2-3-6-63 810138

HARRY HUGHES
GOVERNOR

STATE OF MARYLAND
EXECUTIVE DEPARTMENT

ANNAPOLIS, MARYLAND 21404
Governor's Information Practices Commission
State House - Room H-4
(301) 269-2810

GOVERNOR'S INFORMATION PRACTICES COMMISSION

INTERIM REPORT
January 1981

MEMBERS

Arthur S. Drea, Jr., Chairman
John A. Clinton
John E. Donahue
Albert J. Gardner, Jr.
Wayne Heckrotte
The Hon. Timothy R. Hickman
Florence B. Isbell
The Hon. Nancy Kopp
E. Roy Shawn
Dennis M. Sweeney
Harriet Trader
Donald Tynes, Sr.
Robin J. Zee

STAFF

Dennis M. Hanratty, Executive Director
Thea Cunningham, Research Analyst

CONTENTS

I. INTRODUCTION

We exist today in an information society. The last three decades represented a veritable revolution in the acquisition and processing of information. Today, companies throughout the world rather routinely engage in transactions in a manner that would have been impossible before the 1950s. Individual citizens have benefited from this information expansion in incalculable ways.

In the midst of this revolution, however, a great many people have reservations about the information miracle. Increasingly, citizens are demanding that limitations be placed on the collection and uses of information by public and private organizations. There are frequent requests to limit the types of information that can be collected from individuals by organizations, to mandate organizations to collect information from the individual himself, and so forth. In a word, demands are made on government today to protect personal privacy.[1]

Privacy protection legislation has become important to so many citizens today because, as we have already noted, the character of our society has changed so much from the past. As the United States Privacy Protection Study Commission has recently observed, one hundred years ago our interactions with public and private organizations in society were not as commonplace as they are today.[2] Many people were self-employed, attained only lower-level education, and there was little contact with large agencies and the Federal Government. Records maintained on individuals were also minimal. The formal transactions conducted between one individual and other members of society were limited in scope. Face-to-face information exchanges provided the opportunity to divulge specific information and allowed for the correction of errors or misperceptions on the part of

others. In addition, information gathered was not extensive. Now, however, when transactions in almost every sphere of life require the divulgence of detailed personal information, the scenario has changed. Few individuals are able to obtain credit, insurance, and other necessities of modern living without the final determination being based on personal information.

Over the last decade, the concern of the American public about the potential abuse of personal information has also gradually increased. In the past, many employers collected extensive information on applicants and employees, including data relevant to hiring practices. Unfortunately, informal opinions, comments of supervisors and other non-related information were also often included in files. This possibly inaccurate or outdated information was potentially damaging to an employee when maintained in files without his knowledge. In addition to not knowing what information was collected, the individual could not be sure to what uses it was being put. Many began to question just how much information really was required by organizations.

The use of computers as a base for record systems has also contributed to fears of the American public. Survey research often reveals that the public harbors deep suspicions about the eventual consequence of a fully computerized society. In point of fact, there are numerous advantages that accrue to a society relying on computerized, or automated, systems. The cost-effectiveness of computers permits the extension of services to a greater number of individuals than was ever before possible. These services are provided, in addition, with a higher degree of efficiency and accuracy. Finally, automation has strengthened, in many cases, the confidentiality of an individual's personal record. It is a more difficult process to make an unauthorized entry into a computer system than would be the case with a single manual file.

At the same time, however, the increased usage and concurrent growth in record-keeping abilities of organizations have potential negative ramifications. One of the major problems is that the expansion of our information-gathering ability has far outstripped the ability of individuals to determine what type of personal information is released and for what purposes. While we have taken great strides in increasing the amount and speed of information collection, storage, and retrieval, society has been somewhat slower in making provisions to allow the individual to monitor the development, use, disclosure, and correction of the information maintained on him. Compared to the face-to-face relationships of the past, the individual is often left defenseless to protect himself against possible errors and the indiscriminant dissemination of information.

