P U B L I C H E A R I N G

before

SENATE JUDICIARY COMMITTEE

on

SENATE BILL NO. 3178
(Right to Privacy and Fair Information Practices Act)

Held:
Senate Conference Room
State House
Trenton, New Jersey
August 11, 1975

MEMBER OF COMMITTEE PRESENT:

Senator Matthew Feldman (Acting Chairman)

* * * *

SENATE, No. 3178

STATE OF NEW JERSEY

INTRODUCED APRIL 21, 1975

By Senators FELDMAN, GARRAMONE, SCARDINO, SKEVIN, FAY, HIRKALA and MARTINDELL

Referred to Committee on Judiciary

AN ACT to regulate collection, maintenance and dissemination of personal information on New Jersey residents by agencies maintaining data systems; to create a Commission on Privacy, Freedom of Information and Public Information for the regulation of and adjudication of complaints in regard to collection, maintenance, and dissemination of personal information on New Jersey residents by agencies or organizations maintaining data systems; prescribing the powers and duties of the said commission and providing penalties for violations thereof.

BE IT ENACTED *by the Senate and General Assembly of the State of New Jersey:*

1. This act shall be known and may be cited as the "Right to Privacy and Fair Information Practices Act."

2. As used in this act:

a. "Agency" means any office, department, division, bureau, board, commission or agency of the State of New Jersey or any of its political subdivisions;

b. "Commission" means the Commission on Privacy, Freedom of Information and Public Information;

c. "Data system" means the total components and operations, whether automated or manual, by which personal information, including name or identifier, is collected, stored, processed, handled, or disseminated by an agency;

d. "File" means a record or series of records containing personal information about individuals which may be maintained within an information system;

e. "Individual" means any natural person;

f. "Law enforcement agency" means an agency whose employees or agents are empowered by State law to investigate and make arrests for violations of State law;

g. "Law enforcement investigative data system" means a data system containing information associated with an identifiable individual compiled by a law enforcement agency in the course of conducting an investigation of an individual in anticipation that he may commit a specific criminal act, including information derived from reports of informants, investigators, or from any type of surveillance;

h. "Officer or employee" means an officer or employee of an agency or organization specifically charged with maintaining a file or data system;

i. "Organization" means any individual, group, association, firm, partnership, trust, corporation, proprietorship or other legal entity not provided for in subsection a. of this section which is located within this State or which transacts any business within this State;

j. "Personal information" means any information that identifies or describes any characteristics of an individual, including but not limited to, his education, financial transactions, medical history, 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.

3. Failure of an agency or organization or its employees or officers to comply with the following provisions shall result in the commission of an unfair information practice:

a. No agency or organization shall maintain a data system whose existence and character has not been published in a public notice complying with the requirements of section 4 c. of this act;

b. Each agency or organization shall insure that personal information maintained in or disseminated from the system or file is, to the maximum extent possible, accurate, complete, timely and relevant to the needs of the agency or organization;

c. Each agency or organization shall obtain written consent of an individual prior to the maintenance or use of any data on such individual unless otherwise authorized by law;

d. No agency or organization shall maintain or collect information describing how individuals exercise rights guaranteed by the First Amendment of the United States Constitution unless such maintenance or collection by such agency or organization is authorized by law or regulation;

e. Each agency or organization maintaining a data system or file shall upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system or file permit him to review the record and have a copy made of all or any portion thereof in a form comprehensible to him and further to permit the individual to request amendment of a record pertaining to him;

f. Each agency or organization shall only use or disseminate information on an individual pursuant to the use published as required by section 4 of this act and any alteration in the use of information maintained by such agency or organization shall be publicly noted pursuant to section 4;

g. Each agency or organization shall hold public hearings as to the purpose and operation of its data system before such agency begins collection, maintenance or dissemination of personal information in a new data system or a data system whose use of information has materially altered. Notice to the public of the hearings shall be given 30 days prior to such hearings and

(1) In the case of a State agency, published in the New Jersey register; and

(2) In the case of a political subdivision, published in a newspaper circulating generally within the political subdivision.

h. An agency or organization shall not establish a data system that does not comply with the requirements of this act nor shall such agency or organization establish or operate a data system that violates the rights of individuals protected by this act.

4. Pursuant to section 3 any agency or organization that maintains an information system or file shall:

a. Make available for distribution upon request of any person a statement of existence and character of each such system or file;

b. On the date on which this act becomes effective and annually thereafter, notify the commission and give public notice of the existence and character of each existing system or file simultaneously and cause such public notice to be filed with the commission;

c. Include in such notices at least the following information:

(1) Name and location of the system or file;

(2) Nature and purposes of the system or file;

(3) Categories of individuals on whom personal information is maintained and categories of personal information generally maintained in the system or file, including the nature of the information and the approximate number of individuals on whom information is maintained;

(4) The confidentiality requirements and the extent to which access controls apply to such information;

(5) Categories of sources of such personal information;

(6) The agency's or organization's policies and practices regarding implementation of section 3 of this act; information storage, duration of retention of information, and elimination of such information from the system or file;

(7) Uses made by the agency or organization of the personal information contained in the system or file;

(8) Identity of other agencies or organizations and categories of persons to whom disclosures of personal information are made, or to whom access to the system or file may be granted, together with the purposes therefor and the administrative constraints, if any, on such disclosures and access, including any such constraints on redisclosure;

(9) Procedures whereby an individual can (a) be informed if the system or file contains personal information pertaining to himself (b) gain access to such information, and (c) contest the accuracy, completeness, timeliness, relevance, and necessity for retention of the personal information; and

(10) Name, title, official address, and telephone number of the officer immediately responsible for the system or file.

