and victims suffered or could have suffered loss [14]". I extend this definition to include all <u>unintentional acts</u> of computer (data/information) abuse even when no gain could have been made, or there was no intention of gain by the perpetrator but harm or suffering resulted or could have resulted. This extended definition encompasses all unauthorized, thoughtless, negligent acts such as disclosure or dissemination of information. Take, for example, the release of unauthorized or sensitive information by a government agency to another agency or private interest where the disclosing agency (or employee) would not benefit from any gain but the recipient of the information can possibly or actually does use it to cause harm or suffering.

SOCIETY'S BURDEN

Following are some examples of the kinds of abuses of computer technology that have occurred which the reader may find shocking enough to become outraged and be aroused into demanding appropriate and effective defenses against abuses. The suffering and loss shown in these examples are in Parker's words "only a piece of the top of the iceberg of computer abuse [15]," thus even before we get to the "submerged" abuses we find that we haven't full understanding of all the abuses contained in the top of the iceberg. In other words, our concern is not only with known and undiscovered new methods of abuse but with abuses that are currently happening, some of which may not be discovered for years to come. For example, an employee who is disgruntled or about to be fired during February 1979 may program a computer to erase all or essential parts of data files relating to an agency's activities in the year 1983 thus leaving no indication that such an act may have been caused by him. Also, an employee committing theft of funds may program a computer to cover up or erase all traces of his embezzlement.

Computer Crimes - Some dishonest business firms use computers to bilk their own customers. For example, a brokerage firm in Texas by programming in errors into their computer stole $500,000 from numerous customers' accounts by systematically

overcharging them small amounts. Whenever a customer noticed and complained about the overcharge the company blamed it on computer errors.[16]

- An Internal Revenue Service clerk in Washington, D.C. programmed a computer to list unclaimed tax-refund checks and had them sent to relatives.

- Clerks from New York City's Youth Corps used the agency's computer to "run off 100 extra checks drawn to fictitious names and in 9 months made off with $2,750,000".[17]

- Perhaps the largest known computer- assisted crime was the $2 billion Equity Funding Insurance fraud discovered in Los Angeles in 1973. Because of lagging sales, top officers of the company began inventing and selling fictitious life-insurance policies to several big firms whose business activities involve reinsurance. "The fictitious insurance policies whose face value totaled $2 billion were kept alive entirely by computer wizardry. For more than two years, the computer was used to juggle every detail needed to make them look genuine" [18]

Abuses of Privacy

There are 3.9 billion easily accessible records on individuals held within the personal-data systems of ninety-seven Federal agencies. Should these records be combined (and some have been) on an interagency basis a complete dossier can be compiled on the medical, political, financial and personal life of almost any American Citizen.[19] This extensive profile could be used without the individuals' knowledge of the actual contents and with no opportunity to verify the accuracy or quality of information and sources. When one considers the amount and extent of personal data contained in state, local and private interest data systems it can only be concluded the present state of this situation is increasingly becoming potentially harmful and threatening to our society. Consider these examples of "datamocracy".

- "Many agencies have the power to force individuals to supply information. For example, the penalty for failing to answer the 1970 census question on the number of flush toilets owned was the same as that for indecent exposure."[20]

- "The Internal Revenue Service supplies tax information on individuals to state treasury agencies, to other federal departments, and to congressional committees.

- Federal investigators have access to ...a blacklist of businessmen considered to be poor business risks from the General Services Administration; ... 264 million police records, 323 million medical histories, and 179 million psychiatric records, ...and rosters of individuals considered to be anti-social and anti-American from the FBI"[21]

Most of us would agree that government agencies and private interests need a certain amount of personal information to conduct their activities and deliver services, but, beyond a certain point, the collection of additional information can only prove harmful. Take, for example, the following abuses of individuals' sensitive information as cited at the U.S. Privacy Protection Study Commission in Washington, D.C. on August 3-5, 1978:

- Dun and Bradstreet Companies, Inc. reports on businesses, not individuals, and this is not covered by the Fair Credit Reporting Act. One witness gave testimony that Dun and

Bradstreet ought to be under the Reporting Act because the credit rating firm "...violated his privacy and ruined his business by its reporting and he obtained out-of-court damages only after a 14 year fight." [22]

- St. Louis newpaper editor James Millstone told how he risked losing automobile insurance because of an investigator's report containing "false allegations based on a brief interview with one nearly senile neighbor who had been feuding for two years with my ... family." Although Millstone sued and won $40,000 in damages, and was able to get automobile insurance he is concerned that ...this file may come back and haunt [him] some day."[23]

Commission Chairman David F. Linowes expressed concern that almost every U.S. family is affected and that the "information recorded and communicated about an individual may range from minimum identifying data to the most intimate details of personal, physical and behavioral characteristics." Also, he stated that "there appears to be a trend among consumer-reporting organizations toward ever-increasing computerization and centralization of their record-keeping operations which could

both multiply the incidence and magnify the impact of personal-privacy abuse".[24]

The Internal Revenue Service was in the process of developing a 850 million dollar computer system network with 8300 terminals around the country that "would have given thousands of IRS employees immediate access to detailed tax records of more than 103 million individuals and corporate taxpayers". [25] Ohio Representative Charles Vanik in criticizing the planned system stated that the network "could become a system of harassment, surveillance and political manipulation".[26] This is of concern in part, because evidence indicates that in years past, tax records had been "used in some administrations to pinpoint certain groups and to bother political opponents."[27] The Carter administration decided to stop the development of the network because of worries over the implications of the system in relation to issues of privacy and civil liberties."[28] Government is often the least sensitive to the impacts of its actions. However, the fact that doubts about the new uses of computers are being raised within the bureaucracy itself is another indication of the severity of potential and actual computer abuses.

Federal use of computers has grown from 2 machines in 1950 to around 11,000 in 1978 [29]. Along with this, there has been growth in state, local government and private interest use. With this increase in use have come increases in the amounts and

types of information on individuals in personal data systems and a variety of other targets for computer abuses. The growth in the availability of new, less expensive computers has brought changes in all areas of government activities, business, education and personal use of computers. There is some indication that government is starting to recognize the extent of computer technological use and abuse in a new entity in the U.S. Department of Commerce - the National Telecommunications and Information Administration (NTIA)" [30]. However, what is needed is not another inert powerless bureaucracy but an effective agency that will have the power to regulate and administer all computer-related activity. To reach this goal the strategies for public and individual protection that I recommend are shown below. Also shown, are strategies (actually responsibilities) that management can use to aid in attaining this goal:

Regulatory Agency Strategies. An agency is needed to act as the single administrative tool to monitor computer-related activities within the U.S. and any involvement outside the country (e.g., a domestic corporation doing business in a foreign country). Whether this agency be NTIA, an arm of the department of Justice or some other appropirate agency, or a totally new agency is not significant; what is important is that the agency eliminate where possible existing ineffective agencies that have responsibilities for computer activity and

coordinate and be responsible for the operations of remaining agencies. The agency's overall mission should be to protect individuals and society at large against computer abuses; in order to accomplish this the agency should have the power to:

- Study and investigate the present state of the art and the abuse of it in order to determine where society now stands and what direction should be taken. This should be accomplished by viewing all the problems on a macro and micro scale.

