NCJRS

U.S. DEPARTMENT OF JUSTICE
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
NATIONAL CRIMINAL JUSTICE REFERENCE SERVICE
WASHINGTON, D.C. 20531

Date filmed   12/10/75

PRIVACY AND SECURITY OF COMPUTERIZED
CRIMINAL JUSTICE SYSTEMS

BY

MELVIN F. BOCKELMAN
MANAGER, COMPUTER SYSTEMS DIVISION
KANSAS CITY MISSOURI POLICE DEPARTMENT

Privacy and Security of Computerized
Criminal Justice Systems

Thirty years ago, one of the most fantastic devices ever to be developed by mankind made a rather obscure appearance in this country. Little did the inventors realize, that within the time frame of this century, the computer would assume a major role in processing record keeping systems of our economy and it would also be cited as responsible for effecting profound changes to our society.

We live today, in a time in which 90% of the scientists who have ever lived, are now living; at a time in which knowledge, that prior to this century doubled every 50 years, now doubles every five years; a time in which the dramatic technological advances of the electronic computer has given us the capability to calculate information 500 million times faster than we could prior to World War II. Leading economists have stated that automation is by now so deeply implanted in our economy that we are beyond the point of no return to non-automated systems. We know that we would surely drown in a "sea of unmanageable paper work" and that our economy would quickly evolve into a state of chaos, inefficiency and stagnation without the services of powerful computers. As a result of its powerful calculating capabilities, the electronic computer is today making us aware of many facts and theories that have been hidden from us since the beginning of time. A noted scientist stated that it would require the equivalent manpower of 400 billion people to

perform the information processing requirements if the 80,000 computers in this country would cease to function. It is the computer, more than any other facet of modern day technology, that is providing the capability to solve the complex problems of our environment.

While overwhelming evidence convincingly supports automation, we have been confronted with a great uproar of anti-computerism from some segments of our society. Along with this uproar, some of the young citizens of today show growing signs of a disenchantment towards anything which involves technology, and it is the computer more than anything else, that symbolizes the whole of technology (figure 1). It is a fear, among other things, that reducing the human being to a number means the loss of identity and this is representative of all that is demoralizing and degrading to our society (figure 2).

It has been suggested that people hate computers because they are the first machine in history to really move in on our intellectual and emotional lives (figure 3). The machine is suspected of recording everything in our lives from the womb to the tomb and is thought to replace the activities of numerous individuals (figure 4). Computers are by nature like all other machines, functioning in a state of neutrality. They can therefore be used as effectively against humanity as they can in the service of mankind.
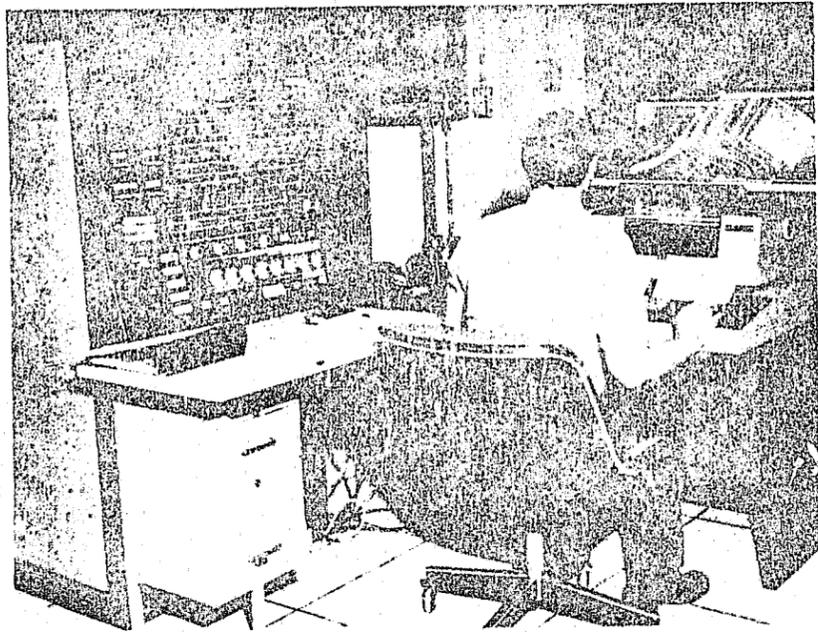
Figure 1 - A machine that can remember more than you and I
could in a thousand lifetimes.

**A GOVERNMENT WATCH ON
200 MILLION AMERICANS?**

Violence by Rebels
Threatens Centers

Winter Could
Be Violent

Centers Increase Security

The Right To Privacy

Contest 'Exposes Misuse'
Best Data Sabotage Plan Wins!