In addition, while it may be more difficult to tap a computerized rather than manual system, the potential for harm remains much greater. The amount of information that could be available to a skilled individual capable of by-passing security procedures of a large organization is enormous. Time after time, computer systems that were hailed as impermeable to outside forces have been shown to be vulnerable. Among problems that have plagued automated systems have been weak supervision over physical access to computers, inadequate storage of programs and documentation, vulnerabilities in magnetic tape controls and poor designing of the manual handling of input/output data. Such problems either facilitate access to computer facilities on the part of non-employees or enable those who have authorized access to make unauthorized uses of the information contained in that system.[3] Devising new ways to ensure security of automated records containing personal information while continuing to provide efficient and accurate services to citizens are major challenges in the 1980s.

It is evident from what has been said up to this point, then, that increasingly the public is demanding some measure of control over the nature of personal information given to organizations. This concern is apparent particularly in terms of information at the disposal of governmental units. Yet while it is important to observe this rising level of interest in the protection of personal records, we should not view this demand in isolation but instead should recognize that it is linked to another, equally important, issue: the right of citizens to gain access to the public records of government.

From its origins, one of the most distinctive features of the American polity was the dictum that the governed must be permitted to scrutinize the actions of those who exercise power in its name. The First Amendment to the Constitution establishing the principle of freedom of the press should be seen as a commitment on the part of the Founding Fathers to the view that the public needed to be informed of the operations of government. This attitude was expressed well by one of the chief framers of the Constitution, James Madison: "A popular Government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; And the people who mean to be their own Governors, must arm themselves with the power, which knowledge gives."[4]

Yet while the foundations of our government rested on the premise of citizen access to public information, frequently the reality of the situation was very different. Regrettably this was often the case in recent times, when abuses of power went undetected as roadblocks were placed in the way of citizens monitoring government action. Contemporary restrictions on public access were all the more unfortunate due to the dramatic growth of the size of government. Three interrelated processes were at work. First of all, bureaucracies impacted on more and

more areas of an individual's life. Second, the traditional distinction between legislatures as policy-making bodies and bureaucracies as policy-implementing bodies was being obscured. Third, bureaucracies were largely unaccountable to constituents or to the electoral process. The cumulative effect of these changes was to heighten the need for public awareness of government behavior; the irony, of course, was the governmental response to place more restrictions on the flow of information.

It should come as little surprise to anyone that a consequence of this situation was a noticeable decline in confidence and trust of the public towards government officials. It is incumbent upon government, however, to take the steps necessary to reverse this trend. Nothing less than the continued health of our democratic system is at stake. It is axiomatic that a free society cannot survive if its government operates in secrecy. In order for the American people to exercise the rights and responsibilities pertaining to them under the Constitution, there must occur an open and accurate flow of information between government and the public.

Two critical issues, therefore, confront both federal and state government and demand resolution. First of all, governments must design appropriate measures to guarantee the privacy of personal records. Second, governments must permit citizens to have access to public records. It is in response to these concerns that Governor Harry Hughes created the Information Practices Commission. Its mandate is to examine the personal record-keeping practices of state agencies with an eye towards achieving an appropriate balance of the individual's right to privacy, the information requirements of public organizations, and the public's right to be informed. In this Interim Report, the Commission details what it has discovered up to this point in time and the future course of its study.