5. Each agency or organization that maintains an information system or file shall, with respect to each such system or file:

a. Refrain from disclosing any such personal information within the agency or organization other than to officers or employees who have a need for such personal information in the performance of their duties for the agency or organization;

b. Maintain a list of all categories of persons authorized to have regular access to personal information in the system or file;

c. Maintain an accounting of the date, nature, and purpose of all other access granted to the system or file, and all other disclosures of personal information made to any person outside the agency or organization, or to another agency or organization, including the name and address of the person or other agency or organization to whom disclosure was made or access was granted, except as provided in section 12 of this act;

d. Establish rules of conduct and notify and instruct each person involved in the design, development, operation, or maintenance of the system or file, or the collection, use, maintenance, or dissemination of information about an individual, of the requirements of this

act, including any rules and procedures adopted pursuant to this act and the penalties for noncompliance;

e. Establish appropriate administrative, technical and physical safeguards to insure the security of the information system and confidentiality of personal information and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom personal information is maintained.

6. Each agency or organization that maintains an information system or file shall assure to an individual upon request the following rights:

a. To be informed of the existence of any personal information pertaining to that individual;

b. To have full access to and right to inspect the personal information in a form comprehensible to the individual;

c. To know the names of all recipients of information about such individual including the recipient organization and its relationship to the system or file, and the purpose and date when distributed, unless such information is not required to be maintained pursuant to this act;

d. To know the sources of the personal information, or where the confidentiality of such sources is required by statute, to know the nature of such sources;

e. To be accompanied by a person chosen by the individual inspecting the information, except that an agency or organization or other person may require the individual to furnish a written statement authorizing discussion of that individual's file in the person's presence;

f. To be completely informed about the uses and disclosures made of any such information contained in any such system or file except those uses and disclosures made pursuant to law or regulation permitting public inspection or copying;

g. To receive such required disclosures and at reasonable standard charges for document duplication, in person and by mail, if upon written request and with proper identification; and

h. To correct or eliminate any information that is found to be incomplete, inaccurate, not relevant, not timely or necessary to be retained, or which can no longer be verified.

7. Upon receiving notice that an individual wishes to challenge, correct, or explain any personal information about him in a system or file, such agency or organization shall promptly:

a. Investigate and record the current status of the personal information;

b. Correct or eliminate any information that is found to be incomplete, inaccurate, not relevant, not timely or necessary to be retained, or which can no longer be verified;

c. Accept and include in the record of such information, if the investigation does not resolve the dispute, any statement of reasonable length provided by the individual setting forth his position on the disputed information;

d. In any subsequent dissemination or use of the disputed information, clearly report the challenge and supply any supplemental statement filed by the individual; and

e. At the request of such individual, following any correction or elimination of challenged information, inform past recipients of its elimination or correction.

8. Upon failure to resolve a dispute over information in a system or file, at the request of such individual a hearing may be granted before the commission with the following provisions:

a. The individual may appear with counsel and must be so notified of that right and may present evidence and examine and cross-examine witnesses;

b. Any record found after such a hearing to be incomplete, inaccurate, not relevant, not timely nor necessary to be retained, or which can no longer be verified, shall within 30 days of the date of such findings be appropriately modified or purged unless otherwise ordered by the commission; and

c. Any findings by the commission shall be conclusive if supported by substantial evidence subject to review by the Superior Court of New Jersey.

9. Each agency or organization covered by this act which maintains a data system or file shall make reasonable efforts to serve advance notice on an individual before any personal information on such individual is made available to any person under compulsory legal process.

10. No person may condition the granting or withholding of any right, privilege, or benefit, or make as a condition of employment the securing by any individual of any information which such individual may obtain through the exercise of any right secured under the provisions of this act.

11. No agency or organization shall disseminate personal information unless:

a. It has obtained the written consent of the individual who is the subject of the information;

b. The recipient of the personal information has adopted rules in conformity with this act for maintaining the security of its information system and files and the confidentiality of personal information contained therein; and

c. The information is to be used only for the purposes set forth by the sender or the recipient pursuant to the requirements for notice under this act.

12. Section 5 c. and 11 a. shall not apply when disclosure would be:

a. To those officers and employees of that agency or organization who have need for such information in ordinary course of the performance of their duties;

b. Pursuant to a determination by the agency or organization that the recipient of such information has provided advance adequate written assurance that the information will be used solely as a statistical research or reporting record, and is to be transferred in a form that is not individually identifiable; or

c. Pursuant to a showing of compelling circumstances affecting health, safety, or identification of an individual, if upon such disclosure notification is transmitted to the last known address of such individual.

13. Section 11 and section 5 c. shall not apply when disclosure would be required or permitted pursuant to the Right to Know Law, P. L. 1963, c. 73 (C. 47:1A–1 et seq.).

14. Section 11 a. shall not apply when disclosure would be from one agency to another agency or to an instrumentality of any governmental jurisdiction for a law enforcement activity if such activity is authorized by statute and if the head of such agency or instrumentality has made a written request to or has an agreement with the agency which maintains the system or file specifying the particular portion of the information desired and the law enforcement activity for which the information is sought.

15. a. The provisions of this act shall not apply to agencies charged with law enforcement with regard to their permanent and investigative data systems or files.

b. The provisions of this act shall not apply to data systems or files kept by fraternal, political, civic, religious or any other organizations whose data systems or files are protected by the First Amendment of the Constitution of the United States.

c. An agency or organization may be exempted from any provision of this act by a showing of need to the commission, if such need is required by the public's interest or by law.

d. The provisions of this act shall not apply to investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for employment with an agency or organization, but only to the extent that the disclosure of such material would reveal the identity of the source who furnished information to the agency or organization under an express promise that the identity of the source would be held in confidence, or prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

e. The provisions of section 3 c. of this act shall not apply to personal information collected by agencies or organizations prior to the effective date of this act.

16. a. Any employee who willfully and knowingly keeps an information system without meeting the notice requirements of this act set forth in section 4 shall be fined not more than $1,000.00 in each instance or imprisoned not more than 1 year, or both.

b. Any employee who willfully and knowingly disseminates any personal information about any individual employee in any manner or for any purpose not specifically authorized by law shall be fined not more than $1,000.00 or imprisoned not more than 1 year, or both.

