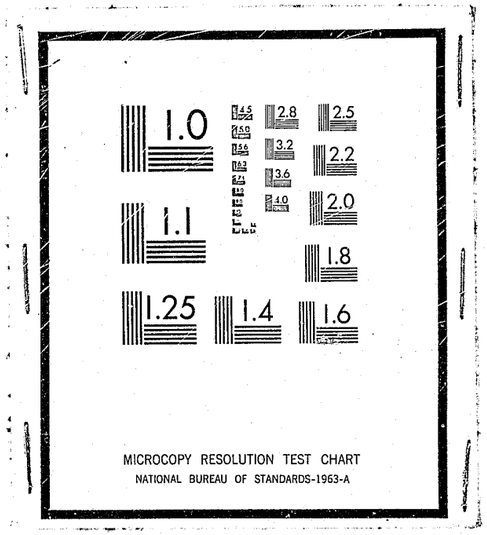

SAC PAPER 75-02

7

ISSUES IN PRIVACY: — 7 GENERAL IMPACT OF INFORMATION SYSTEMS

April 1975

Prepared By

Sarah L. Dalton
Research Assistant

and

Ronald J. Nolfi
Chief
Statistical Analysis Center (SAC)

Office of Criminal Justice Plans and Analysis
1329 'E' Street, N.W.
Washington, D.C. 20004

This paper is presented as the first in a three part series dealing with the concept of privacy, information systems, and criminal justice. It reviews the general issues of privacy presented by the use of automated systems and examines the principal works spawned by the "computer-privacy" dilemna. Proposed safeguards and established regulations which have evolved on these issues is also examined.

The present paper serves as a background and introduction into the general areas of privacy, security, and confidentiality. The impact of these issues in the area of criminal justice is the subject of a separate analysis and will follow as the remaining parts of this series.

Introduction

> In all societies men...have lived in the interstices of their institutions. They have counted on the mercy of error, ignorance and forgetfulness in their dealings with their fellows and the state. They have often been wrong in so doing - morally and/or factually. But in a world of computers this mercy may not long exist. All our failings and achievements, our credit-worth and our petty delinquencies, our obedience and our defiance, can live in the constant present of the machine [1].

Record-keeping is one of man's oldest preoccupations dating back to the hieroglyphics of cave man. With each technological innovation: from the ancient hieroglyphics, the clay tablet, the printing press, the typewriter, the teletype, the photocopier, to the modern computer (this list is intended to be illustrative and is by no means complete), society has become increasingly more reliant on record-keeping. Thus, at a Senate committee hearing in 1974 Professor Arthur Miller attests to the ever increasing trend of record-keeping which pervades American society:

> Americans today are scutinized, measured, watched, counted, and interrogated by more government agencies, law enforcement officials, social scientists and poll-takers than at any other time in our history. Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States [2].

Today many experts believe that we are on the threshold of a so-called "information processing revolution" [3;4] This revolution has been primarily attributed to two interrelated factors: (1) Modern computers permit the organizations to gather, store, and rapidly access enormous amounts of information. (2) Nationwide

information systems, employing the telephone and other telecommunications, greatly increase the number of individuals and agencies who have access to this data. Yet the present "information processing revolution" while greatly facilitated by the present computer telecommunications technology is none the less the result of significant re-enforcing trends which have been at work in American society for considerably longer periods of time than the enabling technology. First, there has been a generalized increase in data collecting and recording as our industrialized society grows more complex, as the public sector expands, as public and private bureaucratic organizations multiply, and as science becomes more empirically oriented. Second, the mobility of individuals and the anonymity of modern life has led to huge private and public investigative systems whose primary functions are to gather data on millions of Americans in order that decision-makers may make "informed" decisions on who to hire or fire, to lend money or extend credit, to insure or to give a passport or visa. A third trend has been the development and expansion of specific government programs where each require more personal data on eligible individuals, i.e., social security, welfare, scholastic financial aid programs, etc. The fourth and last trend which has contributed to the "information processing revolution" is that as our ability to collect and analyze data becomes more efficient, one finds more uses for such information and inevitably seeks to

gather more diverse data on ones' clients, employees, or members. Thus, our predilection towards data collection and analysis begets more data and uses for such data ad infinitum.