II. THE CURRENT STATUS OF PRIVACY POLICY IN MARYLAND

An earlier section of this report raised some of the major concerns regarding privacy protection. However, it would be erroneous to suggest that there does not exist currently any protection of personal records held by agencies of Maryland government. In point of fact, there are several provisions of the Maryland Annotated Code which seek either to ensure confidentiality of such records or to enable an individual to have access to files containing personal facts of his life. Particularly significant statutes in this regard are those which establish the Criminal Justice Information System and delineate explicit privacy procedures for criminal records,[5] classify juvenile court records as confidential and separate from those of adult offenders,[6] and restrict the type of information collected from applicants for State employment.[7] In addition to specific statutes pertinent to privacy concerns, numerous state agencies have issued regulations requiring confidentiality of personal records. For example, the Department of Health and Mental Hygiene restricts access to records of the Maternal and Child and Crippled Children's Programs.[8] Finally, Maryland is subject to numerous federal regulations mandating privacy protection as a precondition to participation in various categorical grant programs. For example, the Office of Family Assistance of the United States Department of Health and Human Services requires states to safeguard public assistance records in those programs involving federal financial participation.[9]

The Information Practices Commission applauds those efforts that have already been taken by the State of Maryland to protect personal records. The Commission believes, however, that though the actions of the state in this area have been noteworthy, much more work needs to be accomplished. More specifically, the Commission asserts that the magnitude of the issue demands consideration of the

enactment of comprehensive privacy legislation. Despite numerous references to privacy in the Annotated Code, the Commission intends to determine whether the absence of a comprehensive statute places considerable restraints on the protection of personal records.

Several examples will demonstrate the uneven and non-uniform character of legislation in this regard, particularly in the area of an individual's right to access to records involving personal facts of his life. Under Maryland law, this "person in interest" is permitted to have access to his personnel files, if he is a state employee, and to examine his educational records.[10] However, no similar explicit access provisions are accorded to the "person in interest" if he is a patient in a Maryland state hospital or a client of a social service agency. This situation has led to considerable confusion regarding the legitimate rights of the "person in interest". For example, the Consumer Council of Maryland recently conducted a survey of eighteen public and private hospitals in the Baltimore metropolitan area and an additional sampling of county hospitals. The Consumer Council asked the following question: "Do patients in your hospital have access to their medical records?" The results demonstrated a clear absence of uniform procedures in this area. Some hospitals indicated that a patient would never be granted access to such records. Others suggested that medical records would be released if the request came from an attorney. Still other hospitals maintained that the request would only be honored if disclosure was authorized by the attending physician. Finally, at least one hospital stated that patients are given access to their records. It is obvious that the findings of the Consumer Council demand further investigation of this issue.[11]

A second area where one finds a lack of uniform procedures involves the inter-agency disclosure of personal information. For example, the state statute governing inter-agency transfer of public assistance records is noticeably stricter than are statutes pertaining to tax information. The Department of Human Resources is prohibited from disclosing public assistance records without either a court order or ". . . for purposes directly connected with the administration of public assistance, medical assistance, or social services programs . . ."[12] In the case of tax records, however, significant amounts of tax information can be disclosed ". . . to an officer of the state having a right thereto in his official capacity . . ."[13] The language used in statutes protecting the confidentiality of tax records (and many other categories of personal records as well) raises important questions. Should an agency be prevented from redisclosing personal information to another agency for purposes not directly related to the original collection of the information? Should the "person in interest" be notified that information is being disclosed to another agency? Should the "person in interest" be permitted to have an opportunity to contest the accuracy of such records before they are released to another agency? What restrictions should be placed on the redisclosure of personal records by third parties? The Information Practices Commission intends to conduct a thorough examination of these, and other, questions associated with the inter-agency disclosure of personal records.

Further evidence of a general lack of uniformity of existing privacy legislation can be seen in the fact that many categories of personal records are considered to be confidential while others are not. Both voter registration records and motor vehicle records tend, as a general rule, to fall within the non-confidential area. For example, under existing law, voter registration lists can be released to the public as long as the recipient agrees not to use

the information for commercial solicitation or other business purposes. The only other possible situation that could prevent public access to voter registration lists would be for the Board of Supervisors of Elections to issue a special order.[14] Similarly, the general premise regarding motor vehicle records is that they are open to public inspection. Access is permitted to driver records, vehicle ownership information and insurance information as long as the Motor Vehicle Administration approves of the purported intended use of the information; a separate medical file, however, is considered to be confidential. The Information Practices Commission will examine the appropriateness of allowing public access to records which contain personal facts of an individual's life.

