COMPUTER PRIVACY AND SECURITY

.....

REPORT OF THE
VIRGINIA ADVISORY LEGISLATIVE COUNCIL
To
THE GOVERNOR
And
THE GENERAL ASSEMBLY OF VIRGINIA

Senate Document No. 27

COMMONWEALTH OF VIRGINIA
Department of Purchases and Supply
Richmond
1976

MEMBERS OF COUNCIL

.....

WILLARD J. MOODY, Chairman

EDWARD E. LANE, Vice Chairman

GEORGE E. ALLEN, JR.

VINCENT F. CALLAHAN, JR.

ARCHIBALD A. CAMPBELL

JOSEPH V. GARTLAN, JR.

JERRY H. GEISLER

ROBERT R. GWATHMEY, III

C. HARDAWAY MARKS

LEWIS A. McMURRAN, JR.

JAMES M. THOMSON

LAWRENCE DOUGLAS WILDER

EDWARD E. WILLEY

.....

STAFF

JOHN A. BANKS, JR.

LAURENS SARTORIS

DENTON ROBERTS

ALAN B. WAMBOLD

CONSTANCE D. SPROUSE

COMPUTER PRIVACY AND SECURITY

Report of the

Virginia Advisory Legislative Council

To the

Governor and The General Assembly of Virginia

I. INTRODUCTION

Man's capacity to gather, order and disseminate information has grown tremendously in the past decades. As this capacity has grown, man has become increasingly aware of the potential dangers to individual liberty posed by possible abuse of this capacity. Not until record-keeping and information dissemination systems acquired a capacity for destroying or severly limiting individual privacy did man come to a full appreciation of his interest in protecing his personal privacy. Despite this developing appreciation, efforts to provide legal weapons for use in defense of personal privacy have not kept pace with technological innovations which continue to make invasion of that privacy ever easier.

The revolution in the use of automated data processing equipment — particularly the electronic computer — has given government and private industry the capacity to compile detailed data on individuals in almost all areas of personal activity (education, employment, credit, taxation, health, government licensing and benefits, law enforcement, and so on). Fears have been expressed as to the possibly chilling effect the existence of such collections of automated personal data systems can have upon a free society such as ours.

Such concerns, and others, caused the General Assembly in 1974 to adopt a resolution directing the Virginia Advisory Legislative Council to study this matter of computer privacy and security and report its recommendations for legislation. The resolution was as follows:

SENATE JOINT RESOLUTION NO. 10

Directing the Virginia Advisory Legislative Council to study and report on Computer Privacy and Security.

WHEREAS, the computer is taking an ever-increasing role in our society; and

WHEREAS, while these instruments are necessary and important in the business, industrial, and governmental growth of the country, if unchecked, they may cause grave inroads in the

privacy of the individual; and

WHEREAS, a study committee of the federal Department of Health, Education and Welfare has made a study of the problems inherent in the untrammelled use of the computer, and has called upon Congress for legislation to "protect us from the protectors", and calls for the creation of a code of fair information practices for all automated data systems, whether run by governmental agencies or private organizations, and to provide criminal penalties for violations thereof; and

WHEREAS, other states have created Privacy and Security Councils, and it appears that a study should be made as to the feasibility of establishing such a Council in the Commonwealth; now, therefore, be it

RESOLVED by the Senate of Virginia, the House of Delegates concurring, That the Virginia Advisory Legislative Council is hereby directed to study and report on all aspects of the problems involving personal privacy and liberty in the use of computers. The Council shall study the experience of other states and make a recommendation concerning the establishment of a Privacy and Security Council in the Commonwealth of Virginia.

The Council shall complete its work and make its report to the Governor and the General Assembly no later than September one, nineteen hundred seventy-four.

As a result of the Council's work in 1974, and owing to the enactment of privacy legislation by the United States Congress, the 1975 Session of the General Assembly adopted a resolution to continue the work of the Computer Privacy and Security Committee of the Virginia Advisory Legislative Council for another year. The resolution read as follows:

SENATE JOINT RESOLUTION NO. 94

Directing the Virginia Advisory Legislative Council to continue its study on Computer Privacy and Security.