- review and analyze all current applicable legislation for effectiveness, appropriateness for current technological circumstances, and for those areas in which present laws may be in conflict (i.e. The Privacy Act of 1974 may have restrictions from disclosing certain information to an individual, agency or private interest while the Freedom of Information Act may require disclosure of that information). Amend existing legislation or design new laws that will allow a degree of flexibility to cover areas previously beyond the reach of the law and provide for protection against new or unantipated use and abuse.

- adminster and enforce applicable areas of existing legislation relevant to computers and data/information systems that will employ as a combination (a cohesive package) such laws for the benefit and protection of society and the individual. The agency should be able to investigate, adjudicate, levy fines and sentence (or recommend for trial for criminal charges) all incidents of abuses.

- set restrictions as to exactly what kinds of data agencies and private interest can have and specify to whom and to what extent it can be disclosed; put an immediate halt to the collection of non-relevant and excessive data; require and enforce the removal from data files all information determined to be irrelevant and/or harmful.

- educate the general public concerning the agency, its mission, pertinent legislation, individual rights of privacy and security, and available remedies for abuse and methods of pursuing them.

- educate and advise persons having direct or indirect access to computer and data/information sources of the certainty and swiftness of punishment for wrongful disclosure or acts. This can be accomplished through such things as trade journals, publications and announcements for posting sent to agencies and private interests, and also through effective licensing requirements. Similar methods can be used for private residential users; for example, in licensing regulations it can be required that purchasers register pertinent data (as is done in applying for a hand-gun permit in may states) be required pass written examinations (initially and periodically) that will demonstrate knowledge of relevant legislation and penalities for abuses. Of course, the degree of regulation would correspond to the degree of the computer capability.

- set and enforce standards of physical security for protection against natural and unnatural disasters (e.g. terroism, fire, etc.) Act as a consulting agency for assisting in the attainment of adequate

physical security. This can be done through actual visits to facilities for on site inspections.

- require high level security safeguards in existing systems, equipment (hardware and software) ready for marketing and for future technological development. Security safeguards for computers and data/information files of a highly sensitive nature (i.e. such things as national defense data storage systems) would have to undergo initial review and approval and before being marketed or put into use and be subjected to periodic inspection and testing after installation and use. Licensing and employment requirements would be much stricter.

- Undertake research in full or jointly with industry to develop adequate computer and data/information safeguards; subsidizing the costs of increased security by tax credits, grants, loans, etc.

Although possibly in conflict with the ideals of privacy and civil liberties, it may be necessary that monitoring and controlling system be developed that can track the movements of

key personnel (i.e. having access to highly sensitive and critical computer and data/information resources) should they cause concern over any suspicious activities on their part. For instance, certain data systems can be programmed to alert computer security managers when a critical employee applies for a passport to leave the country. Even though these measures may restrict privacy and civil liberties they may be necessary in the "public interest" and under these circumstance controls on a few to protect many may not be an outrageous concept.

Another Bureaucracy? - It is difficult to deny the fact that many bureaucracy are inefficient and ineffective more often than not, but this is not necessarily. A single regulatory agency to administer matters of computer technology can be efficient and effective by operating under the proper conditions and by asking and answering the following questions:

- what is the problem? define it, how does the present state of the technology effect society in matters of use, abuse.
- what are the specific goals and objectives to be accomplished? The overall mission of the agency? Define and set goals and objectives clearly.
- what are the present weaknesses in current safeguards; where are additional safeguards

needed?

- what is needed to prevent and correct abuses, methods of detection
- how effective are penalties in present legislation, are they fully enforced?
- What areas of abuse are not covered, or covered ineffectively in present legislation; for example, the Fair Credit Reporting Act does not cover businesses (private concerns) but should be extended to give them protection.
- is current (and future) legislation flexible to cover undiscovered and unanticipated abuses?
- how can the agency work <u>with</u> the computer industry and those in the field to develop adequate safeguards in all aspects of the technology; what can the agency do to fortify the security of systems currently in use (i.e. physical plant, programming, data files, etc.)

This is only a sample of important questions and points that should be considered. What is important is not necessarily the

quantity of the questions but the quality, in other words, to be efficient the agency must have a clear understanding of what it is that it wants to accomplish and how it is going to go about it. Sounds too simplistic? Many agencies are ineffective and inefficient precisely because they don't consider and answer these questions at the beginning of their operations or with each new program they undertake.

The Industry - According to Parker [31] sufficient security cannot be expected for 8-10 years. I ask why? Why can't security measures be devised at the time when the hardware and software are being developed? Is it because it is too expensive? Hasn't the industry recognized its responsibilities in this area? Industry and government can and should work together to develop appropriate safeguards. Through lack of vigilance we have allowed privacy and security safeguards to fall far behind the development of the technology and now we must pay the price of our negligence. Most likely the initial costs of developing safeguards will be high but after the security technology gets underway the costs should become less. What industry can do:

- be willing to make honest efforts in working with the government in the development of computer security technology
- be willing to share in the expense when able

and allow for a gradual recovery of costs.

- assist and advise current and future users of various security precautions (e.g. physical location of computer facilities, devices for use on equipment and in programs, building security features into overall computer activities)

- work with the regulatory agency in the analysis, amending and creation processes of legislation. Recommend changes or additions to the legislative package as needs and situations arise. Lobby for important legislation.

Industry must recognize its responsibilities in this matter and immediately put more effort and resources into the research and development of adequate privacy and security protection safeguards. No longer can industry be allowed to create computer "monsters" and sit back to watch the harm and suffering they cause.

The Manager's Role

The manager should not expect to sit on the sidelines and watch the issues of privacy and security play out before him. There are certain strategies that a manager should employ to aid

in furthering the cause of privacy and security for the benefit of his clients, customers, etc. This is no longer his choice but his responsibility, at least to the extent of his control and capabilities. Managers will increasingly become more accountable for the use and abuse that their computers and data/information systems are being put to. Some strategies the manager can use are:

- collect no other data than what is truly essential to conduct the operation activities.