One final problem remains to be discussed: difficulties associated with the security of personal information in the possession of state government. In point of fact, this is not a problem of ambiguous statutes on this subject in the Annotated Code, but rather a case of inadequate implementation by agencies. Numerous examples abound in this area, of which perhaps the most publicized have been a series of incidents regarding lack of protection of taxpayers' records. In 1977, a security committee of the Data Processing Division, responsible for many tax records, disclosed numerous problems including access to computer operations by unauthorized persons, the unauthorized uses of computer facilities by individuals with authorized access privileges, and inadequate building security.[16] The following year, tax records were found in trash bins outside the Treasury Building on two separate occasions in violation of state law.[17] At approximately the same time, documents containing refund information were provided to a reporter by a state employee.[18] The Commission provides these examples to suggest the obvious need for a thorough examination of security of personal records throughout state agencies.

III. THE CURRENT STATUS OF ACCESS TO PUBLIC INFORMATION IN MARYLAND

Just as in the case of protection of personal records, the State of Maryland has taken significant steps to permit individual citizens to have access to the public records of government. The hallmark of this effort is the Public Information Act, first enacted in 1970 and amended periodically since then.[19] The Act applies to nearly every public agency in the state. It establishes procedures whereby citizens can write to designated custodians of public documents in each agency requesting copies of specified records. This right to access to public information is available to any individual; one does not need to justify the reason why one should be provided with such information. Unless the record requested falls within a specified restricted category, such as records pertaining to criminal investigative proceedings, the information must be provided by the custodian to the individual making the request. If the request is denied, an appeals process is set into motion that could conceivably end up overturning the original refusal by the custodian to grant access.

Though the Public Information Act expands in notable ways the rights of Maryland citizens, there are, nonetheless, a number of questions that have been raised. One of the most serious problems is the fact that the Act does not require the custodian to respond to the requesting individual within a specified time period. Once the custodian actually denies a request, he must provide the individual with a written statement within ten working days specifying the reasons for the denial and the remedies available to the individual. However, prior to making an official denial, the custodian does not operate under a time restriction. The obvious consequence of this situation is that agencies essentially can deny public access to government records without having to make a formal declaration of denial. The Commission desires to receive comments from

any citizens who may have experienced difficulties with this provision of the Public Information Act.

In addition, many people have expressed other questions about the Act. Are there categories of records to which the public cannot gain access under current law which should be open for public inspection? Are the personal records provisions of the Act adequate? Should an agency, by regulation, be allowed to make records confidential and thus prevent their disclosure? Should search and other related costs in finding and reviewing documents be charged to the requesting party? Do custodians in various agencies implement the mandates of the Act in similar ways? The Commission intends to review carefully each of the concerns that have been mentioned here.

IV. ISSUES REGARDING PRIVACY

It is clear from what has been said previously that privacy of personal records is an issue demanding immediate attention. Many experts and state officials have suggested a variety of guidelines for use in management of records. In attempting to accomplish the task before it, the Information Practices Commission intends to examine these proposed general principles regarding privacy in order to determine the extent to which they are appropriate to the management of various types of state records.

1. An agency should be required to collect only such information from an individual which is necessary, timely and relevant to the performance of the duties of that agency.

2. An agency should make every effort to collect personal information from an individual himself.

3. An agency to the greatest extent possible should inform an individual of the type of information that is collected about him.

4. An agency that requests information of a personal nature from an individual should notify the individual of the specific statute authorizing the request, the principal uses of such information, and the consequences of failing to comply with the request.

5. An individual should have the right, to the greatest extent possible, to determine which records are collected, maintained, and disseminated by an agency.