WHEREAS, in 1974 the General Assembly directed the Virginia Advisory Legislative Council to undertake a study and report on computer privacy and security; and

WHEREAS, pursuant to the provisions of the study directive, Senate Joint Resolution No. 10, the Council appointed a committee to undertake such a study on its behalf; and

WHEREAS, the committee has held hearings, reviewed legislation and conferred with representatives of government and industry concerning the impact of possible privacy legislation; and

WHEREAS, the Congress of the United States has recently enacted personal information legislation which affects law and

policy in all states; and

WHEREAS, it is further recognized that the Virginia State Crime Commission has gone forward with a study of the consolidaion of criminal records with the view toward the protection of personal privacy as an adjunct thereto and with a study to determine the proper mechanism for the technical and policy management of criminal justice information; and

WHEREAS, additional time is needed by the committee in view of the enormity of the task set before it and in light of the coordination necessary to be achieved between federal trends and activities of other State agencies; and

WHEREAS, the General Assembly is able at this time to endorse as desirable norms for the initiation and maintenance of personal information systems certain elements of a code of fair information practices; now, therefore, be it

RESOLVED by the Senate of Virginia, the House of Delegates concurring; That

(1) It is the sense of the General Assembly that all personal information systems initiated and maintained by any public or private organization should be operated in conformity with the following principles of fair information practice provided that it is recognized that there is a necessity for the adaptation of the following principles for criminal justice information and for the use of additional principles and requirements for such criminal justice information:

(a) There should be no personal information system whose existence is secret;

(b) Information should not be collected unless the need for it has been clearly established in advance;

(c) Information should be appropriate and relevant to the purpose for which it has been collected;

(d) Information should not be obtained by fraudulent or unfair means;

(e) Information should not be used unless it is accurate and current;

(f) There should be a prescribed procedure for an individual to learn the information stored about him, the purpose for which it has been recorded, and particulars about its use and dissemination;

(g) There should be a clearly prescribed procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information;

(h) Any organization collecting or holding personal information should, as the case may be, assure its reliablity and take precautions

to prevent its misuse;

(i) There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent;

(j) The Commonwealth and any agency or political subdivision thereof should not collect personal information except as authorized by law; and

(2) That the study now underway by the Virginia Advisory Legislative Council relating to computer privacy and security is hereby continued. The present members shall continue as the members of the Committee, provided that if any member be unwilling or unable to serve, or for any other reason a vacancy occur, his successor shall be appointed in the same manner as the original appointment was made; and

(3) That the study now underway by the Virginia Advisory Legislative Council shall be conducted in coordination with the activities of the Virginia State Crime Commission in order that comprehensive legislation applicable to all government and private personal information systems may be developed; and

(4) The Virginia Advisory Legislative Council shall complete its study and make its report to the Governor and the General Assembly not later than November one, nineteen hundred seventy-five.

Acting under this directive, the Council reappointed the Computer Privacy and Security Committee to continue the study and report to the Council. A member of the Council, Senator Joseph V. Gartlan, Jr. of Fairfax, continued to serve as Chairman. The following were also selected to serve on the Committee: Peter K. Babalas of Norfolk, Richard Barry of Arlington, Montgomery Knight of Norfolk, Mary A. Marshall of Arlington, J. Harry Michael, Jr. of Charlottesville, Robert Peck of Norfolk, and Robert E. Summers of Norfolk. The Committee met several times and conducted a series of public hearings. The Committee heard extensive testimony from representatives both of the private and public sectors of the economy, including: Office of the Attorney General, Division of Justice and Crime Prevention, Department of Corrections, Department of State Police, Division of Motor Vehicles, Department of Welfare, State Air Pollution Control Board, Department of Health, Highway Safety Division, Virginia Institute of Marine Science, Division of Automated Data Processing, Virginia Retail Merchants Association, Richmond Corporation, Direct Mail/Marketing Association, Northern Virginia Women's Medical Center, City of Virginia Beach, City of Norfolk, Virginia Bankers Association, Reynolds Metals Company, Virginia Savings and Loan League, Virginia Consumer Finance Association, the Associated Credit Bureaus of Virginia, Allstate Insurance Company, Data Systems Corporation, and several private citizens.