- be actively involved in the planning stages of new computer facilities and resources and in modification/additions to current resources. Demand from vendors of hardware and software as much security safeguards as is presently available, or can be made available. Place privacy and security considerations as a top priority in selecting equipment and program purchases.

- be knowledgeable in computer technology and its jargon to the extent that he can recognize and resist "snow jobs" from consultants, vendors and computer personnel when they make false claims that "This

security measure can't be done...."

- be aware of threats to physical security of computer facilities data/information systems. Consider proposed or present location of facilities and data/information storage; this category ranges from the larger considerations (e.g., if the computer installation is in the basement it may be very vulnerable to flooding) to seemingly minor (but very important nonetheless) details concerning such matters as types of doors and locks leading to storage areas." [32]

- know the relationship of legislation to the kinds of data and information his activities are involved in. Is sensitive information being routinely released without his knowledge? (this could be for the personal gain of an employee or unintentional negligence). What information formerly considered unimportant or not private should be reclassified as being sensitive.

- voice his opinions: make it known through professional associations, to the regulatory agency and industry associations when he discovers where new weaknesses lie or has constructive suggestions that will strengthen privacy and security safeguards.

- be actively involved to the extent possible in setting standards for personnel selection, employee actions; at the very least he should demand high standards of the employees under his control.

- demand accountability: educate his employees as to their responsibilities and the fact that they will be held accountable for negligence and abuse, intentional or unintentional.

This is only a partial listing of methods that managers can pursue in order to assist in affecting change in a direction away from computer abuses. By giving serious consideration to his particular circumstances the manager will discover areas of weaknesses and solutions to improving them and methods of future prevention that are unique to his activities. The manager should not hesitate to ask for assistance and advice from consultants regarding privacy and security. In the past

managers were able to slide by privacy/security issues by remaining aloof from the realities of the seemingly separate world of computer technology with the excuse that it is beyond their realm of knowledge and control, however, this excuse is no longer valid.

Along with computer technological advancements having an increasingly expanding impact on individuals and society the manager will be held increasingly accountable for the abuses to privacy and security caused directly by him or indirectly through the personnel that he is responsible for who have access to computers and data/information resources. The competent manager will realize that strategies for defense against abuses are, in reality, his responsibilities and will make every effort to end abuses.

CONCLUSION

In his 1971 article "The Information Revolution - and the Bill of Rights" Jerome B. Wiesner warned of the possibility of our society becoming inconspicuously overwhelmed to the point that we will be "information-bound" and have the characteristics of a "1984". His concerns were with the fact that "knowledge is power.... [an]... [i]nformation technology put vastly more power into the hands of government and private interests that have the resources to use it"[33]. He further believes that we must recognize and counteract a danger that may result from the

abuse of "computer and communication technology [that] could so markedly restrict the range of individual rights and initiatives that are the hallmark of a free society and the foundations of human dignity" [34].

The great danger we must address and prevent is that "such a de-personalizing state... could occur without specific overt decision, without high-level support and totally independent of malicious intent ... [and that] ... we could become information bound because each step in the development of an information tyranny appeared to be constructive and useful"[35]. Why the reference to a 1971 article in the year 1979, especially in relation to such a rapidly developing field as computer technology; why are Wiesner's comments appropriate today? They are appropriate today because although the technological advancements gained in the use of computerized information systems have been astounding the technological achievements for controlling and eliminating abuses have lagged dangerously far behind. For example, in his 1978 testimony before the U.S. Senate Committee on the Judiciary subcommitte of criminal law and procedure, regarding S1766, the Federal Computer Systems Protection Act of 1977, Parker spoke of the future abuse of the technology. He stated that the "future of computer abuses can be anticipated on the basis of known experience. Massive fraud, organized crime activity, physical and mental harm to people, violation of personal corporate privacy, tapping of data

communication, violation of intellectual personal corporate privacy, tapping of data communication, violation of intellectual property, terroism attack ... computer output hoaxes, time-accelerated fraud, and geographically independent fraud must be anticipated to produce adequate legislation"[36]. Parker further stated that future crime problems should be anticipated in order that they may be included with the legislative considerations of the current bill" [37]. Thus, what Wiesner said in 1971, Parker is in effect saying after a lapse of 8 years: little, if any, progress has been made toward easing the individual and society of the burdens placed on it by computer abuse and that this sould be a major concern of ours!

Wiesner warns us of an information tyranny, Parker also relates to an information tyranny and crimes involving computers. The present state of computer security is the reduction of "... the potential threat of crime among large areas of people who lack sufficient computer skills and knowledge, however, it is putting far greater trust in the hands and minds of the few who have sufficient skills and knowledge to compromise the systems" [38]. Does this fit into the definitions of information tyranny and datamocracy?

Causing further alarm is the fact that there is no expectation of the development of adequate safeguards in the immediate future to protect the individual and society from computer technological abuses. "The design of commercially

available computers is not yet technically secure from these highly skilled people, and sufficient security is not expected for at least 8 to 10 years. Safe in their realization that they cannot be prevented nor detected if they are careful enough, these technologists can do anything they please in sensitive ... systems" [39]. What does all this mean? It means that it is essential that we take a "stop, look, and listen" posture in the computer world around us in order to seriously review and analyze our present position regarding computer abuses. We must make a concerted effort to protect ourselves against computer abuses. Indications that a datamocracy or information tyranny (or whatever designating term you choose) may be close upon us are plentiful; we must not let ourselves be overwhelmed - we all stand to lose!

SECTION II

ISSUES IN PUBLIC ADMINISTRATION - A LITERARY REVIEW

COMPUTER TECHNOLOGY AND PUBLIC ADMINISTRATION IN STATE GOVERNMENT - THE NEED FOR A NEW PERSPECTIVE

by John A. Worthley and James J. Heaphey

THE PROBLEM: ANACHRONISTIC ORGANIZATION PROCESSES

Worthley and Heaphey state that the current use of computer technology in public administration is as pervasive as it is in private industry. This widespread use of various forms of the technology is found at all levels of government - federal, state and local. As a consequence public manager face a daily confrontation with a technology to which they "must relate and work through or around" [40]. Here we find the symptoms of a more deeply hidden causal factor. Public managers should not have to work through or around computer technology but should work with it and have it work for them. Instead of providing a vehicle for maximizing efficiency in their data processing output the technology is (in many cases) causing stress in management functions.