6. An agency should maintain only such information about individuals as is necessary to perform its tasks.

7. An agency maintaining records involving personal facts of an individual's life should publish on an annual basis the name and location of such records, the categories of individuals contained in the record system, the categories of records maintained in the system, the uses of such records, policies and procedures regarding storage, retrievability, access controls, retention, disposal, accuracy and security of such records, the title and address of the individual responsible for each record, agency procedures whereby an individual can be notified on request if the system of records contains a record pertaining to that individual, and the categories of sources of records in the system.

8. An individual should be permitted to have access to information pertaining to him which is contained in an agency record.

9. An individual should be permitted to copy information pertaining to him which is contained in an agency record.

10. An individual should be permitted to challenge the accuracy of information pertaining to him which is contained in an agency record.

11. An agency should make every effort to verify the accuracy and relevance of information concerning an individual before disclosing such information to another person or agency.

12. An agency should make every effort to inform an individual of the nature of the information to be disclosed and to whom the information may be disclosed.

13. An agency to the greatest extent possible should permit an individual to prevent information that was obtained for one purpose from being used or made available for other purposes.

14. An agency maintaining records involving personal facts of an individual's life should maintain an accurate record of any disclosure of such information, including, but not necessarily limited to, the date, the name and address of the person or agency receiving the information, the statutory authority permitting the disclosure of the information, and the purported use of the information by the recipient.

15. An agency disclosing records involving personal facts of an individual's life shall permit the individual to have access to its dissemination logs.

16. An agency which has disclosed records involving personal facts of an individual's life to another agency or person should notify that agency or person in the event either of a challenge to the accuracy of the record or a correction to its contents.

17. An agency releasing information for the purposes of scientific research, statistical reporting, financial auditing or program evaluation must ensure the confidentiality of the identity of individuals.

18. An agency maintaining records involving personal facts of an individual's life should enact and implement appropriate safeguards to ensure the integrity, security and confidentiality of such records.

19. An agency maintaining records involving personal facts of an individual's life should enact safeguards to prevent misuse of such information.

20. In order to determine the appropriate level of security for each category of personal records, agencies should authorize a security risk analysis to be performed.

21. An agency official who discloses records involving personal facts of an individual's life in disregard of existing statutes shall be held accountable for such actions.

22. An agency which is authorized in accordance with state law and regulation to destroy records involving personal facts of an individual's life should ensure that records are destroyed in a secure and thorough manner.

V. THE PLAN OF THE INFORMATION PRACTICES COMMISSION

Increasingly, many groups in society are supporting the above mentioned principles and are asserting that they should be a part of any comprehensive privacy legislation. The Information Practices Commission recognizes, however, that there may be serious questions regarding either the feasibility or propriety of adopting several of the principles. As a consequence, the Commission intends to take a very open approach before recommending any additional legislation.

First of all, the Information Practices Commission is desirous of soliciting opinions and advice from agency officials. The Commission can envisage situations where a principle might work very well for the great majority of agencies but poorly for a few. For example, to compel criminal justice officials to inform an individual that he is currently under surveillance would obviously defeat the purpose of the investigation. The Commission will, therefore, examine reasonable and necessary exceptions to any privacy legislation recommendations, should such recommendations be made.

It is anticipated that agencies will present their concerns to the Information Practices Commission in at least two ways. First, a representative of the Commission will schedule appointments with officials of the major state agencies.

These on-site visits by the Commission's representative will enhance the Commission's understanding of the record-keeping practices of various agencies and its awareness of any special agency needs. Second, hearings will be scheduled during the Spring for agency officials. At these hearings, officials would have an opportunity to present testimony before the full body of the Information Practices Commission. In addition to these two principal methods, the Commission welcomes communication from agency officials at any time.

The Commission is also particularly interested in soliciting testimony at its public hearings from state and local government employees. Maintaining the integrity of public employees' personnel records should be a paramount concern of agency officials. The Commission is anxious to receive testimony either from any employees who may have experienced difficulties in this regard or from their representatives.