Contest Seeks Methods
For Destruction of Data

Radical Rumblings Heeded

The Computer
An Issue Becomes
A Crusade

Electronic Stool Pigeon

invasion
of privacy

CENTRALIZED
PERSONAL DATA FILE

PERSONAL PRIVACY

Figure 2 - A pamphlet illustrating the concern of the
invasion of privacy by computer systems.
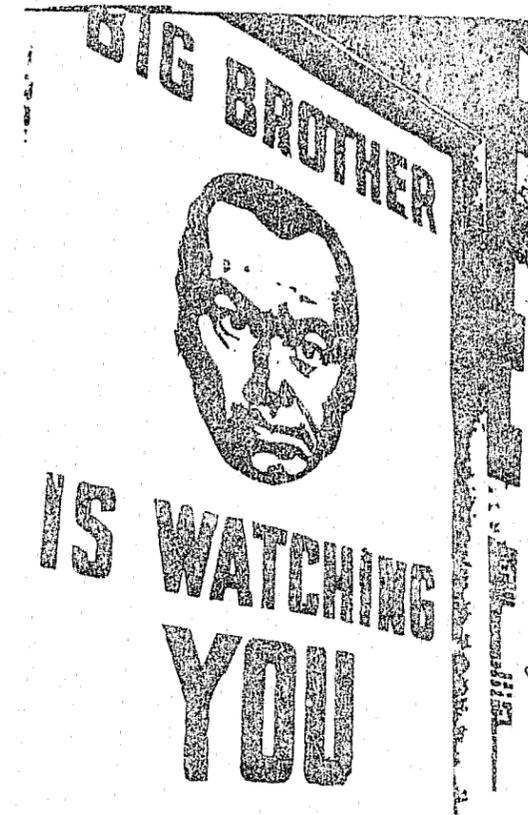
Figure 3 - A pamphlet illustrating the concept of
total knowledge by government on the citizen as a
result of computer tecnology.

Figure 4 - A computer "data bank" capable of storing
400 million characters of information and also capable
of finding the desired information within thousands
of a second.

To some, computers seem to symbolize unresponsiveness and in-sensitivity of modern day life and there is a fear that data banks know a great deal more about us, than we know about data banks. To others, computers symbolize all that is wrong with a slightly tarnished modern day dream and has been suggested in some quarters that Automation may be the very latest form of pollution to inhabit the planet earth.

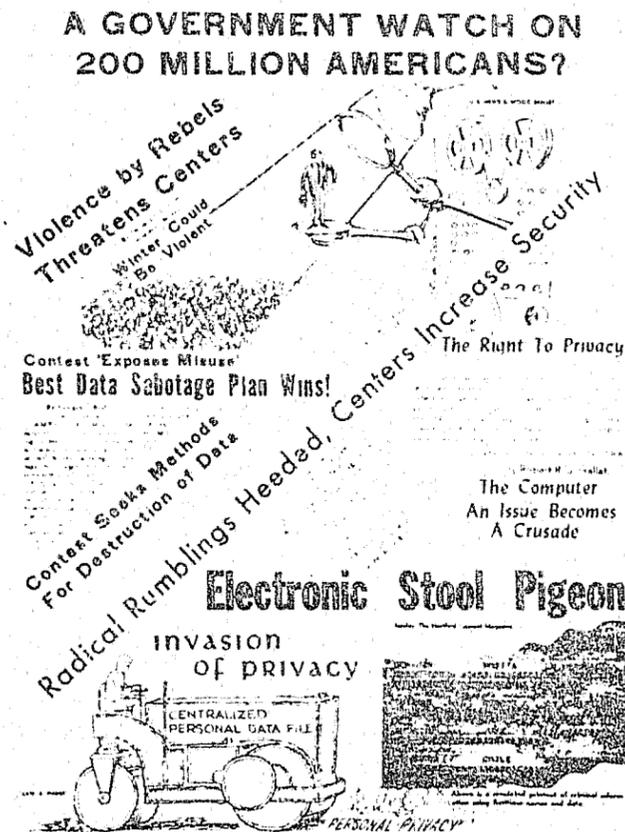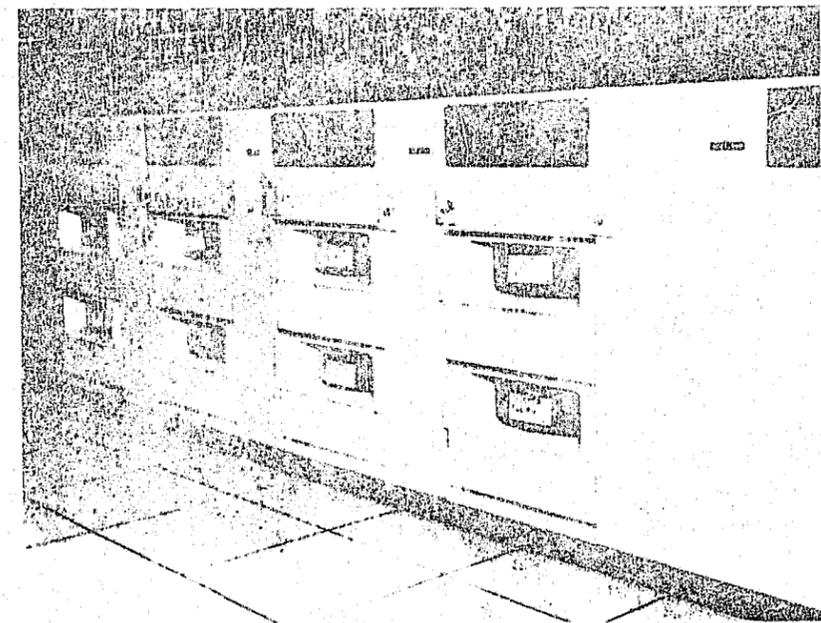Computers are used extensively in the United States in over 1,500 major applications. Manually maintained information systems have been rapidly discarded as government and industry alike have in-vested millions in automating the records of our economy and society.