Based on this study by its Committee, the Council recommends to the Governor and General Assembly of Virginia:

II. RECOMMENDATIONS

It is the consensus of the Council that the data keeping and data processing capacities of government and of private business have grown to such an extent — particularly as the result of the increased application of electronic computer technology — that the right of the citizens of the Commonwealth to personal privacy is threatened by the unfettered expansion of data storage and dissemination capabilities of industry, commerce, and government. It is the intent of the Council that affirmative steps be taken now by the General Assembly to obviate the possiblity of the emergence of cradle-to-grave, detailed dossiers on individuals, the existence of which dossiers would, "at the push of a button", lay bare to anyone's scrutiny, every detail, however intimate, of an individual's life. Such action by the General Assembly would follow in the lead of the nation's courts which have been active in developing a considerable body of case law firmly establishing privacy as an inherent, inalienable human right.

Additionally, the Council is concerned about the harm to an individual which can result from the dissemination of inaccurate, outdated, or superfluous personal data. Along with a concern to protect the privacy rights of citizens, the Council is anxious to afford means by which an individual may challenge and either correct or have expunged erroneous personal data the dissemination of which could work him economic harm or damage his personal reputation.

The Council is aware, also, that the federal government is becoming increasingly aware of the need to regulate the collection, storage, and dissemination of personal data. The Congress has already passed legislation regulating data storage and examination rights as they pertain to federal agencies. Rules and regulations have also been passed by the federal government, and are being implemented by the states, regulating data collection and dissemination by criminal justice agencies. The Council does not feel it would, thus, be appropriate to undertake a legislative project which would, in a short time, be likely to be preempted by federal legislation. What legislation the Council does recommend, however, should be of sufficient flexiblity that it could be easily expanded should the federal government decide to leave this legislative field open to the states.

The Council has not, in this report or in these recommendations, treated the subject of regulation of record keeping and dissemination by criminal justice or allied agencies. The Council has done so with the understanding and assurance that these matters are to be treated by other legislation coming before the 1976 Session of the General Assembly.

To date federal legislation has concentrated its attention on preventing personal information systems abuse by public agencies. At present the Congress is beginning task force studies of the need for and means of expanding data systems' safeguards to the private sector as well. In the course of hearings, the Council was made

aware by numerous representatives of the Commonwealth's business, industrial and financial communities of the many problems and possible pit-falls associated with adoption by Virginia of detailed personal privacy legislation for the private sector of the economy at the present time. The Council feels that it would be prudent, for the moment, to concentrate its attention on regulation of computer privacy in the public sector for two major reasons: (i) this would permit the accumulation of useful experience in tailoring legislation to specific areas of abuse or potential abuse and, (ii) it would also permit Virginia to benefit from study and research by the federal government in this area, while also preventing the possibility of Virginia private sector legislation's being preempted by the federal governement. Thus the Council feels it best, at the present, to concentrate attention on areas of concern common to both the private and public sectors and on those of the public sector in particular.

More concretely, the Council finds: (i) that some form of legislation is needed to prevent the erosion of individual privacy by the growth of automated personal data files; (ii) that the individual data subject be accorded a clearly stated right and easily implemented procedures to know (a) what records about him are being maintained, (b) to whom such records are disseminated, (c) what the contents of those records are, and (d) how he may make corrections to or challenges of the accuracy or timeliness of those records; and (iii) that some means ought be provided by which an individual may obtain redress for harm resulting from improper collection, storage, or dissemination of personal data.