Additionally, the Commission intends to hold hearings in order to receive testimony from interested members of the public. The essence of the Commission's mandate is to ensure the balance between the individual citizen's right to privacy and the citizens' right to access to public information. The Information Practices Commission should communicate directly with citizen groups to be sure that major issues of concern to the public are being sufficiently examined.

Finally, the Commission will closely examine the experiences of other states and the Federal Government in the enactment of privacy and open records legislation. Several states, as well as the Federal Government, have enacted comprehensive legislation in this regard in the last decade. The State of Maryland can learn much from the experience of other governmental units. Whenever new legislation is being considered, many legitimate questions are asked regarding

the bill's potential impact. This might be particularly the case regarding the privacy provisions of such comprehensive legislation. Many are concerned about the eventual cost of enacting privacy guarantees, while others worry that agencies forced to comply with its provisions might suffer a decline in effectiveness. Still others fear that privacy provisions will serve to deny citizens their rightful access to public information. By examining the implementation of privacy measures in other governmental settings, the Commission might be in a position to make useful forecasts for the situation in Maryland. More importantly, however, it will have an excellent opportunity at the policy formulation stage to make adjustments in any possible proposals, thereby learning from the difficulties of others.

Examination of the actions of other governmental units can be particularly useful in one area of the Commission's work: determining procedures to be used to monitor compliance with privacy and open records legislation. Various methods have been used by different states. In some cases, the Attorney General's Office has provided interpretation of the law through the use of opinions. In others, advisory review boards have been created, with final interpretative authority resting with the Attorney General. At least one state has established a Confidential Records Council to hear complaints from the general public. Finally, some units have formed permanent review boards with authority to administer and enforce the law. The Information Practices Commission will be guided in its recommendations by the experiences of these varying methods, as well as by the views of officials within Maryland government.

In summary, the Information Practices Commission commits itself to recommending those measures which will protect the rights of individual citizens concerning personal data while not hampering the performance of state government

or the legitimate access rights of citizens to public documents. The Commission recognizes the delicate and difficult nature of the balance that must be achieved and dedicates itself to arriving at that balance.

FOOTNOTES

1. For an analysis of research findings relating to increases in privacy concerns, see Louis Harris and Associates, Inc. and Alan F. Westin, The Dimensions of Privacy. A National Opinion Research Survey of Attitudes Toward Privacy (Stevens Point, Wisconsin: Sentry Insurance, 1979).

2. U.S. Privacy Protection Study Commission, Personal privacy in an information society. Report of the Privacy Protection Study Commission, 1977. For a further discussion of privacy concerns, see U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the rights of citizens, 1973; National Academy of Sciences, Computer Science and Engineering Board, Project on computer databanks in a free society: computers, record-keeping and privacy; report. Alan F. Westin and Michael Baker, Project directors. (New York: Quadrangle, 1972); Alan F. Westin, Privacy and freedom (New York: Atheneum, 1970); U.S., Congress, Senate, Committee on Government Operations and Committee on the Judiciary, Privacy: the collection, use, and computerization of personal data, Hearings before an Ad Hoc Subcommittee on Privacy and Information Systems and the Subcommittee on Constitutional Rights on S.3418, 93d. Cong., 2d sess., 1974; U.S., Congress, Senate, Committee on the Judiciary, Federal Data Banks and Constitutional Rights, 93d. Cong., 2d. sess., 1974; U.S., Library of Congress, Congressional Research Service, Privacy: Information Technology Implications, Louise E. G. Becker, Issue Brief Number IB 74105,1980; and U.S., Library of Congress, Congressional Research Service, Privacy: Concepts and Problems, Sarah P. Collins, Issue Brief Number IB 74123, 1980.

3. See Donn B. Parker, "Computer abuse perpetrators and vulnerabilities of computer systems", Proceedings of the National Computer Conference 45 (1976): 65-73; and Robert H. Courtney, Jr., Security Risk Assessment in Electronic Data Processing Systems (n.p.: MEC, 1975).