Today each time a citizen files a tax return, applies for life insurance or a credit card, seeks government benefits, interviews for a job, or becomes a subject of the criminal justice system an automated dossier is opened, and an electronic information profile is sketched on the applicant with the result that we are likely to leave electronic records in the memory bank of a computer; records that can tell a great deal about ones activities, habits, associa-tions and personality characteristics.

Should all these data banks be cross indexed or merged into one, we might well find a surprisingly complete record of personal facts relating to our birth, education, religious affiliation,

health history, family status, moral character, professional compe-tance, financial condition, buying habits, political inclination and criminal records, if any. It is readily apparent that such condi-tions could be personally damaging if the data were made available under unauthorized or unethical circumstances.

It is the electronic computer with its capabilities of speed and superhuman thoroughness, that cannot miss finding either the good or bad about us, that seems to leave the citizen in a state of helplessness. Within thousandths of a second, a computer system can pull together and retrieve all facts in one answer, which portray an individual's glorious successes, hideous failures, his most positive personality traits and his most embarrassing habits. The problem boils down to a simple fact, a machine familiar to all of us here, which can memorize more and better than a human being could in a hundred lifetimes and that is more efficient than the combined efforts of a thousand brains, is thought by some to be a threat to the quality of life and society that we all hold dear. Why? Because the subject of privacy has and still continues, in some instances, to be abused as man fails to understand the need to evaluate and establish ethical controls over the computers' great impact on the life of a citizen.

Personal privacy has been defined as "the right to be left alone," "the right to control the outflow of information about oneself,"

"the most comprehensive of the rights of man,' and 'one of the most basic civil rights of man'. The concept of privacy stems from a person's inner desire to shield and control his actions, thoughts, desires and accomplishments or lack thereof from overexposure to the outside world. It is a most subjective and sensitive area of human personality. Essentially privacy involves a host of things which motivate us to think and act as we do and it conveys the total sum of what we are and what it is that makes us function as a unique personality (figure 5).

I believe that it is absolutely imperative that computers must be made to serve the mainstream of a business concern or government agency. If the computer is fully serving the mainstream of the entire organization, then I believe that management is more likely to exercise greater control over the information process .g system and dissemination of data. Too often, the computer has been regarded by management as a 'necessary evil', 'a status symbol', 'someone else's responsibility', or really 'no ones responsibility' at all. As a result of these deficiencies, the computer receives much undeserved blame these days for things that go wrong, and credit for things that go alright, but the real responsibility for success or failure ultimately belongs to no one else but management.

Within the Criminal Justice environment, automation takes on a special meaning because sometimes it reflects the shortcoming of a citizen.