To prevent the emergence of cases of abuse of the tremendous potential power of inter-communicating, automated, computerized, personal data systems the Council recommends the enactment of a code of "fair data practices", based on the approach employed by codes of "fair labor practices". In brief, this code of "fair data practices" would be a statement of public policy of the Commonwealth that would assure its citizens that their government was actively aware of the potential for abuse inherent in the mass of personal data maintained by State government, and that the State was determined to prevent such possible abuse. The data practices policy of the Commonwealth should provide: (i) that there should be no data system the existence and purpose of which is secret; (ii) that no information about individuals ought to be collected unless the need for such information has been clearly established in advance (data ought not to be collected and stored "because we might need it some day"); (iii) that information gathered should be appropriate to the purpose for which it is gathered; (iv) that information should not be obtained by fraudulent or unfair means (no threat of withholding a service should be made to obtain information unnecessary to the supply or determination of eligibility for such service); (v) that information should not be used unless such information be both accurate and current; (vi) that there should be a prescribed procedure by which an individual may learn what information about him is being collected, by whom, for what purpose, and to whom and for what use such information is being or may be disseminated; (vii) that there should be a clear, uncomplicated, and inexpensive procedure by which an individual

can correct, erase, amend, or challenge information, its accuracy, relevance, or timeliness; (viii) that agencies collecting personal information should take steps (including physical security, hardware and software design) to prevent unauthorized or improper use or dissemination of personal information; (ix) that there should be a clear and simple procedure by which an individual data subject can prevent information about him, which was gathered for one purpose, being used for some other purpose; (x) that neither the Commonwealth nor any of its agencies, instrumentalities, or political subdivisions should collect any personal information except as explicitly or implicitly authorized by law.

More particularly, the Commonwealth ought to establish administrative requirements which would make operational the "code of fair data practices" as restrictions upon the data operations of the State and its agencies. The Council recommends that the following administrative requirements be applied to State agencies: (i) collection, storage, use and dissemination of personal data should be engaged in only to accomplish a proper, agency purpose; (ii) collection of personal data, so far a practically feasible, should be from the data subject himself; (iii) categories of confidentiality and access controls should be established for various sorts of personal data; (iv) information collected, stored, or disseminated should be complete, timely, and pertinent; (v) dissemination of personal data should be permitted only after satisfaction of access and security requirements; (vi) requirement of the maintenance of a list of persons or agencies having regular access to stored personal data; (vii) requirement of the maintenance of a list, for three years or until information is purged, of every access to stored information and the reason for such access; (viii) requirement that persons working with personal data be familiarized with rules governing its collection, storage, etc.; (ix) establishment of physical, hardware and software security of personal data systems; (x) under no circumstances shall the State or any of its agencies, instrumentalities, or any of its political subdivisions, collect personal information concerning the political or religious beliefs, affiliations, and activities of any data subject without explicit authorization by statute or ordinance.

The Council feels that special treatment must be accorded those governmental entities and those academic and commercial organizations which have a legitimate need for and make responsible use of personal data for statistical purposes. Information obtained, disseminated, or used for statistical purposes should, so far as possible, be obtained, used, or disseminated without personal identifying elements (e.g., social security numbers, names, etc.), so that aggregate data could not be used to infer characteristics about an individual or class of individuals. In accord with previous recommendations, the Council feels that statistical-type information, even if thus de-personalized, ought to be released only to those having a "need to know", and that these agencies ought to receive only such amount and kinds of information as may be required to fulfill their agencies' institutional responsibilities.

The Council is concerned, though, that in affording individual access to personal information stored about such individual by the

Commonwealth, such access should not be permitted to letters of recommendation or reference or similar writings, whether written by or to a State official or agency, which are used in evaluating an individual's suitability for employment. Such letters are, and ought to remain, confidential.