4. U.S., Congress, Senate, Committee on the Judiciary, Freedom of Information Act Source Book: Legislative Materials, Cases, Articles, 93d. Cong., 2d. sess., 1974, p. 6. For a further discussion of issues relating to citizen access to public information, see U.S., Congress, House, Committee on Government Operations, and U.S., Congress, Senate, Committee on the Judiciary, Freedom of Information Act and Amendments of 1974, Source Book: Legislative History, Texts, And Other Documents, 94th Cong., 1st sess., 1975; U.S., Congress, House, Committee on Government Operations, A Citizen's Guide on How to Use the Freedom of Information Act and the Privacy Act in Requesting Government Documents, 95th Cong., 1st sess., 1977; and U.S., Congress, Senate, Committee on Government Operations, Government in the Sunshine, Hearings before a subcommittee of the House Committee on Government Operations on S.260, 93rd. Cong., 2d. sess., 1974.

5. Maryland, Annotated Code, art. 27, sec. 292, and art. 27, sec. 736-752.

6. Maryland, Annotated Code, art. CJ 3, sec. 828.

7. Maryland, Annotated Code, art. 100, sec. 95.

8. Maryland, Comar, Title 10, Subtitle 03, Chapter 02.

9. U.S., Code of Federal Regulations, Title 45, Part 205, Section 205.50.

10. Maryland, Annotated Code, art. 76A, sec. 3.

11. Maryland, Offices of the Attorney General, Consumer Council, Patient Access to Medical Records in the State of Maryland, 1980. The original survey was conducted in the Summer of 1979. In December 1980 the Consumer Council asked the question again of the same hospitals. The Consumer Council found a general lack of consistency with the responses that were previously received.

12. Maryland, Annotated Code, art. 88A, sec. 6(a).

13. Maryland, Annotated Code, art. 81, sec. 5A.

14. Maryland, Annotated Code, art. 33, sec. 3-11(a), and art. 33, sec. 3-22.

15. Maryland, Annotated Code, Transportation, 12-111, 12-112, 16-118, and 16-119.

16. "Computer data secure", Annapolis, The Evening Capital, 19 September 1978, p. 3.

17. "Md. Tax Data Again Lands in Trash", Washington Star, 26 August 1978, pp. A-1, A-6, and "Tax document security unexplained by State", Annapolis, The Evening Capital, 30 August 1978, p. 3.

18. David Goeller, "Police probe leak of tax information", Annapolis, The Evening Capital, 22 August 1978.

19. Maryland, Annotated Code, art. 76A. For a useful discussion of the Act, see Dennis M. Sweeney and Robert G. Smith, Public Information Act (n.p.: MICPEL, 1980).

APPENDIX

A Selected List of Statutes in the Maryland Annotated Code Pertaining to Protection of Personal Records

Article 27, Section 292 -	Provides for expungement of an arrest record if the individual is not convicted in the particular case and has never been previously convicted of a crime; also provides for expungement of records of first offenders who have been placed on probation.
Article 27, Section 736 -	Provides for expungement of police records for individuals who are arrested but not charged.
Article 27, Section 737 -	Provides for expungement of police records for individuals who are arrested but not convicted.
Article 27, Section 740 -	Restricts employers or educational institutions from requiring an individual who is applying for employment or admission to disclose information concerning criminal charges against him that have been expunged.
Article 27, Section 742 -	Establishes the Criminal Justice Information System.
Article 27, Section 744 -	Establishes the Criminal Justice Advisory Board.
Article 27, Section 751 -	Grants an individual the right to inspect criminal records pertaining to him.
Article 27, Section 752 -	Establishes procedures for challenges to the accuracy of criminal records.
Article 43, Section 54L -	Regulates the disclosure of medical information by the provider of medical care.
Article 43, Section 565C (6) -	Deals with the protection of the records of patients in skilled nursing facilities and intermediate care facilities.
Article 48, Section 354-O -	Regulates the disclosure of medical information by nonprofit health service plans.
Article 76A, Section 1A -	Contains a general statement restricting the collection of personal information.
Article 76A, Section 3 -	Restricts public disclosure of certain types of personal records.