17. a. Any agency or organization who violates the provisions of this act, or any rule, regulation, or order thereunder, shall be liable to any individual aggrieved thereby in any amount equal to the sum of:

(1) Nominal damages of $1,000.00;

(2) Any actual damages sustained by an individual; and

(3) Punitive damages where appropriate, equal to treble actual damages.

b. Whenever it shall appear that an agency or organization or its employees or officers has engaged in, is engaging in, or is about to engage in an unfair information practice as set forth in section 3 of this act, an aggrieved individual or the commission may seek and obtain in a summary action in the Superior Court of New Jersey an injunction prohibiting such person, agency or organization from continuing such practices or engaging therein or doing any acts in furtherance thereof pending a hearing before the commission.

c. The State of New Jersey consents to be sued under this section without limitation on the amount of controversy.

18. There is hereby created a commission consisting of five members which shall be designated as the New Jersey Commission on Privacy, Freedom of Information and Public Information. The members shall be appointed by the Governor with the advice and consent of the Senate for a term of 3 years, beginning on July 1 and ending on June 30, except as hereinafter provided. The Governor shall designate one of his appointees to serve as chairman of the commission. No more than three members shall belong to the same political party. Of the five members initially appointed, two shall serve for a term of 3 years, two for a term of 2 years and one for a term of 1 year. Each member shall serve until his successor has been appointed and qualified. In case of vacancy, however, the successor shall be appointed in the like manner for the unexpired term only. The members shall serve without compensation, but shall be reimbursed for necessary expenses incurred in the performance of their duties under this act. For the purpose of complying with the provision of Article V, Section IV, paragraph 1 of the New Jersey Constitution, the Commission on Privacy, Freedom of Information and Public Information is hereby allocated within the Department of Law and Public Safety, but notwithstanding said allocation, the commission shall be independent of any supervision or control by the department or by any board or officer thereof.

19. The commission shall appoint a full-time executive director, legal counsel and hearing officers, all of whom shall serve at the pleasure of the commission and shall not have tenure by reason of the provisions of chapter 16 of Title 38 of the Revised Statutes. The commission shall also appoint such other employees as are necessary to carry out the purposes of this act, which employees shall be in the classified service of the civil service and shall be appointed in accordance with and shall be subject to the provisions of Title 11, Civil Service, of the Revised Statutes.

20. It shall be the duty of the commission to conduct hearings with regard to possible violations of this act brought forth in complaints by aggrieved individuals. The commission shall impose penalties where appropriate and may order such agencies to cease and desist from an unfair information practice. Findings of fact made by the commission shall be conclusive if supported by substantial evidence. All orders shall be considered final unless the aggrieved party petitions the Superior Court for review within 30 days of the issuance of such order. Failure to comply with a final order or subpena of the commission by any person shall be

punishable by the Superior Court in the same manner as such failure is punishable by such court in a case therein pending.

21. The commission shall have the power:

a. To adopt, promulgate, amend, rescind and enforce suitable rules and regulations to carry out provisions of this act;

b. To subpena witnesses and order the production of documents, compel attendance of such witness and production of such documents, administer oaths, take the testimony of any person under oath and keep records of the proceedings at hearings;

c. To forward to the Attorney General information concerning any violations of this act which may become the subject of criminal prosecution;

d. To prepare and publish, prior to May 1 of each year an annual report to the Legislature; and

e. To promulgate official forms and perform other duties necessary to implement the provisions of this act.

22. In hearings before the commission or any proceeding provided for in this act, an individual shall have the right to be represented by counsel.

23. Appearances by the commission under this act shall be in its own name. The commission shall be represented by attorneys designated by it.

24. If any of the provisions of this act or the application thereof to any person or circumstances be held invalid such invalidity shall not affect the validity of other provisions or applications of this act, which can be given effect without the invalid provision or application and to this end the provisions of this act are declared severable.

25. All acts and parts of acts inconsistent with the provisions of this act are hereby repealed.

26. This act shall become operative 90 days after its enactment.

STATEMENT

The purpose of this legislation is to regulate collection, maintenance and dissemination of personal information kept on New Jersey residents by manual or automated data systems. The bill applies to both private and State-operated data systems. Further, the commission that is created by the bill will have both rule-making and adjudicative powers. Certain rights are created on the behalf of individuals upon whom information is maintained.

SPONSORS' STATEMENT

The purpose of this legislation is to establish safeguards for the collection, maintenance and dissemination of personal information by agencies or organizations. Included in such safeguards are prohibitions against maintaining a data system whose existence is not made public pursuant to the notice provisions of this legislation, using information for a purpose other than those for which the data system was created, and establishing a data system which does not comply with the requirements of this legislation. Further, each agency or organization maintaining a data system must obtain written consent of an individual prior to maintenance or use of personal information maintained on that individual, and each agency and organization must allow an individual to see a record kept on him by such agency or organization. An individual will be permitted to correct any errors found in his record.

An individual has the right to know the sources of information which is entered on his record and names of all recipients of information about such an individual. The uses of information by an agency or organization shall be made known upon request. Standards for dissemination of information are also established and violation of these standards or any other requirement of the legislation shall result in the commission of an unfair information practice.

A Commission on Privacy, Freedom of Information and Public Information is created for the regulation of and adjudication of complaints in regard to this legislation. The commission will be composed of five members and will prescribe rules and regulations as it sees fit.

Damages for violation of the provisions of this legislation are specified as well as criminal penalties for willful and knowing maintenance of a secret data system of dissemination of information in a manner not specified by this legislation.

I N D E X

INDEX (Continued)

INDEX (Continued)

- - - - -

SENATOR MATTHEW FELDMAN (Acting Chairman): A good morning to everyone and I thank you for coming here this morning.