Along with these somewhat more comprehensive provisions, the Council is of the opinion that specific attention ought to be given to the need for restricting the trend toward establishing social security account numbers as universal or quasi-universal personal identifiers. The use of an individual's social security number as his driver's license number, insurance policy number, college student identification number, etc., makes it all the easier for unauthorized individuals or organizations to gain access to data about an individual data subject in circumvention of safeguards recommended above. The Council strongly recommends that legislation be enacted to forbid the use of social security account numbers as personal identifiers, account number, policy number, license number, or the like unless such use be specifically authorized by law.

Nothing enacted by the General Assembly pursuant to the recommendations of the Council ought to contain any provision which might have the result of requiring any organization to divulge trade secrets as a part of compliance with personal privacy regulations. There is no intent on the part of the Council to interfere with proper business activities. It is the purpose of the Council's recommendations better to secure individual rights and prevent data system abuses, not to harass the business or financial communities.

In undertaking to implement the above recmmendations, the Council is aware that these protections of individual, human rights cannot be afforded without costs. In government, for example, the costs of upgrading physical, hardware and software security may prove to be not insubstantial. However, the Council feels that the increased costs to operating agencies cannot properly be compared with the human benefits to be derived from increased personal privacy. It is conceivable that certain agencies may experience no cost increases, or might possibly experience cost decline, because implementation of the Council's recommendations could cause some agencies to purge now-stored data and narrow the range of information being sought, stored or used.

The Council is aware of its responsibility to see to it that its recommendations do not generate more problems than they obviate. The Council is aware of the problems associated with the tremendous volume of paperwork and bureaucratization associated with federal personal privacy legislation. The Council is not anxious to create any sort of super agency or another layer of government. The Council does, however, believe some action along the lines of these recommendations is necessary and can be implemented now at modest cost and with a minimum of additional bureaucratization.

Along these lines, the Council has rejected suggestions that a Privacy Board be created at the State level to guard individual

privacy rights. This agency's cost and complexity would, when balanced against possible benefits, probably be prohibitive, especially in economically uncertain times.

The Council has also rejected suggestions which would have required periodic notification, either by direct mailings or by publication, of data subjects of the existence and nature of files being maintained about them. Instead, the Council feels a more appropriate approach would focus on improving the ability of an individual to find out, should he so desire, what data is being collected, by whom, and to what end. Such discovery process would be subject-activated, not compiler-initiated.

In enforcing the "Code of Fair Information Practices" the Council feels it is advisable that victims of prohibited practices may seek injunctive relief and civil damages in the courts of the Commonwealth. This would provide for relief to victms, and would permit the development of a body of personal privacy case law by the courts instead of promulgation of rules and regulations by an administrative agency.

The Council has also recommended legislation, following the pattern of the Freedom of Information Act, which would open an individual's personnel records kept by his employer to scrutiny by the employee. The Council recommends, however, that medical or psychological records contained as part of personnel records be excepted from such inspection.

In summary, the Council feels now is the appropriate time to introduce legislation to set a basis for minimum standards for personal data collection, storage, and dissemination in the Commonwealth. The General Assembly would be well advised to avoid potential gross abuse of the power of intercommunicating data banks by setting reasonable, easily implemented standards of conduct. Well managed, responsible, data systems industries and support systems are as essential to the orderly and efficient operation of modern business, industry, and government as uncontrolled, unrestricted gathering of total information dossiers about total populations are antithetical to a free society. The Council is anxious to assure the former and prevent the latter eventuality.

Respectfully submitted,

.....

Willard J. Moody, Chairman

.....

Edward E. Lane, Vice Chairman

.....

George E. Allen, Jr.

.....

Vincent F. Callahan, Jr.

.....

Archibald A. Campbell

.....

Joseph V. Gartlan, Jr.

.....

Jerry H. Geisler

.....

Robert R. Gwathmey, III

.....

C. Hardaway Marks

.....

Lewis A. McMurran, Jr.

.....

James M. Thomson

.....

Lawrence Douglas Wilder

.....