PRIVACY
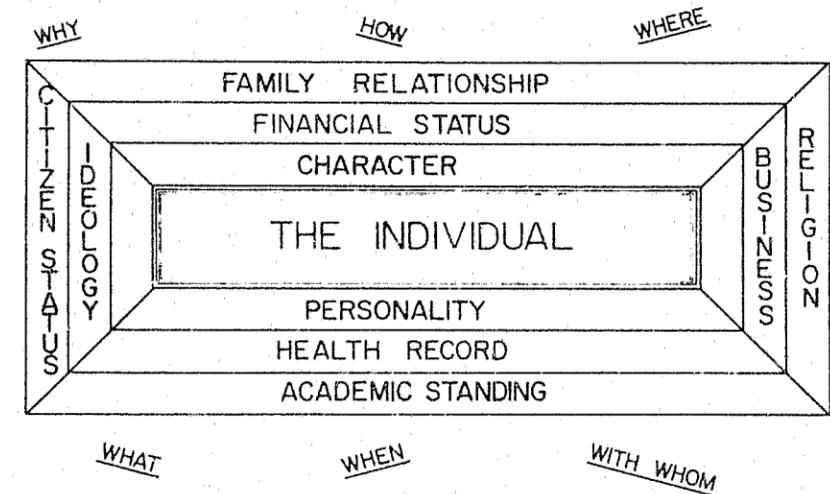
Figure 5 - Concepts of the ingredients which form the things that the human being considers sensative and personal, known to us as 'Privacy'.

CRIMINAL JUSTICE SYSTEM PLANNING MODELS
Assist administrators in defining goals for more efficient Police, Prosecutor, Court and Correction operations.
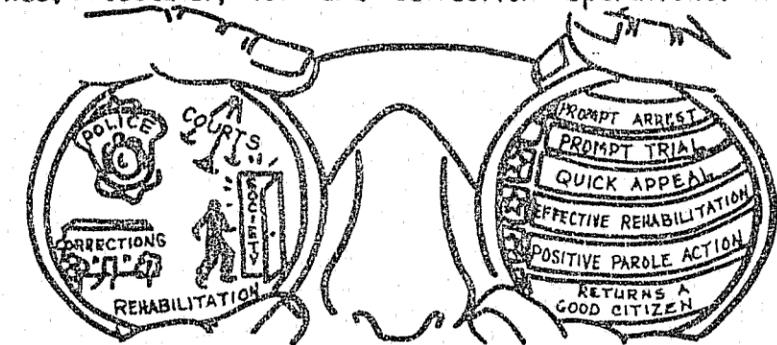
Construction of Criminal Justice Systems Models are technically feasible. Such systems can be computerized in a manner to project the total resources required to significantly reduce crime.

Figure 6 - An illustration of how computers can assist the Criminal Justice System to be responsive to society.

The Criminal Justice System has been slow in casting aside old, outmoded and antiquated ways of operating our American system of justice. Today the picture is changing rapidly as a result of automation and so are the social implications that result from the new technologies. The benefits of an automated criminal justice system are too numerous to mention but perhaps the greatest single benefit would result from an examination of old ways of doing things against our willingness to take an in-depth look at our systems and project them into the future (figure 6).

Members of the Kansas City Regional Criminal Justice System view the collection of information on occurrences where the police become involved, as part of their duty to impartially and accurately record these incidents exactly as they occur (figure 7). Sometimes this is considered by the citizen to be for his benefit, and other times from the citizen's viewpoint, it is not. In any case, ours is a solemn duty and responsibility to protect the public, to assist the victim, to apprehend the violator of the law and to process each case rapidly thru the criminal justice system and to accomplish these tasks with all the efficiencies we can command from present day technologies.

Each time a police officer writes a parking ticket, stops a car on an alleged violation, investigates a case on reasonable grounds of unlawful violations, all subjects, vehicles and in some instances, serialized property are checked thru the computer by communications center personnel for records of outstanding warrants and prior record of criminal history (figure 8). In this day of mobility of the active criminal element, it is of great importance to the officer in the street to be made aware of potentially dangerous criminals that he may be in the process of coming into contact with. Our on-line system is flagged with 1,000 subjects known to be armed, dangerous or resist arrest, subjects with histories of multi-offenses against laws of our society.

Today the system is used extensively by the Criminal Justice family within 10,000 square miles of Western Missouri and Eastern Kansas. Records show that our Criminal Justice Data Bank Alert II is being accessed either for entry of data or for inquiry of information an average of 35 times every minute of the 24 hour day and our computer is exchanging information automatically with the FBI's NCIC Computer 3,000 times each day concerning the nation's criminal element (figure 9).

Police information is exchanged frequently over radio systems, however, as a result of advanced computer technology, the contents are quite frequently that of a sensitive nature. Mobile terminals are beginning to be used in police operations and this advancement in modern day technology will greatly enhance the cause for privacy and security of criminal justice data (figure 10). Our data base is extensive and we record on-line 26 major categories of information which total over one million on-line records (figure 11).

Figure 7 - On-Line information entry of Police records Computer Systems Division Kansas City Missouri Police Department.