As you know, this hearing has been put off week after week and month after month because of the very long session that the Senate had to endure this legislative year. Finally, rather than see this go into the fall season, this date was selected without the knowledge that many of my colleagues would be on vacation. Nevertheless, we will continue with this and transcripts of the proceedings will be available to all members of the Judiciary Committee. You can rest assured that your testimony will be studied before this bill is formally presented for the Judiciary Committee's consideration.

I want to introduce the people who are sitting with me at the table. To my left is Joseph Behot. He is the Director of the Seton Hall Law School Legislative Bureau, which has been involved and has been very helpful in the drafting of S 3178. Leon Sokol is to my immediate left; that is, only geographically. He is much more conservative than I. He is Administrative Assistant to the Senate Majority Leader. Then there is Larry Zucker, who is Legal Counsel to the Senate Majority Leader; and Gayl Mazuco, who represents the Judiciary Committee. I am pleased to present the hard-working members of our staff to you. They contributed a lot of input to this bill, as did Evelyn Sosower, who is my Ledislative Aide.

Today, we are conducting a public hearing on a bill which I believe will have a far-reaching effect on the life of every individual in the State of New Jersey.

The Right to Privacy and Fair Information Practices Act is the product of intensive efforts by a nationally-recognized authority on the subject, Dr. Alan Westin of Columbia University, assisted by members of the Seton Hall Law School Legislative Bureau, as well as members

of my own staff.

Our objective was to create new legislation that would provide safeguards for individuals against the proliferating tendency of private organizations and public agencies to gather data about individuals.

The bill is designed to give the State the power to regulate the practices of both public and private data system operators, as they collect, maintain and disseminate information about New Jersey residents.

The need for regulation is underlined by the incredible growth of consumer credit in our nation. According to the Federal Reserve Bureau, consumer credit grew from $125 billion in 1970 to $182 billion in mid-1974.

As the amount of credit extended to consumers has grown, so has the business of investigating the personal affairs of consumers who seek credit.

Today, about 2,000 credit bureaus exist in this country. Perhaps 100 million credit reports on consumers are transmitted to client companies by credit bureaus each year.

One of the largest consumer investigative agencies in the United States says that it has dossiers on 48 million people. And one of the main problems with this industry has been that until recently it was almost entirely unregulated.

In 1969, a Subcommittee of the Senate Committee on Banking and Currency held hearings on a bill to correct abuses in the prevailing system of credit reporting.

This Subcommittee heard some hair-raising testimony. Some consumers who had at one time or another received permission from creditors to postpone several installment payments because of unusual circumstances, such as illness, and had subsequently completed all their payments,

found themselves in difficulty later on in obtaining credit elsewhere, because the records of the credit bureau had omitted the true circumstances of the temporary delay in payments.

And there were other reasonable circumstances under which some consumers might not have paid their bills in full; for example, if, through clerical error, they had been billed for goods they had not bought. In many such cases, letters of protest against the incorrect billing had simply gone unanswered by the merchants involved. But a black mark had nonetheless appeared in the credit records of these unfortunates, sometimes devastating their chances of obtaining further credit.

All too many consumers were left to suffer the palpable consequences of invisible forces at work against them.

In 1970, following the Senate Subcommittee hearings on the problem, Congress passed the Fair Credit Reporting Act, which went into effect in April of 1971.

One of the fundamental weaknesses of this act is that it is always up to the consumer to correct the problems of the entire system.

Accoring to Lewis Engman, the Chairman of the Federal Trade Commission, who testified at a public hearing on the operation of the federal law, his Commission made an investigation of how well the disclosure provisions of the Fair Credit Reporting Act were working. He said, "We found that there is often wholesale withholding of information concerning character, reputation or morals."

It is still very difficult for a consumer to find out why he has been refused credit. Frequently, he is shuttled back and forth by the company from which he sought credit and the credit reporting agency, always being referred from one to the other. From all available

evidence, getting a straight answer is far from easy.

Furthermore, a consumer who is not persistent may never find out about the negative aspects of a report in his file, and this old information in bureau files is reused routinely, without any serious attempt at re-investigation, as the basis for further reports.

Critics of the current system have pointed out that the work load imposed on investigators for credit reporting bureaus does make for widespread abuses. Burdened with a quota that is virtually impossible to meet, the harried investigator may take shortcuts that involve presumptions about the applicant's worthiness for credit, based on such factors as his race or the neighborhood in which he lives.

According to these critics, middle-class citizens living in suburban areas may get off with relatively clean slates, but this does not necessarily hold true for lower-income-class people, especially those living in the inner cities.

There is a movement afoot to amend the Fair Credit Reporting Act to correct some of the abuses that continue to plague American consumers. It is my understanding that Senator Proxmire intends to reintroduce in the Congress after recess amendments he first proposed in August of 1973.

Meanwhile, however, there is a substantial body of evidence to support the belief that consumers continue to be the victims of a credit-investigating system that is less than equitable.

This, my friends, is the framework within which we hope to make changes that will benefit the consumers of New Jersey.

The Right to Privacy and Fair Information Practices Act defines the circumstances under which credit reporting services may collect, store and disseminate data.

To correct what appears to be widespread abuses, our bill gives the individual ample opportunity to inspect data in his own file and to challenge or correct such data, not only for credit purposes but also for personnel records, labor union records, hospital records and certain bank records, such as cancelled checks.

If our bill becomes law, no agency, public or private, will be able to maintain or use information about an individual without his written consent, unless the agency has specific, legal authority to do so.

As for data that is already on file, the individual will have the right to correct or eliminate information that is incomplete, information that is inaccurate, information that is not relevant, not timely or necessary to be retained, or which can no longer be verified.

If there is a dispute about the validity of the data, the individual will have the right to provide a statement outlining his position on the disputed information. Whenever the disputed information is used thereafter, the reporting agency will be obliged to report the person's challenge, and to provide the statement of rebuttal he has provided. Furthermore, at the individual consumer's request, the reporting agency will be required to inform past recipients of the elimination or correction of data.