Edward E. Willey

A BILL to amend the Code of Virginia by adding in Title 2.1 a chapter numbered 26, containing sections numbered 2.1-377 through 2.1-388, to protect the constitutional right of privacy of individuals concering whom identifiable information is recorded and to provide penalties for violations.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 2.1 a chapter numbered 26, containing sections numbered 2.1-377 through 2.1-388, as follows:

Chapter 26.

Privacy Protection Act of 1976.

§ 2.1-377. Short title.—This act may be cited as the "Privacy Protection Act of 1976".

§ 2.1-378. Findings and declaration of policy.—A. The General Assembly finds:

1. that an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

2. that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

3. that an individual's opportunities to secure employment, insurance, credit and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and,

4. that in order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

B. The purpose of this chapter is to ensure safeguards for personal privacy by record keeping agencies of the Commonwealth and her political subdivisions by adherence to the following principles of information practice:

1. There should be no personal information system whose existence is secret.

2. Information should not be collected unless the need for it has been clearly established in advance.

3. Information should be appropriate and relevant to the purpose for which it has been collected.

4. Information should not be obtained by fraudulent or unfair means.

5. Information should not be used unless it is accurate and current.

6. There should be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.

7. There should be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

8. Any agency holding personal information should assure its reliability and take precautions to prevent its misuse.

9. There should be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.

10. The Commonwealth or any agency or political subdivision thereof should not collect personal information except as explicitly or implicitly authorized by law.

§ 2.1-379. Definitions.—As used in this chapter:

1. The term "information system" means the total components and operations of a record keeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

2. The term "personal information" means all information that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject.

3. The term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system.

4. The term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means.

5. The term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization.

6. The term "agency" means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the Commonwealth or of any unit of local government including counties, cities, towns and regional governments and the departments and including any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function. Any such entity included in this definition by reason of a contractual relationship shall only be deemed an agency as relates to services performed pursuant to that contractual relationship.

§ 2.1-380. Administrative requirements.—Any agency maintaining an information system that includes personal information shall:

1. collect, maintain, use, and disseminate only that personal information necessary to accomplish a proper purpose of the agency;

2. collect information to the greatest extent feasible from the data subject directly;

3. establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

4. maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

5. make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto, and (ii) determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

6. maintain a list of all persons or organizations having regular access to personal information in the information system;

7. maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained;

8. take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter, the rules and procedures, including penalties for noncompliance, of the agency designed to assure compliance with such requirements;

9. establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

10. collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any agency unless authorized implicitly or explicitly by statute or ordinance.

§ 2.1-381. Special additional requirements.—A. Any agency maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from its system, or from other systems shall:

1. make available to any data subject or group, without revealing trade secrets, methodology and materials necessary to validate statistical analysis, and

2. make no materials available for independent analysis without guarantees that no personal information will be used in any way that might prejudice judgments about any data subject.

§ 2.1-382. Rights of data subjects.—A. Any agency maintaining personal information shall:

1. Inform an individual asked to supply personal information whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences which are known to the agency of providing or not providing such information.

2. Request permission of a data subject to disseminate part or all of this information to another agency, nongovernmental organization or system not having regular access authority, and indicate the use for which it is intended, and the specific consequences for the individual, which are known to the agency, of providing or not providing such permission, however, documented permission in the hands of such other agency or

organization will satisfy this requirement.

3. Upon request and proper identification of any data subject, or of his authorized agent, grant such subject or agent the right to inspect, in a form comprehensible to such individual or agent:

(a) All personal information about that data subject except in the case of medical and psychological records, when such records shall, upon written authorization, be given to a physician or phychiatrist designated by the data subject.

(b) The nature of the sources of the information.

(c) The names of recipients, other than those with regular access authority, of personal information about the data subject including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority.

4. Comply with the following minimum conditions of disclosure to data subjects:

(a) An agency shall make disclosures to data subjects required under this chapter, during normal business hours.

(b) The disclosures to data subjects required under this chapter shall be made (i) in person, if he appears in person and furnishes proper identification, (ii) by mail, if he has made a written request, with proper identification, at reasonable standard charges for document search and duplication.