Figure 8 -
Kansas City Missouri Police Communications Center using computer terminals to relay criminal information to Police officers.

Figure 9 - Alert II Symbol denoting involvement of the computer with all elements of Criminal Justice.

Figure 10 - A mobile terminal with a visual display installed in the police car.

Conviction in the courts is by law a matter public record, however, we still affort those records general security. The use and release of arrest information is controlled by Police Department General Order 71 - 18 which says in part, "Members of the department shall not disclose arrest information to anyone outside of the Criminal Justice jurisdiction or agency".

We have implemented many other extensive security precautions to protect the release and flow of information. Both manual and software controls have been implemented and are constantly being strengthened as we recognize new and better ways to protect all aspects of data security. These range from administering extensive personality tests to computer applicants in an effort to weed out those with troubled personalities, to installation of bullet proof security walls in the computer complex.

Procedural Instruction 73-3 recognizes the right of each element of criminal justice to exercise management control over data stored in the Regional Criminal Justice Computer (figure 12). This document prohibits the processing of reports without the approval of the Criminal Justice Agency responsible for the data being processed. The following policy statements outline major steps taken by our department to protect the security and confidentiality of computerized information systems (figure 13):

(1) Data included in the system must be limited to that based upon

Figure 11 - An illustration of the various parameters by which computer data can be accessed by Alert II System.

Figure 12 - K.C. Police Department Procedural Instruction 73-3 which prescribes policy and procedures related to automated information systems.

a source document maintained on file in the agency which exercises

management control over the system and identified with unique case

numbers assigned to the report.

(2) Adoption of a careful and permanent program of data verifi-

cation against source documents; I believe we must be committed

to the spending of approximately 5% of our total automation budget

in support of validation of automated information files. We

accomplish this task in three steps.

(a) Printout of automated files for validation against

source documents which were the original authority for

the data entry in the first place.

(b) Creation of computer programs which can identify

incorrect codes and data, earmarking these for correction

against the source document of entry.

(c) Creation of computer programs which can edit against

relationship conditions and requirements. This is a very

valuable "caution indicator" and has in many instances

alerted our department to a whole series of inconsistencies.

(3) Education programs are administered for all who access data from

remote terminals.

(4) The computer is programmed to screen all inquiries to exclude

those inquiries inconsistent to system rules (figure 14).

(5) Our telecommunications system activity is logged for all actions

occurring on the network and this permanent record of activity may be
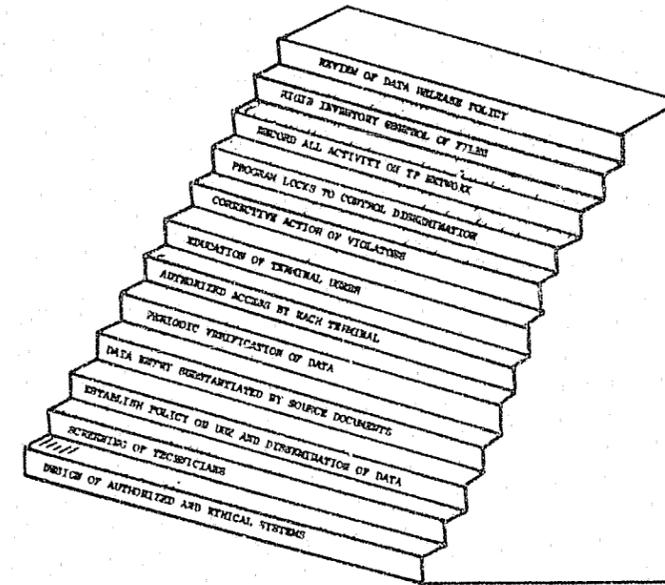
examined at any time (figure 15).

Figure 13 - Illustration of steps taken in the Alert II
System to maintain ethical control over computer based
systems.

NJ.TEST.ZXAMPLE.JUDY.R.W.F.061357

NOT AUTHORIZED JUVENILE DATA AT THIS TERMINAL

Figure 14 - A computer terminal printout showing that inquiries
are rejected when access to unauthorized files is required.

(6) Program systems are designed to provide for 'Locked Data Files'

in which records cannot be accessed until the proper codes or terminal

identity is read and matched to the master terminal access list that

is core resident.

(7) Rigid security and inventory controls are in effect in computer

library operations to prevent duplicating files and removal of

same to unathorized sources (figure 16).

(8) Discarded criminal record printouts are all subjected to a

shredding machine to insure the contents cannot be reconstructed

for later use (figure 17).

(9) Remote terminal operations are under programmed control to

rigidly control access to only those real time files that the user

has prior clearance to access (figure 18).