Our act also provides for a hearing procedure if the individual and the reporting agency are unable to resolve a dispute. These hearings would be the province of a Commission on Privacy, Freedom of Information and Public Information.

The Commission's five members, all unsalaried, will be appointed by the Governor with the advice and consent of the Senate. This act gives the Commission rulemaking and adjudicative powers, as well as the authority to levy fines up to $1,000 or impose jail terms of not more than

a year for wilful and knowing violations of the provisions of this bill.

The Commission will have the authority to appoint a full-time executive director, legal counsel, hearing officers and other employees required to carry out the provisions of the Act.

In the preparation of this bill, we made a conscientious effort to strike a balance. While our primary motive was to protect the rights of the individual, which we do believe to be paramount, we did not seek to place unnecessary constraints on the efficient operation of public and private reporting agencies.

We do believe that the Right to Privacy Act achieves a proper balance between these interests. The purpose of this public hearing is to test public reaction to our success in achieving these objectives.

It is my belief that this Act provides profound and far-reaching safeguards of the rights of the individual, at a time when sophisticated data-gathering techniques are threatening those rights. To those of us who feel that Orwell's book "1984" may be uncomfortably close at hand, we submit the Right to Privacy and Fair Information Practices Act as one step in the direction of reversing this trend.

Copies of Bill S 3178 are here if you care to look at the bill.

May I suggest that any written statements you may have you give to our very talented recorder.

I was very pleased this morning to be handed a copy of a statement from Congressman Rodino. He was to have been here this morning. He felt that this piece of legislation is very importance because of its impact on the lives of us who live in New Jersey. Unfortunately, he is not here, but we do have a statement from Congressman Rodino that I will ask Mr. Sokol to read and then submit

formally for the minutes of this hearing.

L E O N S O K O L: (Reading Statement of Peter W. Rodino, Jr.)

"In support of S 3178, the New Jersey Right to Privacy and Fair Information Practices Act, Mr. Chairman and Members of the New Jersey Senate Judiciary Committee, I would like to indicate my endorsement of S 3178, the New Jersey Right to Privacy and Fair Information Practices Act.

"I believe this legislation provides a substantial state complement to the protection afforded to our citizens through the Federal Privacy Act and the Fair Credit Reporting Act.

"If enacted by the New Jersey Legislature, this Act would combine with existing federal legislation to create the most comprehensive program for the protection of the fundamental right to privacy now available in any of the 50 states in our nation.

"I believe the State of New Jersey, which was in the forefront of our nation's first battle for freedom, some 200 years ago, should continue to lead in the protection of individual rights. This Act is a step in the right direction since it addresses directly those areas of private and state data collection which were not dealt with by the federal government.

"The safeguards provided New Jersey citizens in the collection and retention of private data by state agencies and corporate entities operating in our state are clearly an extension of the intent of Congress in the Federal Privacy Act and the Freedom of Information Act. I therefore urge you to consider carefully the merits of the Right to Privacy and Fair Information Act. I hope you will agree with me that this bill deals forthrightly and effectively with the most fundamental rights of our citizens." (End of Congressman Rodino's statement.)

SENATOR FELDMAN: That statement is from the Chairman of the House Judiciary Committee.

I will now recognize those who have advised Miss Mazuco that they desire to testify. First, I will call on Robert Martinez, Special Assistant to the Attorney General.

R O B E R T P. M A R T I N E Z: Senator, I guess I am here representing to some degree the State governmental interest that is regulated by the proposed legislation. I won't pretend, however, to be exhaustive on that subject because it seems to me that a number of departments of State government that are affected ought to take the initiative and the responsibility of commenting directly to you.

Just from a broad State governmental point of view though, I think it is important to note at the outset that the notion of controlling informational privacy held by State government is one that is really fairly recent in terms of the difficulty that has been encountered. Up until perhaps ten years ago, the quantity of information possessed by State government was small and more often than not quite superficial. It made it very difficult to track people and the other type of abuses that one might think of in terms of the collation of information, because of the highly mobile society that we are.

On top of all that, I don't think that it can seriously be said that government had the resources in terms of people to actually interpret data that may have come to their attention in any fashion that could be considered tortious under our current notions of what is harmful and what is not to our citizenry.

So I think the important point to be made is that it is only very recently that we have confronted a situation where it is quite possible that substantial harm can come to citizens by virtue of government collection, collation and dissemination of data. This situation came

about with the advent of computer technology, largely the result of developments in the private sector where there was a profit motive; and, in the academic sector, for research purposes. I suppose to some extent it has been compounded by the fact that in very recent years government has moved more thoroughly than ever before into social-welfare type programs, where information about individuals becomes relevant to discharge of government obligations that serve some public need.

Perhaps on top of all that is a sense that we have today more than ever the need to plan ahead for the allocation of our resources, to plan ahead anticipating social needs or dangers, and this all entails an interpretation, a collection and dissemination of data of one kind or another.

The point to be made, however, is that I don't think government, at least State government, has necessarily been laggard in its efforts to cope with the type of harmful problems which we have all sensed as the basis for this legislation. Attorney General Hyland, for example, last year took note of the problem that we are facing in a commencement address at Gloucester County College and he said that "While we enjoy the fruits of our advanced technology, that same technology threatens some fundamental privacies. The flow of information about a person's background, his activities, his habits and his beliefs is greater than ever before. In many cases, this information is given voluntarily by individuals in return for certain privileges, such as that of a license or to do business or to engage in a profession or secure a loan or a job or to secure a pension or an insurance benefit. In other cases, this information is gathered without an individual's knowledge or specific consent by officials of public agencies, acting legitimately, to discharge

their duties in the furtherance of what the Legislature has recognized to be a public good. But our technology - that's maybe the heart of it - has provided us now with the means for such a speedy relay of information, for such a secretive or inaccessible storage of information and for such an impersonal handling of information, so as to create a potential for abuse that was unheard of just a few years ago."