The advent of computer technology held the promise that these developments "would make the job of the administrator easier and his/her performance better. The experience has not matched the promise" [40]. Instead of a state of nirvana manager find themselves in a "technological hell" - they are constantly faced with phenomena they don't understand and, in many cases, fear. Although they tell data processing personnel what their information needs are they are provided with

information that the electronic data processing units (EDP) decide managers should have. Public managers find that the EDP units have collected, programmed and organized data in a way that is not only incompatible with their needs but aggregate into "data pollution" [40] which they find overwhelming and complicating managerial tasks. The lack of the required time needed to sort through reams of computer printouts in order to locate significant data in order to compile meaningful and timely informational reports has caused a number of managers to maintain the old manual data systems [40]. Thus many organizations go through the motions of utilizing computer technology for data processing at the compounded expense of computer personnel, equipment and facilities in addition to the costs of maintaining the manual system. The result of this is a very poor return on government investment. However, the authors believe that the economics of investment return and dealing with the technological implications of computerization are not the true problems. The failure to obtain maximum efficiency from computer technology is an organizaional problem.

According to Worthley and Heaphey "the problem is not a matter of the computer failing to help the public administrator do his job better; rather the problem is that the computer is often impeding the public manager from doing his job at all" [41]. This is because "the technology has changed the organizational environment within which we must operate" [41].

The technology created a need for new approaches and viewing of organizational structure. Because computer technology is so ubiquitous in public administration the technology can no longer be ignored as many managers have been doing" [40]. when facing the reality that we cannot return to "those simpler, non-automated days of yesteryear" we find that we are in a serious predicament. The failure to maximize computer efficiency "lies in a mismatch of information technology and organizational design, information technology has drastically changed while organizational processes have remained the same. The organizational processes utilized today were designed for coordination of fragmented, scattered and limited pockets of information. Compuerized information systems are, on the other hand, integrative, unscattered, and quite unlimited. They are concentrated and overabundant systems. Thus, in terms of information realities we have anachronistic organizational processes" [41]. These outdated organizational processes (the organizational structure) interprets into the organizational problem.

The authors say that, traditionally, organizational processes were designed to deal with mechanical work processes concerned with coordinating the division of labor; however in an automated age "organizational processes need no longer be determined by work division units because work division units are no longer required... Work units today are largely complete

units unto themselves. The problem is that we attempt to deal with these units through an authority and decision-making structure which presupposes interdependency of work processes" [42]. Although work is still done in units "these units need no longer be considered parts or divisions of larger work units for information processing" [42]. In other words, instead of being dependent mechanical processes, today units function as independent subsystems even though they are parts of an overall system.

In organizations today information for decision-making is normally gathered and compiled by persons who are completely separated from the decision-making process. This organizational separation of the information function from the decision function increases the chances that irrelevant information will be presented to public managers for decision making. Although modern technology has greatly improved information processing it has undercut information relevancy [42]. In brief, the authors are saying that organizaitonal structures have not adapted to modern technology and "by trying to deal with computer technology as we did with machine technology, managers may become more and more handicapped" [42].

THE SOLUTION: A NEW ORGANIZATIONAL PERSPECTIVE

Worthley and Heaphey believe that we can no longer ignore the organizaitonal implications of modern information technology

and that "a new perspective is needed by public managers if computer technology is to assist rather than impede public administation. Such a perspective should, as a beginning, focus on managerial knowledge, user involvement, and organizational adaptation" [43].

Managerial Knowledge

One of the most serious problems of computer usage is a fear of the technology by public managers. As a consequence the management and use of computer technology has been left to technicians or to outside consultants. There has been a communication gap between managers and technicians because of a presumption of the inability of these two groups to relate to each other. This situation is further worsened by the specialized jargon of computers as well as time constraints on managers preventing them from learning more about the technology [43].

The authors are not suggesting that public managers need to become experts in computer technology but that the technology can be mastered. It is not so complex as the jargon and aloofness of the technicians would lead us to believe. The authors suggest that there should be an increased interaction by schools of public administration and relevant literature to help overcome this problem [44]. Also, to develop familiarity and comfort with the technology requires an investment of time

by managers. Because this investment "should no longer be considered a luxury" [44] it is now necessary that organizations recognize this fact and in some manner (i.e., scheduling during work hours; compensation for personal time invested) allow for this.

The range of managerial knowledge should include:

- what it is to program a computer,
- and understanding of the implications of the technology for privacy and security,
- an understanding of designing modern information systems
- knowledge of what the technology can do to them as well as for them [44].

User Involvement

The authors state that the "public manager who receives and needs information output must understand it, must determine its format, must plan it, lest the output be polluted, disorganized, and irrelevant" [44]. Managerial involvement in the design and operation of computerized information is very essential to the success or failure of computer usage. User involvement is needed to clarify goals and identify needs. Yet as decision-makers, public managers are seldom even involved at all. Instead, the "common practice is for the EDP function to be relegated to technicians in a staff relationship organizationally remote from the manager who needs to use the data" [44]. However, we expect that the information we receive will be relevant

to our needs. User involvement is needed "in order to prevent automation of nonsense and consequently output of irrelevencies and creation of data pollution" [44]. In summary, managers who use the information should be involved in the design and operation of data processing system in order to manage effectively and efficiently.

Organizational Adaptation

The authors new organizaitonal perspective also "includes consideration of the implications of the technology division of labor and decentralization notions that work units also function independently. Major adaptations ... might at least be contemplated for the long term, and adjustments might be considered immediately" [44]. In other words, organizational adjustments must be made to give managers more actual interaction with the EDP departments.

Another aspect of the concept of organizational adaption is the "fact that the public manager operates within a political context, and that there are various political reasons why change is difficult to realize" [44]. The authors use the politics of job protection as an example. Obtaining a proper balance of organizaton and computer technology may require some job elimination. Part of the politics of public administration is to protect jobs. Also, there are "situations in which actions by people on the line must be answerable for... in terms of political repercussions; this will be a constraining force on the willingness to adapt" [44].

The phenomenon internal, interpersonal relationships in organizations is also a critical consideration in organizational adaptation. We find situations "in which management not only fails to understand the nature of the problem being analyzed and criticized [the relationship between organizaitonal change and computer technology] but also uses a defense mechanism to justify the status quo." [44] The manager does this to prevent the disturbing of internal, interpersonal relationships.