In view of these four basic trends, it is not surprising that America is considered to be the "greatest data gathering society in human history [3]." Moreover, these trends have been dramatically facilitated in the last two and one-half decades by enabling technology. As Westin and Baker explain:

> The past 25 years have witnessed the development of steadily more powerful and versatile computer and communication systems, with larger storage capabilities, faster access to stored data, and devices which make data input and output cheaper and available in more varied formats. There has also been dramatic reductions in the cost of performing computations [5].

In general, this revolution offers immense benefits to society for more efficient and equitable resource allocation and social control and assists, in particular, various public and private agencies and agents to make more fact-related, logical, and knowledgeable decisions than ever before possible.

The Problem

In recent years there has been a growing public awareness and apprehension over various data gathering activities and applications in respect to their adverse affects on the data subjects' privacy. This concern has focused on the governments' and private organizations' insatiable appetite for the collection of

personal data and its dissemination and the computer-communication technology which facilitates these transactions. Since their inception, data gathering activities and applications of the public and private sectors have proceeded relatively unhampered by formal safeguards or regulations to protect informational privacy. In the mid-1960's public opinion was gradually aroused by the rapid growth of these records systems and their implications on privacy, security, and confidentiality of personal information.

Until recently the privacy of the individual data subject was relatively easy to protect or at least not unduly threatened for a number of reasons: large amounts of information about individuals were not generally available; the information was generally decentralized; available information was relatively superficial; access to information was difficult to secure; individuals in our mobile society were difficult to keep track of; and most people were not able to interpret much from the data available [6]. However, our present computer-communication technology no longer offers these superficial yet comforting privacy protections. Instead it permits: infinitely more information to be available; it is available exceedingly more quickly; it is transmitted with vastly greater speed; and it is able to be stored for substantially longer periods of time. Thus, computerization permits users to greatly expand their data processing capacity. Moreover, it greatly facilitates data

access within an organization and permits sharing of data across organizational lines. With the present information processing technology it is now possible to set up powerful nationwide data banks which could momentarily amass thick personal dossiers from data contributed by various organizations on vast numbers of data subjects. (For a detailed description on how this can be done see reference [7]).

The Response

The computer-privacy issue spawned in the mid-1960s has generated a large number of public and private studies, a plethora of legalistic, technical, and popular literature, and a growing number of guidelines and regulations to deal with the issues of privacy, security, and confidentiality of personal information raised by automated record-keeping systems. Both the public and private sectors have attempted to deal with these issues by defining anew the central concepts, by in depth studies of such systems, and by recommending various guidelines and safeguards to protect the individual data subject. In addition, Congress has taken an active role in sponsoring many bills to safeguard individual privacy in record-keeping systems, however, only a small number have actually been enacted into law. The purpose of this paper is threefold: (1) to examine the reformulated concepts of privacy, security, and confidentiality; (2) to re-

view the most noteworthy and representative contributions from the private sector; and (3) to discuss contributions of the public sector. Privacy issues related to criminal justice systems are excluded from this review and are the subject of another paper.

A. Definition of the Issues

The vast increase in record-keeping systems generated by the increasing sophistication of computer technology has led to an intensive reassessment of the concepts of privacy, security, and confidentiality. Neither the common meaning of these terms or past legal definitions sufficiently embrace modern society's computer practices in the handling of personal information. First in terms of privacy or the right of privacy, it is generally agreed that the dictionary's definitions of "secrecy" or "seclusion" are not appropriate to most record-keeping systems. This is due to the fact that much of the data in the information systems are public facts and available for anyone to see or use. For example, much census data, police and court data, tax records are of this type and a matter of public record, i.e., a record required to be kept by law.

No comprehensive or consistent legal definition can be found in common law or in the Constitution of the United States. Prosser, in attempting to define the concept of privacy in com-

mon law found that three elements were necessary for the violation of the right of privacy: disclosure to more than a few persons; the facts disclosed were not public facts, and the facts disclosed had to be offensive [8]. These common law principles have generally been applied to situations involving reputational or financial harm of one private individual by another. Thus, such a definition encompasses no consistent nor conceptually unified approach to balancing the interests of society or public and private organizations against the interests of the individual. Nor does it address the basic issues of personal privacy in relation to automated record-keeping systems.