Now the notion of privacy, informational privacy as we are dealing with it here today, is one that has been kicked around in the legal world quite a bit without any real resolution. One can find cases that sense a notion of privacy and First Amendment freedoms of speech; and Fourth Amendment, freedom from unnecessary search and seizures; and Ninth Amendment, reservation of all rights to the people that aren't otherwise secured in the Constitution; and the Fourteenth Amendment, secure personal liberty by virtue of due process of law. These constitutional concepts have been variously articulated by the United States Supreme Court in cases on contraception, pornography, abortion, press freedom and organizational integrity, such as the famous case of Alabama versus NAACP.

I think personally, if one had to pick and choose a constitutional theory that may be at the heart of the legislation before you, I would tend to prefer looking for some informational privacy in the notion of due process, looking at its due process ramifications. I noticed, Senator, in your introductory remarks, you perhaps labelled as paramount the notion that an individual should have visitational rights on information that is retained about himself.

I think if I had to construct a constitutional theory that requires this type of legislation, it would be on that Fourteenth Amendment ground. There must be

certain minimum levels of procedural fairness required when a person's reputation or financial integrity or ability to perform professionally or in a business sense may be jeopardized.

I don't believe, however, that those of us here today, regardless of our position on this bill, have to necessarily look for any constitutional underpinnings of this legislative proposal or others like it. There is plenty of precedent legislatively to regulate the flow of information, both in the public sector and in the private sector. While, personally, one can grapple ad infinitum in an intellectual sense, looking for some constitutional mandate to do this, I am not sure it is necessary so long as we have the legislative recognition that there are abuses here that ought to be corrected and things here that ought to be regulated. And we have done so before. In the private sector alone, the Legislature and our courts have regulated trade secrets, not because there is any necessary constitutional mandate to do so, but because it makes good sense to do so. It establishes certain fundamental fairness to do so.

Likewise the Legislature and the courts have recognized testimonial privileges, not necessarily because they have constitutional underpinnings, but because it makes sense to do so. It is fair to do so. It encourages basic values of our society.

Likewise more recently, and in another area that is analogous but oft' debated, there has been some legislative recognition certainly in existing law as well as even in avant-garde legislative proposals that deal with the meetings of public agencies, acknowledging that in certain circumstances government, on behalf of the people, has a right to privacy of its own, just as people, themselves, have a right to privacy when they are being discussed by government. So it cuts all ways.

I suppose even the most very recent example of legislative precedent for regulating the flow of information, not necessarily - and certainly in this case definitely not - urged by any constitutional mandate has been in this Committee's dealings and amendments to the wiretap statute, in which it ventured to regulate further the entire area of consent surveillance, even though there is no constitutional mandate to do so, a move which this Attorney General has applauded and concurred with.

So I hope that those who may come before you later, Senator, to oppose this bill or to take issue with some of its technical difficulties don't attempt to make this into a public constitutional issue, nor should its defenders really talk too much about constitutional mandates when a society at this point engages in a discussion of reasonable ways to regulate and control felt abuses.

The present bill, if I have read it and understood it correctly, seems to have two very fundamental sources, dating back to the legislative history of such matters. Many years ago, there was an HEW report on records, computers and the rights of citizens. The major recommendation of that HEW report was to guarantee by legislation some procedural rights for people affected by information collected on them.

I think the second major source, which probably ought to be noted for the record - maybe counsel can correct me if I am incorrect in my assessment of it - seems to be Sweden's Data Protection Act, which, it must be noted, that in addition to the procedural safeguards that HEW has recommended, places a great deal of emphasis on the need for an independent state level or government level agency to control, regulate and administer the Act that establishes it.

I think the notion of "independent" here is quite

important. To the extent that this Commission in your bill, Senator, is allocated to the Department of Law and Public Safety, but is completely independent of it, we applaud that move too.

I have spoken with some - quite a few, in fact - representatives of private industry who may be here today who I am sure are going to regale you with a lot of technical arguments about the bill. I don't want to get into that too much. But I think it is important to note for the record that this subject should not come as a great surprise to the Legislature of this State or to the people of this State because it is one that has had a great deal of attention paid to it at the federal level. Senator, you have already mentioned the Fair Credit Reporting Act and the underpinnings of this bill in that federal legislation. But there is quite a bit more happening at the federal level right now that affects us all.

We all know that Senator Sam Ervin has been a moving factor at the federal level on this type of thing and he originally proposed legislation that covered both civil and criminal - private and public - data collection agencies. That original proposal has been broken down in several respects. The Fair Credit Reporting Act is one. The 1974 Privacy Act, which I don't think can be understated, is another one, affecting mostly federal civil agencies as well, however, to some extent federal criminal justice agencies.

We have under very active consideration in the Congressional Judiciary Committees detailed legislation to control criminal justice information systems and, I believe, federal legislation that would control or extend the provisions of the federal Privacy Act to state government agencies as well as to private data collection agencies, possibly with some jurisdictional limits involved.

So while this may be a subject that has not been frequently or ever, perhaps, publicly discussed in this State, it is not a subject that is wanting in examination by many, many people.

Let me very briefly recount some of the activities which the Department of Law and Public Safety has undertaken in this area, which I think may be important to your considerations.

As I noted at the outset, the development of data systems information and the ability to disseminate it is extremely recent. We have not had the capability perhaps up until as late as 1968 or '69 to even do any harm, simply because of the inability to assess the information and interpret it in any way, harmful or good, and do anything with it. Around 1968, however, when we, meaning the State, got into computer technology for the first time, it became apparent that we had to put together some regulations, not only in the privacy area, but perhaps even more importantly, particularly in your start-up years of any such project, in the area of security and accuracy.