Another dimension of organizational adaptation concerns the large financial investment made to computerize. Rather than openly admitting inefficeint and ineffective use of computer technology, many managers find it easier to maintain the status quo. The authors provide the following scenario to illustrate this:

Many bureau chiefs assure that they have an alternate source of information by maintaining the old manual system, using it for all their needs, and thus can tolerate the existence of the computer. However, a problem arises when a commissioner believes the information system operates as he has been led to believe and actually does try to use the technology for management purposes. He requests deliery of a report within one day (which the computer has the ability to do) but the bureau chief (dependent on the manual files) is "unable to respond in less than a week. The manager claims that this time lag is evidence that more personnel are needed [40].

The authors suggest that new organizaion perspective is needed because modern information tehnology has caused an organizaitonal information mismatch. This mismatch has made information integration difficult. They further state that there are no easy answers because there is little experience in operationalizing such a new perspective. However, they believe that "experimentation by individual managers in individual organizations is perhaps the necessary first step ... to improvement." The intent of the article by Worthley and Heaphey "has been to begin the kind of thinking they believe is needed to inspire and assist such an effort" [45].

THE NATIONAL CRIME INFORMATION CENTER (NCIC) OF THE FBI: DO WE WANT IT?

By Stanley Robinson

NCIC is a nationwide automated police information network. Teletypes connected by telephone lines to state police computer center are installed at local police stations. The state police computer centers are connected to a central computer in Washington, D.C. The central computer center is operated by the Federal Bureau of Investigation which stores and searches records on-line with both state and federal computers. The system is designed to provide immediate information of a criminal justice nature ranging from revoked drivers' licenses to stolen guns and narcotic drug intelligence. Robinson believes that these services currently hold great potential for abuse. He states, for example, that policemen are instructed to arrest "suspicious" persons for disorderly conduct in order to perform an NCIC record check [47].

Robinson finds the future of the system even more frightening than the potential for current misuse. His fear is based on the great amount of uncertainty in relation to NCIC:

1. "Future plans are in state of flux;
2. Officials responsible for those plans insist the planning is confidential, and the public will be

notified only after decisions are made;

3. There is some variation in conception among the different sources [he] consulted; and

4. Part of the sales talk for NCIC is that it is infinitely flexible and expandable" [47].

THE PROBLEM: THERE ARE REASONS FOR ALARM

Robinson believes that NCIC should be a "growing source of alarm for all of us who are concerned with human rights - especially the rights of those who are black, poor, or politically unpopular" [46]. His article gives reasons for alarm and explains his challenge of local police hookup (which, as will be explained, later is part of his solution to the problem). Robinson's alarm revolves around the following issues:

- the number of records, their content and quality
- plea bargaining
- the potential for a police state
- privacy, etchics and civil liberties: suggested polices to safeguard these are weak
- possible other misuse of the system against citizens; the very basic premise of NCIC that police need arrest records and can use them safely

- the methods of funding and "selling" the system
- the system contains the ingredients of a "police state"

The Records

NCIC Would give its users rapid "electronic access to 19,000,000 individual citizens arrest records - nearly 10% of the country's population" (1971 figures) [47]. Called "criminal histories" these records will assist police in making decisions concerning arresting, seaching, detaining, questioning, and investigating suspects and offenders [47]. Robinson finds the term "criminal history" offensive because it makes it sound that anyone who was ever arrested has a history of criminality. He also believes that the poor quality of criminal records is reason enugh that they not be used as a guide for police action. He bases this on the following reasons:

- many forms of arrest records do not note dropped charges nor results of trials and appeals
- even when complete records are kept, arrests that were unfounded or did not stick are listed, creating a suspicision or presumption of guilt which can lead to further arrest and harassment.
- the belief by many policemen, judges, employers and society in general that "a person doesn't get arrested unless he was asking for it" [47].

Plea Bargaining

Records containing conviction information often contain the result of the courtroom practice of plea bargaining-agreeing to plead guilty to a lesser offense). Although an attorney may be able to get an innocent person acquitted of unjust charges (judged not guilty) such legal assitance is expensive. Also there is still the chance of losing, even on appeal, which costs even more. "Therefore, many individuals agree to plead guilty in exchange for a reduced fine, reduced or suspended sentence, or probation. The same idea extends to appeals of unfair trials: making an issue of anything is expensive and risky" [47]. Thus we have a situation in which an innocent person may have a record of conviction that police will use as a basis for future police action. As Robinson states: "Nowadays citizens can be arrested unfairly, searched illegally, charged with violating dubious laws (disorderly conduct, ... loitering, conspiracy), and railroaded into prison by ignorant or vindictive police, prosecutors, and judges ... Yet, in the name of modern law enforcement, all these arrests and the convictions that go with them will go into the NCIC system" [48].

Police State

Robinson is concerned that computerizing and centralizing arrest records - complete or incomplete - and allowing routine access by local police departments constitute the "ingredients of a police state" [48]. He states that the best that we can expect from this situation is that "discriminatory law enforce-

ment and harassment practices will be cascaded, because an arrest becomes a justification for another arrest, and so on. [He has] never seen any evidence that this kind of law enforcement helps prevent crime" [48]. However, he does believe that there is growing evidence of the day-to-day effect of such a system on individual's lives. The systems effect is in the areas of "free speech, free association, free petition for redress of grievances, etc." [48].

NCIC Concern About Privacy and Ethics

Robinson's alarm over these issues stem from the fact that in the policies suggested for safeguarding these concerns the concept of discriminatory or politically inspired arrest and harassment are not even touched upon, nor are the "self-fulfilling properties of "criminal histories" [49]. He cites "four major concerns about data banks in relation to human rights:

1. loss of privacy through security loopholes
2. transactions about individuals without their being notified
3. merging and correlating dangerous information from diverse sources, and
4. operational without principal supervision

NCIC has no features that satisfy a single one of these concerns" [50].

Other Potential Misuse/A Weak Premise

Robinson regards NCIC to be dangerous because of its "basic premise that police need arrest records and can use them safely" [50], however he finds no evidence to support this thesis [48]. In addition to this being an unfounded reason to have a centralized data bank of criminal histories Robinson states other reasons for alarm:

1. "NCIC forms the basis for a total 'gestopo' (literally 'secret federal police') system, since the public has no access to its data, nor is any person notified of inquiries and transactions affecting himself. It could take the last vestiges of the 'criminal justice system' entirely ot of public hands.

2. The addition of surveillance data to NCIC is but a small step, technologicaly. The modern, aggressive style of surveillance and infiltration needs computer resources just like this, and there are reasons to believe the NCIC system would be used for surveillance data.

3. NCIC could easily be used in the administration's [federal] preventive detention program and in gathering data for future 'conspiracy' indictments.