The elusive right of privacy has not been articulated by the Constitution of the United States. The Supreme Court, however, has recognized various aspects of the right to privacy on Constitutional grounds; basing its decisions at different times on the various Amendments incorporated in the Bill of Rights, namely, on the First, Fourth, Fifth, Eighth, Nineth, and Fourteenth Amendments. In a recent and much cited case involving privacy, Griswold vs. Connecticut (381 U.S. 479), the Court described the right of privacy as emanating from the penumbra guarantees found in the Bill of Rights. These guarantees - the First Amendment's right of association; the Third's a prohibition against quartering soldiers in one's home, the Fourth's, the right to be protected from unreasonable search and seizure;

the Fifth's, protection against self-incrimination; and the Nineth's, guarantee that the rights enumerated shall not be construed to deny or disparage others retained by the people - create "zones of privacy". In this case the Court held that the "zones of privacy" included marriage; it also clearly specified that there were other such zones which were yet to be defined. Therefore, although the Court has recognized the right of privacy, one finds no clear articulation of this right in the Constitution nor case law. More specifically, the Courts have never dealt squarely with the issue of privacy and automated records.

In the absence of a consistent and comprehensive definition of personal privacy or the right of privacy, various individuals and groups have attempted to define this concept in relation to automated record-keeping systems. Some of the more noteworthy attempts are as follows:

> The right of privacy is the right of the individual to decide for himself how much he will share with others, his thoughts, his feelings, and the facts of his personal life [9].
>
> The right of individual privacy...(is) the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public [3].

> As a first approximation, privacy seems to be unrelated to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves [10].

> Privacy is or should be the inherent and legal right of individuals, groups or institutions to determine for themselves when, how and what information about them is communicated to others (Robert P. Henderson, Vice President of Honeywell Corporation, addressing a Congressional hearing[11]).

> Privacy has to do with collecting the information in the first place; with the individual's right to control information about himself [12].

All these definitions suggest that the core of the right of privacy is that disclosure of personal information is up to the individual data subject, and it is the individual's perogative to decide the extent and manner of disclosure. It is also inferred that there may be mandatory disclosure of personal information under extraordinary unspecified circumstances which may be understood to mean, if authorized by a constitutional or legislative mandate. However, if disclosure is mandated, the personal data subject still retains control over how this information is disseminated.

The above definitions consider the data subject as having more or less exclusive control over disclosure and dissemination of personal data. None of these seem to address the fact that there

may be legitimate record-keeping functions in which personal information must be gathered and disseminated for the good of society at large and the individual data subject. For example, the IRS requires personal data on income, wealth, and personal expenditures from individuals in order that they may be assessed their equitable part in supporting various government services. School systems, welfare departments, credit bureaus, banks, and criminal justice agencies all maintain necessary personal record-keeping systems which benefit the general good and/or the individual data subject. The every-day impact of these systems is known to all citizens, and, indeed, it is questionable whether modern society as we know it could continue to function without their existence. This is not, of course, to condone the existence of all such systems, nor the fact that some practices are harmful and lead to abuses of privacy.

Hence, the above formulations on privacy need to be reformulated to reflect the idea that both the individual data subject and/or society, on the one hand, and the record-keeping organization, on the other, have a mutual interest in maintaining personal records. The concept of mutuality suggests, as one approach, a "proper balance" to the right of privacy in respect to personal record-keeping systems. The Secretary's Advisory Committee on Automated Personal Data Systems has pointed out:

> It would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record. To the extent that people want or need to have dealings with the record-keeping organizations, they must expect to share rather than monopolize control over the content and use of the records made about them [13].

The concept of mutuality recognizes that it is not in the interest of society or the individual to permit the record-keeping organization to have exclusive control over decisions about content and use of personal records. Yet the Secretary's Advisory Committee also affirms that to be the case:

> It is our observation that organizations maintaining records about people commonly behave as if they had been given such a unilateral role to play. This is not to suggest that decisions are always made to the disadvantage of the record subject; the contrary is often the case [13].

The pendulum in the past has swung towards the organization. The present social climate suggests that a more equitable balance may be struck between the individual or society and the record-keeping organization. Whatever the outcome, it is clear that the traditional notions of privacy require considerable reshaping to keep pace with modern day practices.