(10) Users of system data have been informed that careless use of

system data represents unprofessional conduct and may be subject

to disciplinary or litigation action.

(11) An Operating Procedure has been published which clearly indenti-

fies to whom data may be released, under what circumstances, and it

requires the removal of names and addresses before any reports are

released to non-criminal justice agencies (figure 19).

(12) Access to the bullet proof computer complex is rigidly con-

trolled by electronic locks (figure 20).

(13) The computer has been programmed to identify each printout

with a reminder of security contained information (figure 21).

Figure 15 - A printout of computer log showing events
occuring on the telecommunications network system.

Figure 16 - Computer library showing millions of historial
records (abstract and detail).

Figure 17 - Computer printouts of Criminal records no longer needed are subjected to a "Shredder Machine" with the results as indicated .

Figure 18 - A page out of program documentation showing types of information accessable by each terminal.

SCOPE

This computerized telecommunications network was designed for Regional Kansas City area agencies involved in the criminal justice process. It represents a step forward in the common cause of increasing the effectiveness of the criminal justice process.

This network is dedicated to the operation and goals of local, state and national criminal justice systems. All participating agencies must subscribe to the general policies and guidelines announced by the Policy Committee of the National Crime Information Center. That policy and security agreement is furnished under separate cover to each administrator who is a participant in this network system.

RESPONSIBILITIES

The technical requirements outlined in the ALERT Computer Teleprocessing Manual, the NCIC Operating Manual, and the Remote Terminal Manual of Instructions are established to insure the greatest efficiency of the network operations. Participating agencies must insure all facets of these technical requirements are completed.

The following policy is established and is mandatory for all agencies participating in this network.

1. For law enforcement agencies, the terminal ideally should be located in or adjacent to the Dispatcher Center and, further, should be manned on a 24 hour basis by personnel under control of the law enforcement agency.

Figure 19 - Operating procedure of the Alert II Network which binds all agencies of criminal justice to abide by established rules for maintaining ethical control of the system.

Figure 20 - An employee accessing the bullet proof door to the Computer Systems Division with an electronic card.

In recognization of the citizens right to review his files the Police Department operates a policy of purging arrest records when a citizen applies for the expunging of arrest records and when the facts substantiate his request.

Security and confidentiality agreements have been executed within the Criminal Justice System to insure management control over the use and release of information generated within the system.

There are a great variety of means and ways to enhance the physical security of a criminal justice computer complex. The most important is restricting access to the computer center by non-authorized personnel who must be identified and be under escort while in the Computer Systems Division (figure 22).

Thru software control, on-line remote terminals are deactivated from the computer center for non-24 hour agencies to insure access is denied to anyone who might attempt to use the terminal while the working staff is off-duty (figure 23).

Smoke detection devices, emergency lights and a fire alarm are installed and these devices provide control capabilities important to the overall security of the complex.

I believe that computerized information systems properly designed and operating in an environment where management is exercising proper controls, can provide much greater security than ever possible under manually maintained record systems.

```
N.TEST.ZXAMPLE.BENJAMIN.D.W.M.010240


N.TEST.ZXAMPLE.BENJAMIN.D.W.M.010240

****** FOR OFFICIAL USE ONLY WITHIN THE CRIMINAL JUSTICE SYSTEM ******    KCPA
ZXAMPLE              BENJAMIN    D J WM 010240 KS 511 200 BR BR          MOKPD0000
                     DANGEROUS        RESIST ARREST     ***SUBJECT IS 10-31***
                                                        10-31 CRN = 99999999
MOKPD0000 SID*
MOKPD0000 107               S 170         ST KANS CITY MO         031572
MOKPD0000   OC012145 CP S ASSAULT AGGRAV  102672
     ***HOLD SUBJECT ON PICKUP ORDER ISSUED BY KCMOPD CRIMES AGAINST PERSONS UNIT
MOKPD0000 00114460 RFL 060556 JACKSON CTY JAIL (FORGERY)
MOKPD0000 00999922 MENTALLY RETARDED
MOKPD0000 JKT* ZXAMPLE    TV-005 TC-004 OV-012 OC-009 MA-013 MC-008
FA-016 FC-002
LOCAL INTELLIGENCE SUBJECT-PREPARE FIC
REGISTERED FELON-PREPARE FIC
NATIONAL INTELL SUBJECT-PREPARE FIC
ASSAULT AGAINST POLICE OFFICER
10-32 J-4 ASSAULT SUBJECT-PREPARE FIC
10-32 J-6 SHOPLIFTING SUBJECT-PREPARE FIC
10-32 J-6 LARCENY SUBJECT-PREPARE FIC
10-32 J-5 BURGLARY SUBJECT-PREPARE FIC
10-32 J-3 ROBBERY SUBJECT-PREPARE FIC
10-32 J-1 MURDER SUBJECT-PREPARE FIC
10-32 J-7 AUTO THEFT SUBJECT-PREPARE FIC


MOLESTATION SUBJECT-PREPARE FIC
10-32 J-2 RAPE SUBJECT-PREPARE FIC
10-32 J-8 KNOWN TO POSSESS NARCOTICS-PREPARE FIC
10-32 J-8 KNOWN TO SELL NARCOTICS-PREPARE FIC
KNOWN ACTIVIST-PREPARE FIC
MILITANT(LOCAL) - PREPARE FIC
MENTAL SUBJECT
ALERT/0000004                    100%
ALIAS ZXAMPLE           POB         MOKPD0000
****** FOR OFFICIAL USE ONLY WITHIN THE CRIMINAL JUSTICE SYSTEM ******   KCPA
```