4. The FBI runs NCIC. It's large scale undercover surveillance activities force one to view the FBI's ethics with suspicion, to say the least.

5. Computers are notorious for making mistakes themselves* as well as transmitting unevaluated data, while policemen may well believe 'anything a computer tells them'" [50].

Who Pays For NCIC? Who Sells It?

Another issue that causes alarm is Robinson's belief that the structure of financing used to defray the cost of NCIC equipment and operattions is being used to avoid issues of democracy (substantial dangers to human rights). Aimed at persuading local town officials to hook-up to the system the finance structure, along with "selling techniques" by a private "interest" are used to increase the "reaches" of NCIC [50]. Robinson gives the example of towns in Massachusetts:

To join NCIC the towns need only pay their individual Teletype rental ($2000 annually in 1971). To encourage towns to

* It is my contention that computers do not make errors - humans do! Computers can only do what they are programmed to do, therefore 'computer error' is really 'human error'. But this is another issue not to be discussed here.

join a 40% federal subsidy was provided. Also subsidized federally are expenses borne by the state (including lines and computer center operation). Under the Safe Streets Act of 1968 the rest of NCIC is 100% federally funded. "We all pay for NCIC, of course. But the fragmentation of payments fosters a carefree feeling among budget-minded local and state officials that 'somebody else' is paying". [50].

Even though town officials may be attracted to NCIC by its "apparent bargain price" they may still question the merits of the system. "To minimize this problem in [Massachusetts] the sales staff of New England Telephone Company (supplier of lines and teletypes) visited 117 towns [during a year] to educate local boards and committees on the need for NCIC in modern police operations" [50]. After hearing one of those sales talks Robinson states: "It was very smooth and professional indeed. Human rights were not mentioned. The officials present agreed 'the advantages outweight the disadvantages', and incorporated NCIC in their towns budget" [50].

THE SOLUTION - LOCAL CHALLENGE TO NCIC

In a Wayland, Mass., Town Meeting on March 8, 1971 Robinson was defeated in an attempt to delete the NCIC budget line until "further investigation and a full explnation" of the system. However, despite angry opposition he was able to introduce and carry by majority vote of those present the following motion:

"Moved: That the Police Department be directed to include in next year's Annual Report a statistical tabulation of its usage of the NCIC computer system, including the following information if at all possible:

1. number of inquiries by type of inquiry and reason for inquiry

2. Results of inquiries, including arrests and known convictions

3. A similar summary "entered" by Wayland police, and

4. Troubles encountered (down-time, false arrest, invasion of rights, etc.)" [51].

Robinson's challenge begins locally and includes various aspects of accountability. In other words, rather than allowing the advent of the system to quietly occur, he believes the implications and potential impact of NCIC should be recognized from the outset. Officials consenting to the implementation of the system should be aware of its use and misuse and be held responsible for them.

Robinson is hopeful that the reporting system approved in the town of Wayland will "accomplish one or more of the following objectives in addition to generating a list of features and how and why they are used:

1. Stimulate discussion and questioning of NCIC by exposure to the public of its existence;

2. Abate the chilling affect on free speech, association, etc., by removing the veil of mystery from NCIC operations;

3. Deter questionable operations by the police by requiring an accounting of such operations (thereby opening them to criticism and veto);

4. Convey the doubts of concerned citizens about NCIC to town fathers, police, state officials, legislators, and Congressmen;

5. Stimulate public realization of the sham of the so-called "criminal justice system" in which NCIC is grounded; and

6. Give people courage to demand public accountability of all governmental functions, computerized or not.

The objectives could be served if the police misconstrue or falsify the required report! Actually the report will be difficult to falsify because all NCIC transactions are logged verbatim at the state level, thus facilitating crosschecking.

Finally, if town officials fail to report as directed, perhaps because of secrecy statutes, then outraged citizens can demand removal of NCIC from the police department. (Wayland

officials have indicated they intent to cooperate...)"[51].

Debating NCIC at town meetings provides some hope of controlling or at least influencing, the widespread implementation o the system [52]. Robinson believes this is important because "all repression and manipulation of public trust could be related in one way or another to this alleged anticrime computer system" [51].

Through indirect financing and professional selling techniques, NCIC has begun operating with little awareness or approval of the public on which it impacts [50].

Proponents of NCIC argue that police departments already have 24-hour, 5 minute telephone access to nationwide arrest records for any individual. They claim NCIC will provide fairer, more detailed and accurate arrest records. Also, the system's fast response will allow cleared suspects to be relased sooner,* and arrested persons with clean records to be released on recognizance, thereby enhancing civil liberties [48]. Robinson contention is that regardless or accuracy, arrest records do not constitute probable cause for arrest, and detention without bona fide arrest is illegal in any case. Also, he believes that selective release on recognizance is

* Why can't these practices be followed with the present "5-minute access"?

actually preventive detention in disguise. Another fear is that "police access to arrest records will be stepped up tremendously by NCIC thereby damaging civil liberties irretrievably" [48].

Thus, we can see that Robinson's alarm is seeded in many issues involving the use and misuse of the NCIC system. These range from the very basic premise of the system that police need arrest records to make arrests to issues involving privacy, ethics and civil liberties in general. His concerns are mainly of what the future of NCIC holds for citizens - "gestapo" police actions, surveillance, etc.? Strategic defense against the NCIC system has its origins in local challenges.

* * * * * * * * * *

Implications for the Public administrator

Robinson's alarm over the potential abuse of sensitive information contained in individuals' records also applies to any data bank. Whether a large centralized system, as NCIC is, or one of a smaller scale (as may be the case in a local agency) the abuse of sensitive information can cause great harm and suffering to individuals. The point here is that managers should strive to act responsibly and expect to be held accountable for their actions.

As explained in the "The Manager's Role" (Section I, page 24) there are strategies that public administrators can use to help safeguard citizens' privacy. The list is not exhaustive

and thus the administrator may find steps he can take that are peculiar to his agency or situation. at the very least, the manager should have an awareness of his information system's potential abuses.

COMPUTERIZATION: PANACEA, OR PART OF THE PROBLEM?

By Richard E. Anderson

Anderson's article refers to the subject of computerizing municipal functions, that is, installing and operating computer driven Integrated Municipal Management Information Systems (IMMIS) in cities. He contends that public managers "are in trouble and do not even know how to find out how much"[53].