In examining the privacy-automated personal records issue, it has also been necessary to define security and confidentiality. Privacy, security, and confidentiality have often been used interchangeably and, thus, incorrectly. Security has been defined as:

> Security means insuring that information will not be destroyed, modified or disseminated improperly [12].
>
> ...A descriptive term that connotes the degree to and means by which information and the machines and facilities for processing, storing and transmitting it are protected from loss and unauthorized access or modification [14].

Confidentiality has been denoted as:

> Confidentiality has to do with...the explicit or implicit agreement between the individual providing the information and the organization gathering it - that that information will be used specifically for the purposes for which it was collected. It has also come to mean restricting information from people who do not have a right and need to know it [12].
>
> ...A loose concept which minimally connotes some commitment to withhold from unauthorized users information obtained from or about an individual or institution [14].

Privacy, security, and confidentiality are all key concepts in automated personal data systems; all must be dealt with as separate and distinct elements in protecting informational privacy. Having defined these key terms in relation to automated personal data systems, it also seems worthwhile to define what is meant by an automated personal data system. An automated personal data system is:

> A collection of records containing personal data that can be associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files [13].

The Secretary's Advisory Committee has distinguished two fundamental types of automated personal data systems: administrative systems and statistical-reporting or research systems [13]. The difference between the two is of a functional nature. An administrative personal data system maintains records on persons in order to make direct decisions about these individuals - to make judgments concerning their character, qualifications, rights, benefits, etc. Administrative personal data records may be subdivided into two categories: (1) Administrative records which includes public facts whose collection is mandated by law and facts which are obtained in the process of a transaction - obtaining a marriage license, credit, passport, etc. The personal data contained in these records is usually self-reported or obtained by open inspection of the individual's affairs; (2) Intelligence records which are of many forms - security clearance files, law enforcement investigative reports, and personal credit reports. Intelligence records may contain administrative record data, but in most instances much of the data is gathered from informants and investigators without the data subject's knowledge or confirmation. Thus, such "facts" are unconfirmed and untested.

The other fundamental type of automated personal data system is the statistical-reporting or research system. This system maintains statistical records about persons for use in statis-

tical reports or research, and these records are not intended to affect the data subject directly. A statistical record may be generated from administrative records or created expressly for statistical reporting or research purposes, i.e., a population census or sample survey. In most cases, the personal identity of the subject is eventually severed from the record.

The privacy and security issues of automated personal data systems are different depending on the type of system. Most public and private attention has been focused on administrative systems because of the characteristics of such records, containing personal identifiers and whose purpose it is to directly affect the data subject. Statistical-reporting and research systems have received considerably less attention in relation to privacy and security. This is due to the fact that statistical records usually lack personal identifiers and have an innocuous affect on the individual data subject. However, privacy and security concerns arise when administrative records are utilized for research and statistical purposes or vice versa, and personal identification can be made on the basis of these records.

B. The Private Sector

Many segments of the private sector have demonstrated support for enhancing the privacy, security, and confidentiality aspects

of automated personal information systems. It is not within the scope of this paper to examine the multitude of works stimulated by these issues. Hence, only a very small number of the most important and representative works have been singled out for discussion.

One of the most thorough and respected studies was done by the National Academy of Sciences and sponsored by a grant from the Russell Sage Foundation. The final report, DataBanks in a Free Society which was co-authored by Westin and Baker, summarizes a three year in depth survey of 55 private and public computerized data banks and their effects on informational privacy. Some of the study's more important findings include:

> 1. (C)omputer usage has not created the revolutionary new powers of data surveillance predicted by some...
>
> 2. (C)omputerization is definitely bringing some important increases in the efficiency of organizational record-keeping. The most important of these are: the production of more complete and up-to-date records; faster responses to inquiries; more extensive use of information already in the files; more extensive networks for interorganizational exchange of data; and the creation of some large data bases that would not have been feasible without computers.
>
> 3. (O)rganizational policies which affect individual rights are still generally following the precomputer patterns in each field of record-keeping [5].