Figure 21 - A statement entered on the top and bottom of a computer printout reminding the user to safeguard the information.
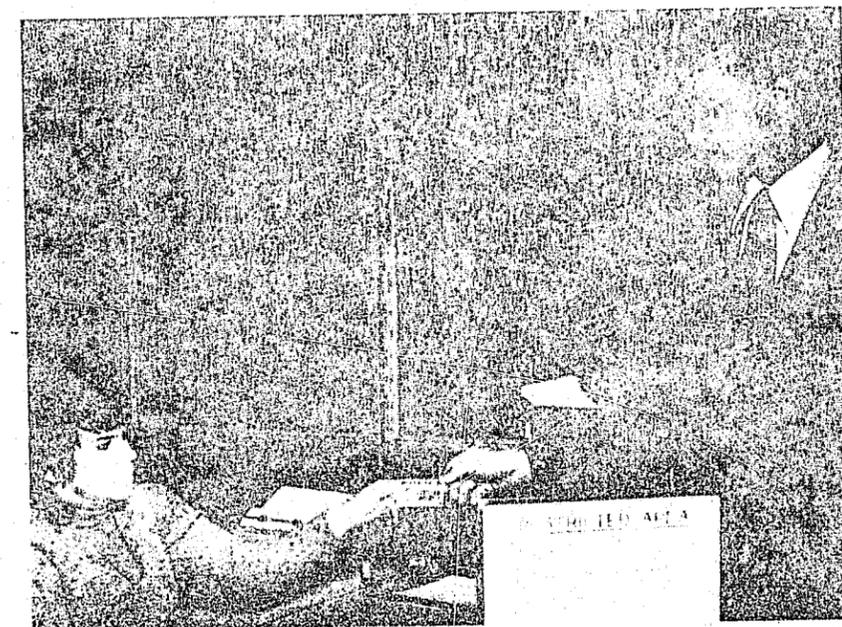

Figure 22 - A visitor presenting identification before allowed access to the Computer Division.

One of the major problems in the past was the rapid buildup of computer installations in which the computer technician was not motivated to feel he was a part of the organization. The result was a lack of loyalty in which the qualities of trust and reliance were in many cases absent. This unfortunate condition must be overcome as security and confidentiality issues demands that the qualities of loyalty must be ever present.

The subject of privacy although greatly influenced by machines is nevertheless completely dominated by humanity vs. humanity. It is a state of condition totally subject to man's control, as it is misused by man's weakness yet protected by mankind's desire for dignity of his fellow man.

This document portrays concepts, ideas and policies at one computer installation related to the subject of privacy and security. These policies and ideas are by no means the ultimate answer as we continue to develope new ways to insure that the vast information repositories are used in a positive manner; to erradicate poverty, to promote medical technology and to get at the root of what really fosters crime and to enhance the freedom and well-being of all mankind.

In the final analysis, these considerations all boil down to a balancing of values; the need for informed managers of government and industry and the need of the citizen to expect ethical control

by government and industry in the use of data about himself and his private life (figure 24).

Once we all have a thorough understanding of these problems and have developed systems which insure the ethical processing and use of information, we shall begin to implement new and more productive ways of using the computer. As our society and economy becomes more complex so will the need for vast data banks to support the complicated operations of our modern day society and economy.

On the horizon we see new, meaningful and creative roles in which the powerful processing capabilities of computers will begin to be used in assisting mankind in decision making capability (figure 25). Where computers are used today in record keeping and communication functions they will be used tomorrow in forecasting, predicting, analyzing and projecting problems and their solutions.