THE PROBLEM: BEING GUIDED BY MYTHS

Anderson believes that managers have accepted and are perpetuating an extraordinary number of myths about computerization. Although he gives numerous examples, some of them are:

- that computerization simultaneously reduces the workload of operating departments, the number of employees, and expenditure levels;
- that computer salesmen can best determine what equipment is neeed;
- that programmers can allowed to be inefficient simply because there is excess core;
- that multiple copies of reports are required, even

though most users (including managers) merely transfer them from the "in" to the "out" basket;

- that expensive, on-line, real time capabilities can be used economically for most applications. [53].

Although installing an IMMIS has intrigued managers, there has been few examples of success. This is because "few managers have but the vaguest notion of even what such a system might entail". Rather than having accurate data readily available in a proper format to apply to day-to-day problems we find a negative effect of the system. Too often obtaining the data requires more time and costs more money than the penalties for suboptimizing the solution of a problem, and frequently actually becomes part of the problem" [53].

Anderson is not positive that even the experts of computer technology understand or are able to solve the problem. He has "concluded that even if the 'experts' really understand the problem and have chanced on a solution, they are not (or at least have not been) anxious to enlighten the rest of us" [53,54]. Moreover, managers do not seem concerned that there is a problem or that they are in trouble. The author states that he seriously doubts that managers really know what is going on. Compounding the problem is the fact that "intuition, which has served managers admirably in so many areas, seldom can be depended on where computers are involved" [53]. An additional

concern is the fact that few cities have an adequate staff of analysts to be able to determine objectively which functions should be automated and in what priority [54].

All of these singular problems formulate into a basic problem: public managers really don't understand how a city functions in terms of data generalization and flow. These functions have not (or at least have not sufficiently) been examined from these particular perspectives [54]. As a consequence, managers allow themselves to accept and perpetuate myths regarding computer technology.

THE SOLUTION: STEP BACK FROM THE TREES

Anderson is not advocating wholesale discarding of present operating systems, nor is he compaigning against purchasing new systems. He is trying to get public managers to stop and take a look at their present situation. He recommends that managers "at least step back from the trees long enough to decide what kind of a forest [they] are in and, more importantly, what part of the forest" [54]. By doing so managers can start getting to the roots of their problem. However, managers should not expect the situation to be solved overnight, or in the immediate future. He states that "developing a truly integrated system will cost about twice as much and will take about three times as long as the most liberal estimate" [54].

This not only structures his position in the system, but forces the manager to become more involved, or

- assign a qualified systems analyst to report directly to major using department heads. "The burden should be placed on the user to demonstrate their conceptual understanding of their functions and how they interrelate, and to present the justification for proposed additional applications" [54].

Bridging the Communication Gap

"Data processing personnel have developed some rather curious techniques that are often counter-productive. As a group, they seem to make little distinction in what they are planning to do, and what they have done... They... review a department head's requirements, determine what he wants, and then provide something quite different without being overly concerned" [54]. In brief, there is a communication gap between public managers and data procesisng personnel. Anderson states that we must somehow "improve both the level and extent of our communciations if we are ever to understand what we are saying to each other. perhaps a new computer 'language' is required" [54].

Justification of Systems

Anderson challenges the public manager to take a critical look at what he is actually doing. He questions: How many managers that have computer systems today truly believe that they could justify them on a cost/benefit basis to an impartial observer [54]?

The author believes that it is possible to attain an integrated system and that it will ultimately be discovered that there is considerable transferability of an organization's applications. Moreover, "without such an integrated system, urban government as a delivery system for municipal services as we know it will not survive. In the future, it may be that the internal organization of local government will be replaced by a new functional structure designed around the use of data"* [54].

In sum, Anderson is saying that it is time that public managers take a critical look at their relationship to computer technology. No longer can they afford to be oblivious to the world around them. No longer can they accept and perpetuate the myths surrounding computerization.

---

*This parallels Worthley and Heaphey [40]; see page 32

MASTERED OR MASTER?

Erwin D. Canham

The Problem: Computers Controlling Society or Society Controlling Computers?

This article brings to one's attention the fact that we must make a decision regarding the use of computer technology in our society. The alternatives are "whether to permit computers to pull us into a robot society, or to control them so that we attain higher degrees of freedom than were ever believed possible before" [55]. An example of a higher degree of freedom is a return to individualism.

The author finds it ironic that although machines brought in the industrial revolution and created a "mass society", the most sophisticated of those machines - the computer can make it possible to return to individualism. "Data processing can usher in a whole new age of indivudalizing" [55]. Individualism would lie in the various applciations of computers. For instance, the computer may make it possible for:

- consumer products to be styled to personal tastes
- education to be paced to a student's individual abilities

- new media or entertainment could be available exactly to individual choice [55].

Individualism is not the problem, however. While the computer holds exciting possibilities for individism, it is "also a formidable force in the realm fo decision making. Here ... is a great challenge and threat. Will we be sure not to give the computer ultimate decisionmaking power? Will we always set it up so as to present alternatives, from which men and women can make their choices?" [55]. Canham believes there is the danger that we might trust to the computer certain decision making tasks "which must be the responsibility of men's consciences, striving to reflect the utmost wisdom" [55].

The challenge and threat do not lie in computer technology. They lie in the use or abuse to which men put the technology. "Mankind has faced this problem before ... He has not done too well in avoiding the hazards. He has learned to control the machines better than he has learned to control himself" [55].

Thus, we have the problem of selecting among two alternatives: to use or abuse computer technology. Will we control the technology to allow us freedom of choice? Will we allow the computer to take the place of conscience and humanitarian considerations in decision making processes. For example, in decisions of war and peace "elements which cannot possibly be physically programmed must be included in the

decision process: moral and ethical and spiritual considerations must have their part. And the possibility of error must be rigorously surveyed and prevented" [56]. An easily solved problem? An obvious choice among alternatives? If so, why has mankind failed to do well when facing this type of problem before [55]?

The Solution: Master, Not Mastered

How can we prevent the prediction: "Pessimists say that some day computers may run men instead of men running computers" [55] from becoming a reality? Canham advocates an awareness of the implications of computer technology for society. This awareness involves knowledge of the use and abuse of the technology in relation to an individual's immediate environment and the potential far-reaching consequences of his actions. Those who collect or have access to information of a sensitive or critical nature (privacy; war or peace) must use it for the benefit of mankind. Those individuals who have control of the technology - computer equipment and its operations - must put their functions in proper perspective. Canham, quotes Dr. Simon Ramo, who says this very profoundly: "...the same system that can tell millions of people exactly what to do, as though they were robots, can just as well ask them to choose what they prefer to do from a group of well-presented alternatives.