The report demonstrates that organizational efficiency has been greatly enhanced by conversion from manual to automated

personal data systems. However, in view of the dramatic increase of informational sharing within organizations, the expanding data bases, and the increasing utilization of data without new policies to deal with these new developments, the dangers to personal privacy are increasingly apparent. Thus, Westin and Baker recommend legal restraints to insure personal privacy is protected. They also recommend the establishment of a "Citizen's Guide to the Files," the development of effective technical safeguards, the imposition of new limits on all personal information, and the establishment of new restrictions on the use of social security numbers.

The computer industry has also taken initiative upon itself to sponsor a large number of studies and reports on privacy and security. Most of these works have focused on the security problems involved in automated personal data systems. In 1972 International Business Machine Corporation (IBM) announced support of an initial series of studies on the problems of data security in automated processing. The outcome of these studies in which specific aspects of data security were examined at four study sites - the Massachusetts Institute of Technology, the State of Illinois, TRW Systems, Inc., and the IBM Federal Systems Center - is a six-volume report. This report represents a comprehensive examination of the technical aspects of the problems of data

security in an automated data processing system. The Rand Corporation has also taken an active role in behalf of computer security [16;17].

Many books, both popular and scholarly, have been written by concerned citizens on the rights of privacy in the technological age. Some of the more popular exposes which have roused public opinion by examining the drift toward depersonalization and the increasing erosion of personal privacy and freedom are: The Organization Man [18]; The Naked Society [19]; and The Privacy Invaders [20].

Two comprehensive and scholarly texts which are much quoted in relation to the "computer-privacy" issue are Alan F. Westin's Privacy and Freedom [3] and Arthur Miller's The Assault on Privacy [7]. Westin examines the impact and implications of surveillance technologies for personal privacy. In addition, he reviews in detail from a legalistic perspective what is the right of privacy and makes recommendations on how it may be preserved. Miller, also, explores various aspects of informational technology in relation to individual privacy and evaluates (as inadequate) the present responses of the legal system and government and private organizations to the new methods of handling personal data. Both Miller's and Westin's seminal works graphically illustrate the inherent dangers of automated data systems for the individual's privacy.

C. The Public Sector

The public sector has also demonstrated concern with the privacy issue and the growth of automated personal data systems. The Executive branch has sponsored a number of studies, commissions, and conferences. In 1973 the Secretary's Advisory Committee on Personal Data Systems of the Department of Health, Education, and Welfare issued a widely acclaimed report on Records, Computers, and the Rights of Citizens [13]. The Advisory Committee examined the inherent dangers to personal privacy posed by computerized record-keeping and the use of the social security number as an all-purpose data bank identifier. The report has had widespread and significant impact on the need to protect personal privacy. The report recommended the enactment of a Federal "Code of Fair Information Practices" in which five principles are to be recognized as minimal safeguards for automated personal data systems. These principles are:

1. There must be no personal data record-keeping system whose very existence is secret.

2. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for an individual to correct a record of identifiable information about him.

> 5. An organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data [13].

The report stresses that these are the minimum standards to be adopted; and violation of this code would represent "unfair informational practice" subject to criminal sanctions and civil remedies. The HEW group also recommends that excessive and widespread use of the Social Security Number should be halted until further study determines the effects of such use and more stringent safeguards for personal privacy have been found.

In February of 1974, President Nixon established the Domestic Council Committee on the Right of Privacy under the Chairmanship of Vice President Ford to study individual privacy and the collection of personal data. This Cabinet level Committee is still active today. The focus of the Committee has been on the Federal level, and it is responsible for recommending effective measures to protect individual privacy in this area. Some of the major privacy problem areas the Committee has identified and is studying are: Federal computer and communication systems, computer system and network security, notice of rights and individual access to Federal records, consumer transactions, cable television systems, Federal mailing lists,

IRS taxpayers data, electronic funds transfer, Federal employees' rights, and criminal justice information systems. The Domestic Council is also attempting to encourage and support state and local government initiative to develop safeguards for informational privacy [21;22]. An effort in this direction was the Committee's co-sponsorship with the Council of State Governments of a "Seminar on Privacy" in December 1974 in which key representatives of the states convened in Washington, D.C. to discuss these major issues.