While S 3157 takes due notice of the need for accuracy, I don't think it can be understated. We are trying to secure privacy, but more important than that even where dissemination is legislatively recognized as appropriate, with or without consent, is the accuracy of that information and the subsequent putting of it in a form that one is able to interpret. S 3178, I might add parenthetically, relies heavily on a self-policing mechanism; i.e., the ability of an individual to come in and challenge information, and that is essential. It is absolutely essential.

But it seems to me before you even reach that point, government or anybody collecting data has the responsibility, be it a moral one or, hopefully, a legislative one, to assure itself that the information it is collecting is accurate.

To that end, the Department of Law and Public Safety in 1968 formed an internal committee to assure ourselves that we would be meeting not only some privacy standards, rudimentary perhaps, but there, but more importantly the accuracy standards and some security standards that were absolutely essential. I am pleased to report that one of the first things Attorney General Hyland did when he took office was to ask for an examination by his staff of the prevailing security and accuracy requirements that were imposed on our data collection systems. We feel that we have complied with some of the best and toughest standards that have been articulated in an advisory fashion by the federal government.

Nonetheless, that effort is not one which we consider over. In 1973, under Former Attorney General Kugler, that internal committee was formalized into a comprehensive data coordinating committee. Its charge was not only to oversee the continuing application of the security and accuracy standards to our internal data collection system, but also to begin to develop legislation or other guidelines, dealing with information system that are automated.

When we came to office in 1974, it became quite clear that the charge of that comprehensive data coordinating committee was not extensive enough. Because of their preoccupation perhaps with computer technology, electronic technology, we or they overlooked in a minimal sense, the fact that we are dealing here with rights that should extend or not be circumscribed by the fact that data may be in an electronic form rather than in written form. So the charge of that committee was expanded to review not only the need for legislation dealing with criminal justice systems, involving automated processes, but also those involving manual collection and dissemination systems.

That committee began its work at the same time that the Ervin bills evolved into specific acts dealing with criminal justice systems which we now have before us and, at the same time, that proposed regulations came to our attention prepared by the Department of Justice, regulating the privacy of criminal justice systems.

We are in the process right now of assuring ourselves that we are in compliance - and I believe we are in most all respects - with the federal regulations promulgated in May of 1975 by the Justice Department. We will be in a position to certify that compliance by the end of this year. It is not an easy problem because of the extensive question of accuracy and dissemination that we have to assure ourselves on firsthand. But I have every reason to believe that we will be able to bring ourselves into compliance in large measure.

It is unclear whether federal legislation that is now pending will reach both the manual and automated computer systems that are operative in the criminal justice field. When I say "all of them," it is very clear that they are going to reach those that they fund and those that are otherwise engaged in the interstate transmission of information. But whether they will reach as far down as the local police departments' files, on whomever, that they accumulate over the years in the course of their official business, I am not prepared to say now as a matter of legislative law.

It would be our view, however, that if the federal legislation does not reach that level, then State legislation is absolutely essential and must be a companion measure to whatever is done in the private or civil area.

The Attorney General, I think, is going to insist to the extent that his powers as the State's chief law enforcement officer permit him to do so, regardless of

whether or not the state or federal legislation reaches this problem in the criminal justice area, that we in fact do it administratively. And we have already taken several steps to do that. For example, the Attorney General has forbidden the dissemination of any criminal history information outside of the law enforcement community, which is a standard perhaps rudimentary to some people, but a step we felt had to be taken.

Senator, I am going to address just a couple of general comments on this bill because I believe this hearing has got to be the beginning of what should be a substantial public debate on the subject. We are not going to iron out all our technical problems today.

SENATOR FELDMAN: I don't expect to recognize the bill after today.

MR. MARTINEZ: I mentioned before the need for security provisions. I find that the bill in its present form - and this is not intended as criticism because it is probably something that is not often thought of - does make some passing reference to it; for example, in Section 3 (b) and Section 11 (b). It seems to me, however, that just as much as one has to guarantee some procedural rights and set some standards for dissemination of information, one ought to set some standards for the collection of information. I am not going to make any friends with my former friends in the private sector by saying so, but it seems to me that we have to have some regulation of minimum security standards, both for the collection-accuracy point of view as well as the dissemination access point of view of both automated and manual systems.

I commend to your attention the federal regulations of the Department of Justice dealing with criminal history information which were promulgated May 20th of this year, as possibly a guideline for doing so.

Reaching somewhat into the heart of something that is probably going to be very contentous as far as this legislation is concerned is the notion that it is going to cover privately-maintained data systems as well as those maintained by the State.

I am not certain whether Sections 3 and 4 contemplate the holding of hearings and the publication of notice by private information systems or employers or organizations.

MR. SOKOL: It was an error. For those who weren't notified about that, that one section in the bill, which is on page 3, Section 3, subparagraph (g) where it referred to the mandatory holding of public hearings - that imposition is placed only on public agencies and the inclusion of organizations was an error in the transcription of the bill.

MR. MARTINEZ: I was going to suggest, Leon, that also in 4 (b) you have "giving public notice." That also would apply to organizations. That is line 6, Section 4.

I have a thing against public notices. I don't think anybody reads them. I think what is probably more relevant ---

SENATOR FELDMAN: They read them today.

MR. MARTINEZ: You mean I got here.

SENATOR FELDMAN: Others too.

MR. MARTINEZ: Those are short ones though.

MR. ZUCKER: Can you explain what you mean about the public notice on line 6, under 4 (b)?

MR. MARTINEZ: It is pretty clear that Section 4 applies to organizations, which would mean the private sector people. The question is, other than notifying the Commission, what does it mean to give public notice for an organization? Does that mean publication or ---

MR. SOKOL: Subsequently it talks about filing with the Secretary of State.

MR. MARTINEZ: Okay - and that constitutes the notice. I think the point I am trying to make, however, is that it seems to me that one aspect of this Commission that has got to be emphasized to any agency that is going to administer this Act is that it has to be a place where a citizen can go to find out what the devil is going on. To me, the paramount importance is that the organizations or agencies have to file with the Commission some description of what they are doing.