But even such a process is only partly objective. The selection of alternatives and the manner of their presentation involve many value judgements" [57]. We must be sure to provide "wise safeguards against hasty decisions of an omnipotent majority. Rights of minorities, even of individuals, must be safeguarded" [56].

Man must remain a close partner to the computer. "In its approach to decisionmaking,t he machine should present choices, asembling the data on which a human decision could be based" [57]. These decisions should include moral and ethical considerations and the searching of one's conscience. It must always be realized that computer technology is the "product of intelligence, not the creator of intelligence" [58].

In Canham's words: "The conclusion which emerges most sharply from today's estimate of data processing is that men and machines must be partners, but that men must always retain the upper hand. Moreover, it is possible to distinguish between what man can do best and what the machines can do best" [56].

* * * * * * * * * * *

Implications for the Public Administrator

The public administrator should not feel a remoteness to the challenges and threats Canham is alarmed over. He should give serious consideration to the use (or abuse) of information and computer technology that he has access to or control over. For example, he should act responsibly when disclosing information: determine the inquirer's "need to know" and to what extent (the degree of sensitivity). The manager should not feel that his actions will have little or no impact on controlling computer technology. It is the aggregate of all public managers acting responsibly that will determine if society will be the master of computers, or mastered by them.

REFERENCES

[1] Emily d'Aulaire and Ola d'Aulaire [also reference 3].
Ape that "talks" with people.
Reader's Digest 107 (642):98, October 1975

[2] Time Magazine 103(9):74, 4 March 1974
Lessons for Lana

[3] Emily d'Auliare and Ola d'Aulaire [also reference 1].
Ape that "talks" with people.
Reader's Digest 107 (642):98, October 1975

Emily d'Aulaire and Ola d'Aulaire
Put a computer in your pocket
Reader's Digest 107 (641):115-118, September 1975
[4] page 118
[5] page 118

Walter S. Ross
Computers: New dimension in patient care
Reader's Digest 104 (624):118-122, April 1974
[6] page 119
[7] page 119
[8] page 120

[9] Medical Dialogue - With a Computer
Reader's Digest 110 (660):37, April 1977

[10] Lawrence D. Maloney
New York's success against cheaters
U.S. News and World Report 84 (26):31, 3 July 1978

When IRS Computers Dig Into Your Tax Return
U.S. News & World Report 84 (14):49-50, 10 April 1978
[11] page 50
[12] page 50

Donna B. Parker [also references 31, 36-39]
Computer systems protection: testimony before the U.S. Senate Committee
Computers and People 27 (10):7-12, October 1978
[13] page 9
[14] page 9
[15] page 7

Robert S. Strother
Crime by Computer
Reader's Digest 108 (648):143+, April 1976
[16] page 146
[17] page 148
[18] page 147-148

[19] Donald C. Bacon and Orr Kelly [also reference 25-28]
Uncle Sam's computer has got you
U.S. News and World Report 84(14):44-48, 10 April 1978

[20] Donald H. Sanders [also references 21, 33-35]
Computers and Management - In a changing society
McGraw Hill, 1974, page 82

[21] Jerome Lobel
Privacy, security and the data bank
Government Data Systems, November-December 1970, pages 38-46.
As reproduced in Sanders [20] page 84

Rating Your Credit - Another Threat To Privacy
U.S. News and World Report 81(7):62
[22] page 62
[23] page 62
[24] page 62

Donald C. Bacon and Orr Kelly [also reference 19].
Uncle Sam's computer has got you
U.S. News and World Report 84 (14): 44-48, 10 April 1978
[25] page 45
[26] page 45
[27] page 45
[28] page 45

[29] Senate Committee on Government Operations: U.S. Office of Management and Budget; U.S. General Accounting Office
Information on graph

[30] John H. Schenefield
Computers, communications and antitrust: Some current myths and realities
Computers and People 27(6): 11+, June 1978

[31] Donn B. Parker [also references 13-15, 36-39]
Computer systems protection: testimony before the U.S. Senate Committee
Computers and People 27 (10): 7-12, October 1978, page 11

[32] Brandt R. Allen
Computer security
Data Management, January 1972 pages 18-24 and Febraury 1972 pages 25-30, provides a more thorough discussion of physical and other types of security problems

Jerome B. Wiesner [also reference 20-21]
Information revolution And the Bill of Rights as reproduced in Sanders [20], pages 525-532
[33] page 525
[34] page 527
[35] page 527

Donn B. Parker [also reference 13-15, 31]
Computer system protection: Testimony before U.S. Senate Committee
Computers and People 27(10): 7-12, October 1978
[36] page 11-12
[37] page 12
[38] page 11
[39] page 11

John A. Worthley and James J. Heaphey
Computer Technology and Public Administration in State Government - The Need for a New Perspective
The Bureaucrat, Fall 1978, pages 32-37
[40] page 32
[41] page 33
[42] page 34
[43] page 35
[44] page 36
[45] page 37

Stanley Robinson
The National Crime Information Center (NCIC) of the FBI: Do we want it?
Computers and automation, June 1971; as reproduced in J. Mack Adams and Douglas H. Haden, Social Effects of Computer Use and Misuse, Wiley and Sons, 1976, pages 245-251
[46] page 245
[47] page 246
[48] page 247
[49] page 248
[50] page 249
[51] page 250
[52] page 251

Richard E. Anderson
Computerization: Panacea, or part of the problem?
Public Management, October 1971, pages 20-21
[53] page 20
[54] page 21

Erwin D. Canham
Mastered or Master?
The Christian Science Monitor, August 31, 1967.
As produced in J. Mack Adams and Douglas H. Haden, Social Effects of Computer Use and Misuse, pages 273-276
[55] page 273
[56] page 275
[57] page 274
[58] page 276

Stanley Robinson
The National Crime Information Center (NCIC) of the FBI: Do we want it?
Computers and automation, June 1971; as reproduced in J. Mack Adams and Douglas H. Haden, Social Effects of Computer Use and Misuse, Wiley and Sons, 1976, pages 245-251
[46] page 245
[47] page 246
[48] page 247
[49] page 248
[50] page 249
[51] page 250
[52] page 251

Richard E. Anderson
Computerization: Panacea, or part of the problem?
Public Management, October 1971, pages 20-21
[53] page 20
[54] page 21

Erwin D. Canham
Mastered or Master?
The Christian Science Monitor, August 31, 1967.
As produced in J. Mack Adams and Douglas H. Haden, Social Effects of Computer Use and Misuse, pages 273-276
[55] page 273
[56] page 275
[57] page 274
[58] page 276