The National Bureau of Standards (NBS) has sponsored a number of workshops and conferences on privacy and security problems involved in automated personal record systems. NBS has focused primarily on the development of new tools and techniques that will provide security in computer systems. Two of their recent publications which deal with this area are "Approaches to Privacy and Security in Computer Systems" and "Government Looks at Privacy and Security in Computer Systems" [23;24].

Bipartisan Congressional efforts on behalf of informational privacy have led to a large number of studies and hearings, a substantial collection of bills, and a handful of statutes. Beginning in the mid-1960's with the examination of a controversial proposal for a National Data Bank, various House and Senate Subcommittees have conducted numerous studies and hear-

ings on informational technology, computers, and the privacy rights of individuals in order to identify and remedy problem areas. In view of time and space limitations, only a small number of these legislative endeavors have been singled out for discussion.

In 1966, as the debate over the National Data Center galvanized Congressional concern over the impact and implications of such a center, the Senate Judiciary Committee on Administrative Practices and Procedures undertook a survey of "Government Dossiers" to determine "the amount, nature, and use of information which government agencies currently maintain on individuals [25]. The survey revealed that Federal files contained more than 3 billion records on individual citizens and almost one-half of these files were computerized. The study concluded that a majority of government forms contained irrelevant information about individuals and that, in a large minority of cases, confidentiality and security provisions are non-existent or not meaningful [25]. In 1968, a report, "Privacy and the National Data Bank Concept," was issued by the House Committee on Government Operations which summed up Congressional response to the proposal [26]. The Committee stated, on the basis of the testimony before it, that a National Data Center poses serious problems in respect to the collection, use, and security of personal information. Thus, the Committee strongly urged that a National Data Center

not be established until the technical feasibility of safeguarding automated records was fully explored and privacy could be assured. This concept has not as yet been revived as a viable legislative proposal.

The Senate Subcommittee on Constitutional Rights under the Chairmanship of Senator Ervin has taken a most active role on behalf of individual privacy. In 1971, the Subcommittee initiated hearings and an extensive survey of 858 Federal data banks housed in the Executive branch in order to determine how these information systems affect the privacy and other constitutional rights of the individual data subject [11]. The result was a six volume report "Federal Data Banks, Computers and the Bill of Rights" which revealed "not only a disturbing absence of laws to control the new information capabilities of government, but an equally disturbing absence of knowledge of what data banks the government had, what they contained, and what they were used for [27]." The actual study spanned four years and is considered to be a monumental accomplishment in regard to documenting the nature and scope of the data maintained by Federal agencies. The outcome of the hearings and survey revealed a large number of unusual and suspect data bank and surveillance activities were being conducted by various Federal Executive agencies. For example: the report documented

such programs as HEW's blacklist of scientific personnel, the Secret Service's computer file on individuals who had expressed anti-government or anti-American sentiment, and the FBI's and Army's automated civil disturbance and intelligence files on citizens and organizations who have voiced similar sentiments.

In 1974, this Committee and its complement in the House conducted hearings on criminal justice data banks [28;29]. These hearings were inspired in large part by the potential for accessing criminal justice information through an extensive and already established computer network of the FBI's National Crime Information Center (NCIC). These hearings will be dealt with more fully in another paper dealing with criminal justice information systems.

Some other hearings in the past few years which have dealt with informational privacy are: hearings on insurance industries before the Judiciary Antitrust Subcommittee; hearings on privacy abuses by the credit reporting and banking industries before the Senate Banking, Housing and Urban Affairs Committee; and hearings before the Select Committee on Watergate which delineated widespread improper and/or illegal collection of personal information and the improper access and disclosure of personal files by Federal government agencies and agents.

These numerous Congressional hearings and studies have resulted in a large number of bills; however, only a few of these have actually come to fruition and been enacted into law. The 93rd Congress has been known as the "Privacy Congress" because of its sponsorship of over 200 bills dealing with privacy. Some of the areas addressed by these bills have been army surveillance, government record-keeping, criminal justice information, census data, financial records, mailing lists, social security numbers, and a privacy bill of rights for individuals. Despite legislative efforts only a handful of statutes offer any protection of privacy for individuals.