(c) The data subject shall be permitted to be accompanied by a person or persons of his choosing, who shall furnish reasonable identification. An agency may require the data subject to furnish a written statement granting permission to the organization to discuss the individual's file in such person's presence.

5. If the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

(a) The agency maintaining the information system shall investigate, and record the current status of that personal information.

(b) If, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, it shall be promptly corrected or purged.

(c) If the investigation does not resolve the dispute, the data subject may file a statement of not more than two hundred words setting forth his position.

(d) Whenever a statement of dispute is filed, the organization maintaining the information system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

(e) The agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

(f) Following any correction or purging of personal information the organization shall furnish to past recipients notification that the item has been purged or corrected whose

receipt shall be acknowledged.

B. Nothing in this sfection or found elsewhere in this chapter shall be construed so as to require an agency to disclose any recommendation or letters of reference from or to a third party which is a part of the personnel file of any data subject.

§ 2.1-383. Information and publication of same concerning systems.—Every agency shall make report to the Division of Automated Data Processing of the existence of any information system which it operates or develops which will include a description of the nature of the data in the system and purpose for which it is used. The Division shall compile and arrange the information so received and annually provide the same to the Secretary of the Commonwealth for publication in the annual "Report of the Secretary of the Commonwealth".

§ 2.1-384. Exemptions to applications of requirements.—A. The provisions of this chapter shall not be applicable to personal information systems:

1. maintained by any court of this Commonwealth;

2. which may exist in publications of general circulation;

3. maintained by the Department of State Police, the police departments of cities, towns, and counties, sheriff's departments, offices of Commonwealth's Attorneys, the Department of Corrections or any of its divisions, the Parole Board, the Department of Law, the Crime Commission, the Criminal Justice Officers Training and Standards Commission, the Judicial Inquiry and Review Commmission, the Department of Alcoholic Beverage Control, or any federal, State, or local governmental agency or subunit thereof, which agency or subunit has as its function the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders; and

4. relating to the parentage of any person.

B. Any data subject denied access to personal information under this section shall be entitled to judicial review of the grounds for that denial in the circuit court wherein the agency has any office or place of business.

§ 2.1-385. Use of social security number.—It shall be unlawful for any agency to require an individual to disclose or furnish his social security account number, for any purpose in connection with any activity, or to refuse any service, privilege or right to an individual wholly or partly because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by federal or State law.

§ 2.1-386. Criminal penalty.—Any officer or employee of an agency who willfully disseminates personal information or any person who fraudulently or improperly obtains any personal information, in violation of this chapter, shall be guilty of a Class 1 misdemeanor.

§ 2.1-387. Injunctions for compliance.—Any aggrieved person may bring an action against any person or agency which has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this chapter to enjoin such acts or practices. The action shall be brought in the circuit court of any county or city wherein the person or agency made defendant resides or has a place of business. In the case of any successful action by an aggrieved party, the person or agency enjoined by the court shall be liable for the costs of the action together with reasonable attorney's fees as determined

by the court.

§ 2.1-388. Civil liability for unfair personal information practice.—Any natural person who negligently or willfully violates the provisions of this chapter, shall be liable to any person aggrieved thereby in an amount equal to the sum of:

1. any actual damages sustained by an individual;

2. punitive damages where appropriate;

3. in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

#

A BILL to amend the Code of Virginia by adding a section numbered 40.1-26.1, relating to employee inspection of files.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding a section numbered 40.1-26.1 as follows:

§ 40.1-26.1. Employee inspection of personnel files.—Every employer shall, at reasonable times upon the request of an employee, permit that employee to inspect such personnel files which are used or have been used to determine that employee's qualifications for employment, promotion, additional compensation, or termination or other disciplinary action.

This section shall not apply to the records of an employee relating to the investigation of a possible criminal offense nor shall it apply to letters of reference nor to a person's medical and mental records except such medical and mental records can be inspected by a physician or psychologist of the subject person's choice.

#