Article 81, Section 5A -	Establishes the confidentiality of property tax records.
Article 81, Section 300 -	Establishes the confidentiality of income tax records.
Article 81, Section 302A -	Places restrictions on the disclosure of income tax returns by those who have assisted in the preparation of such returns.
Article 81, Section 366 -	Regulates the disclosure of retail sales tax information.
Article 88A, Section 6 -	Regulates the disclosure of social service records.
Article 100, Section 95A -	Places limitations on the types of questions to be asked of applicants for employment.
Article 100, Section 95B -	Prevents public and private employees from using polygraph tests for purposes of employment.

The State of Maryland

Executive Department

EXECUTIVE ORDER

01.01.1980.11

Information Practices Commission

WHEREAS, The Constitutions of Maryland and of the United States guarantee a fundamental right of privacy under certain circumstances; and

WHEREAS, There must be a reasonable balance between an individual's right of privacy and the public's right to be informed; and

WHEREAS, A society founded on democratic values necessaril requires governmental openness and accountability and

WHEREAS, It is well recognized that in an age of computers there are contrasting dangers of overexposing personal information and underexposing informatio that should be made public; and

WHEREAS, State government must seek a proper balance between the individual right of personal privacy, the practices of public organizations in accumulating, maintaining and disseminating informatio about people, and the need of the public to be informed;

NOW, THEREFORE, I, HARRY HUGHES, GOVERNOR OF MARYLAND, BY VIRTUE OF THE AUTHORITY VESTED IN ME BY THE CONSTITUTION AND THE LAWS OF MARYLAND, DO HEREBY PROMULGATE THE FOLLOWING EXECUTIVE ORDER, EFFECTIVE IMMEDIAT

1. The Information Practices Commission is hereby created.

2. The Commission consists of thirteen members appointed by the Governor, one of whom shall be a member of the House of Delegates, one of whom shall be a member of the Senate, one of whom shall represent the Department of Personnel, one of whom shall represent the Comptroller of the Treasury, one of whom shall represent the Department of General Services, one of whom shall represent the Attorney General's Office, and seven public-at-large members. The Governor sha designate a chairperson from among the thirteen members.

3. The Commission shall conduct a thorough study of policies and procedures regarding the collection, maintenance, use, security, dissemination, and destruction of personal records held by State government and, in connection with that study, shall:

(a) Study the policies and procedures of the Uniform Freedom of Information Act and the proposed Uniform Fair Information Practices

(Privacy) Act, and, where appropriate, examine the extent to which they interact and interface. The points for initial study may include:

(1) The draft proposal of the National Conference of Commissioners on Uniform State Laws entitled, "Uniform Privacy Act;"

(2) House Bill 112 of 1980;

(3) The report of the United States "Privacy Protection Study Commission";

(b) Hold hearings in which persons with an interest in information practices may present their views;

(c) Conduct meetings, research programs, investigations and discussions as necessary to gather information relating to information practices.

(d) Submit by October 1, 1980, an interim report together with any preliminary legislative proposals regarding the Public Information Act (Art. 76A, §1 et sec. of the Maryland Annotated Code) or any other provision of State law that would be necessary to implement the recommendations of the report; and

(e) Submit a final report by October 1, 1981, together with any legislative proposals necessary to implement the recommendations of that report.

4. Each State agency shall cooperate fully with the Commission in its efforts to accomplish its mandate under this Order.

GIVEN Under My Hand and the Great Seal of the State of Maryland, in the City of Annapolis, this 25th day of December, 1980.

Harry Hughes
Governor of Maryland

ATTEST:

Fred L. Wineland
Secretary of State