One of the first legislative statutes to deal directly with informational privacy was the Fair Credit Reporting Act of 1970. This Act regulates the vast consumer-reporting industry and the primary objective of the Act, as stated therein, is:

> to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy (15 U.S.C. 1681-1684t).

Most notably, the Act gives the consumer access to his credit records and allows for procedures to correct inaccurate and absolute information in his records.

In 1970, Congress also passed the Freedom of Information Act which has recently been amended (November, 1974). The Act re-

quires public disclosure of information held by Federal agencies upon request; however, several categories of Federal records are exempted from mandatory disclosure, including much of the personal information contained in personnel files which constitute a "clearly unwarranted invasion of personal privacy (5 U.S.C. 552)." The statute gives the particular agency discretion as to what constitutes an invasion of privacy regarding such exemptions. Thus, the individual data subject has no control over whether or not his or her information is to be released, nor is the said individual provided with any recourse with respect to disclosure or non-disclosure of exempted personal information. The recent Amendments, in essence, place more of the burden on the Federal agencies to release information contained in their files rather than on the public to seek out this information. Procedures are laid down to provide civil remedy and criminal sanctions for violations of the Act by government employees. In addition, Federal agencies are now required to periodically publish an index of the information in their files. Thus, the Act's intent is to facilitate public access to information within the Federal agencies rather than an attempt to balance the conflicting interest of the public's right to know with the individual's right to privacy. It is conceivable that this Act may actually be used to abuse rather than enhance the individual's right of privacy.

The most significant and recent legislative action dealing with the individual's right of privacy in record-keeping systems is the Privacy Act of 1974 signed into law on January 3, 1975 by President Ford. The law represented a compromise between the tougher, more extensive Senate bill (S.3418) and the House bill (H.R. 16373). With few exceptions, this general privacy statute applies to non-criminal justice information contained in Federal depositories. The new law restricts the kind of data the Federal agencies may disclose to outsiders and provides the individual access to assure that the information retained is accurate. It also requires that agencies publish reports periodically on types of files it maintains. This law basically incorporates the Federal "Fair Information Practice Code" developed by the Secretary's Advisory Committee on Automated Personal Data Systems of HEW and establishes a Privacy Protection Commission to study the implications of this Act.

Thus, while only a few Federal statutes are now on the books to regulate automated data systems and safeguard individual privacy, the new 94th Congress has already demonstrated its interest in this area and is likely to extend these safeguards further to include other areas. A comprehensive privacy bill, appropriately entitled H.R.1984, has been recently introduced in the House by Representatives Koch and Goldwater to extend

to the private sector and state and local governments the privacy safeguards now guaranteed to personal information in Federal repositories. In addition, both the House and Senate have reintroduced bills which cover the collection and dissemination of criminal justice in order to insure security, privacy, and confidentiality of such information.

Conclusion

In summary, automated personal record-keeping systems offer great benefits to society in terms of efficiency and economy. However, these systems also pose serious potential threats to the individual data subjects in terms of invasion of personal privacy. Concern has been voiced by both the private and public sector, and slowly formal guidelines and safeguards are being evolved to deal with the problems of privacy, confidentiality, and security involved in these technologically advanced informational processing systems. However, there are many areas which are not covered by any formal consistent or comprehensive mandates to insure personal privacy. One of these as yet neglected areas is that of criminal justice information in which the data subject who comes in contact with any part of the criminal justice system is, except in a few spotty instances, offered no guarantees for privacy nor any recourse for action if his privacy is indeed abused. This subject will be discussed in great detail in another paper which follows in the series of papers developed on the issue of privacy.

References

1. MacRae, Donald G. "Introduction" to Spencer's The Man Versus the State, Baltimore: Penquin Books, 1969.

2. U.S. Congress, Senate, Committee on Government Operations. "Protecting Individual Privacy in Federal Gathering, Use and Disclosure: Report to Accompany S.3418," Washington: U.S. Government Printing Office, 1974.

3. Westin, Alan F. Privacy and Freedom, New York: Atheneum Press, 1967.

4. Rosenfeld, Arnold R. "Privacy vs. Enforcement and Rehabilitation: A Practical Approach" Proceedings of the Second International Symposium on Criminal Justice Information and Statistics Systems, Sacramento, Cal.: Search Group Inc., 1974, pp. 517-523.