In reality, a computer is nothing more than an extension of the intelligence and creative ability of man. It is one of mankinds newest and most versitile tools. I strongly support the vigorous use of these machines as a positive resource for the nation and the improvement of the quality of our lives.

A noted philosopher once said, "Computers are incredibly fast, accurate, but stupid. Man is unbelievable slow, inaccurate, but brilliant." I submit that these combinations of attributes will provide the ingredients that will continue to move mankind to attain the goal of operating ethical systems that are acceptable to our society.

TCAM V KNAR,OFFTP,B	BUREAU OF NARCOTICS & DANGEROUS DRUGS
TCAM V KLEC,OFFTP,B	KANSAS CITY, MISSOURI PROSECUTOR
TCAM V KSPR,OFFTP,B	MISSOURI STATE PROBATION/PAROLE
TCAM V KFPI,OFFTP,B	FEDERAL BUREAU OF INVESTIGATION
TCAM V KRPP,OFFTP,B	ROELAND PARK,KANSAS POLICE DEPARTMENT
TCAM V KCPB,OFFTP,B	PAYROLL UNIT, KCMOPD
TCAM V KJP1,OFFTP,B	JACKSON COUNTY PROSECUTOR'S OFFICE
TCAM V KJP2,OFFTP,B	JACKSON COUNTY PROSECUTOR'S OFFICE
TCAM V KJP3,OFFTP,B	JACKSON COUNTY PROSECUTOR'S OFFICE
TCAM V KJP4,OFFTP,B	CIRCUIT COURT, 16TH DISTRICT
TCAM V KJP5,OFFTP,B	JACKSON COUNTY WIFE/CHILD SUPPORT

Figure 23 - A printout on the control terminal in the computer center showing the duty operator which remote terminals have been deactivated from the computer.
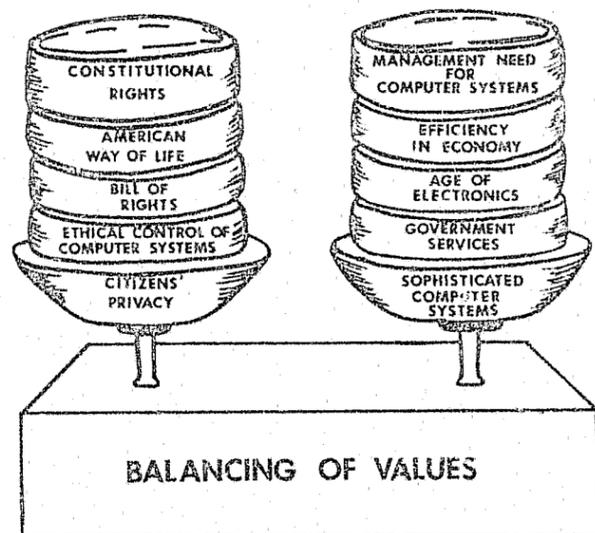

Figure 24 - An illustration portraying the balancing of values: The need to computerized information vs the right of the citizen to personal privacy.
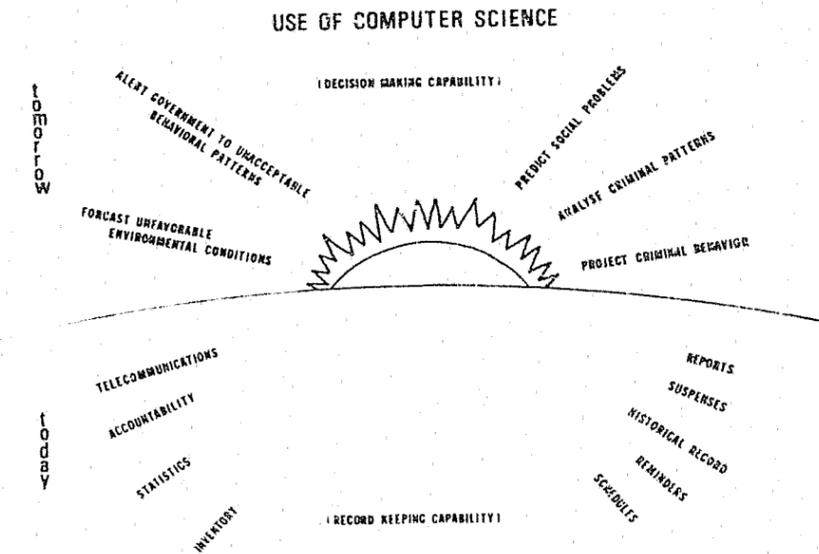
USE OF COMPUTER SCIENCE

Figure 25 - An illustration denoting further use of the Computer in the Criminal Justice System.