5. Westin, Alan F. and Baker, Michael A. Data Banks in a Free Society: Computers, Record-Keeping and Privacy, New York: Quadrangle Books, 1972.

6. Miller, Arthur R. "The Dossier Society "University of Illinois Law Forum 1971:2, 1971, pp. 154-167.

7. Miller, Arthur R. The Assault on Privacy: Computers, Data Banks, and Dossiers, Ann Arbor: The University of Michigan Press, 1971.

8. Prosser, William H. "Privacy" California Law Review 48:3, 1960, pp. 383-423.

9. Office of Science and Technology of the Executive Office of the President. Privacy and Behavioral Research. Washington: U.S. Government Printing Office, 1967.

10. Fried, Charles. "Privacy" The Yale Law Journal 77:3, 1968, pp. 475-493.

11. U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Constitutional Rights. "Federal Data Banks, Computers and the Bill of Rights: Hearings, 92d Congress, 2d Session (Part 1 and 2), Washington: U.S. Government Printing Office, 1971.

12. Orr, Kenneth T. "Privacy, Confidentiality and Security and the Management of Local Criminal Justice Information Systems" Proceedings of the Second International Symposium on Criminal Justice Information and Statistics Systems, Sacramento, Cal.: Search Group Inc., 1974, pp. 507-516.

13. Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare. Records, Computers and the Rights of Citizens, Washington: U.S. Government Printing Office, 1973.

14. Domestic Council Committee on the Right of Privacy and Council of State Governments. "Glossary of Some Frequently Encountered Terms" Seminar on Privacy, Washington, Dec. 15-17, 1974, pp. 1-5.

15. International Business Machines Corporation. Data Security and Data Processing: Study of Specific Aspects of Data Security (6 volumes), White Plains, N.Y.: IBM Corporation, 1974.

16. Ware, Willis H. "Data Banks, Privacy and Society: Report No. 5131," Santa Monica, Cal.: the Rand Corporation, 1973.

17. Turn, Rein. "Privacy and Security in Personal Information Data Bank Systems," Santa Monica, Cal.: the Rand Corporation, 1974.

18. Whyte, William H., Jr. The Organization Man, New York: Simon and Schuster, Inc., 1965.

19. Packard, Vance. The Naked Society, New York: David McKay, 1964.

20. Brenton, Myron. The Privacy Invaders, New York: Coward-McKay, 1964.

21. Metz, Douglas W. and Trubow, George B. "The Complexity of Privacy" Trial 11:1, 1975, pp. 13,24.

22. Metz, Douglas W. "The Domestic Council Committee on the Right of Privacy" Bulletin of the American Society for Information Science 1:3, 1974, pp. 17-18.

23. Renninger, Clark R. (ed.). "Approaches to Privacy and Security in Computer Systems," Washington: National Bureau of Standards, U.S. Department of Commerce, 1974.

24. Renninger, Clark R. and Branstad, Dennis K. (eds.). "Government Looks at Privacy and Security in Computer Systems,". Washington: National Bureau of Standards, U.S. Department of Commerce, 1974.

25. U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Administrative Practices and Procedures. "Government Dossiers," Washington: U.S. Government Printing Office, 1967.

26. U.S. Congress, House, Committee on Government Operations. "Privacy and the National Data Bank Concept," Washington: U.S. Government Printing Office, 1968.

27. U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Constitutional Rights. "Federal Data Banks and Constitutional Rights: A Study of Data Systems on Individuals Maintained by Agencies of the United States Government," (Part III of the Subcommittee's Study of "Federal Data Banks, Computers and the Bill of Rights"), Washington: U.S. Government Printing Office, 1974.

28. U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Constitutional Rights. "Criminal Justice Data Banks - 1974: Hearings, 93d Congress, 2d Session on S.2542, S.2810 and S.2963," (Volume 1 and 2), Washington: U.S. Government Printing Office, 1974.

29. U.S. Congress, House, Committee on the Judiciary, Subcommittee on Civil Rights and Constitutional Rights. "Dissemination of Criminal Justice Information: Hearings, 93d Congress, 1st and 2d Session on H.R. 188, H.R. 9783, H.R. 12574, and H.R. 12575," (To be published).

END

7 [illegible]