I am going to dip once more into perhaps the hardest part of this thing to intellectually handle; I am referring to Section 15 (b) on page 7. I am going to characterize my problem here as the question of a conflict of privacies. Essentially what it is saying in Section 15 (b) is that there are First Amendment protections afforded to persons and organizations, etc., to collect information and to disseminate information, and that those First Amendment protections must cause perhaps the lesser regulations of a mere state done on legislative whim, as it were, to yield.

Let me make this very concrete. There have been some proposals in the criminal justice area that would preclude the Attorney General as the State's chief law enforcement officer from giving to the Governor criminal history information about prospective appointees of the Governor - i.e., to his cabinet. It is my understanding that the Governor has called this problem one of the major problems in the pending federal legislation dealing with criminal justice information systems. However, that very information - arrests without disposition information - is available in any large city newspaper morgue and can be disseminated by the newspapers to the Governor whenever they choose. I find this a very difficult anomaly to accept. The Attorney General cannot inform the Governor

at a certain point that someone he is considering may have a bad reputation or, in fact, a history of arrest or whatever, yet the newspaper under a First Amendment privilege apparently would be entitled to not only have access to that information, but to disseminate it, and surprise the Governor with it.

I am not sure that that is fair. I don't know the solution to it though.

15 (b) is a very broad exclusion from the Act of any organization which can assert that First Amendment privilege. I don't necessarily have a quarrel with the First Amendment privilege and I really can't say that the First Amendment privilege has got to somehow yield to the privilege that may be accorded somebody on the other side of the coin by virtue of some other amendment which gives rise to the right of privacy, like the Fourth or the Ninth or something like that. So I have to say that throwing in some exemption for First Amendment privilege is probably apropos even though we are not sure entirely everything that it means; at least I am not. However, I am not sure that that exemption should be a total exclusion from the Act, my thought being that perhaps there are some portions of the Act - and this is where I am really going to get in trouble with the press - which really ought to be subject to those organizations that can assert a First Amendment privilege.

For example, if we say that the visitorial rights of a person about whom information is collected are grounded in Fourteenth Amendment, due process notions, why shouldn't that person be able to assert those rights, even though it is a non-government agency, although a protected agency like the press,against the press to get the information that he needs, with appropriate counter-veiling privacy considerations for any informants? What I am driving at is that you have privacies on every

side of the coin, both by the collector of the information as well as the person about whom it is collected. I am not sure when an organization which is collecting information can assert a First Amendment privilege, it ought to cut off any collateral or analogous rights that the person about whom the information is collected may have, vis-a-vis that information.

As I say, I don't have the solution to it. It is a philosophical problem and I think it is a serious one. I think that if anything ought to be covered, even with respect to organizations that may be able to assert some First Amendment right, it ought to be at least the visitorial rights of a person about whom the information may be collected.

There is one final point I think has to be made about the bill - and this is something you are going to probably hear about in great detail, particularly from the private sector, but it is equally applicable to State government - and, that is, the notion that this kind of thing is not easy to administer. From our point of view, the law enforcement point of view, alone, I can cite a recent example in which Attorney General Levi reported that the FBI under the Freedom of Information Act had received 92 requests for information per working day. This volume of activity led him to explain that he thought that the Freedom of Information Act was supposed to give visitorial rights to people, but not a trespassorial easement, as far as their files were concerned. I am not concerned about a trespassorial easement so much, but I am concerned about raising the public expectation that we have some rights here and not having the resources with which to respond.

This bill is not applicable to the criminal justice information system so I can't give you any

fiscal information on it, but I think it is absolutely essential to get it. In my own view, without knowing the figures, I would judge that whatever it costs, it is probably worth it, at least from a government point of view, even if those costs may be high. But I can tell you as a matter of fact that we have difficulty even now coping with the flow of the requests for information that our own administrative regulations which are similar to these have generated. For example, the Attorney General has said that,upon proper identification, he will give any person the right to see his criminal history information. Proper identification, again to protect the privacy of others who may be inadvertently involved, means that the person has to establish affirmatively his identification by fingerprinting, which we do, at this point, as far as I understand, at no charge to the individual. But it is a time-consuming process to pull all this stuff together.

I can imagine that just that aspect of this legislation or anything similar to it alone would be very expensive. Probably the Legislature is going to have to make the judgment about whether or not it views that expense as being worth it. In my view, I think it will be.

Senator, just in summary, this area is very much in flux as far as the technical details are concerned. I think it will be important over the next few months, as hopefully the debate that is starting today continues, that we watch very carefully the federal developments; and, if for no other reason than a matter of comity, we assure ourselves that our State legislation, if any, is consistent with things like the federal Privacy Act, the Freedom of Information Act, as well as anything new that might come out of the Koch-Goldwater proposals.

I think you have to be complimented for initiating this whole thing, Senator.

SENATOR FELDMAN: Thank you.

You mentioned the federal law. I would like you to comment on that. I am not an attorney. You are. And I am flanked by competent attorneys. But it is my understanding that the federal law about which we spoke and about which you testified to some extent does not apply to records, whether employment records or personnel records or labor union records or hospital and medical records or transactions involving credit cards by the populous of the nation, or keeping one's checking account sacred and keeping outside agencies other than law enforcement agencies, such as the IRS or SCI from going into one's banking or checking account. Am I correct in making the statement that there are limitations to the federal laws that do not touch upon those areas that I have defined?

MR. MARTINEZ: I believe there are some limitations, but the limitations are perhaps not total exclusions from the law. My understanding of the federal Privacy Act of 1974,which applies to the civil records of federal agencies, is that employment records, which is one of the things you mentioned, are covered by the Act. Their dissemination is also limited by the Act, but the visitorial rights of the employee are not guaranteed by the Act, particularly to the extent that material may be there that came in from another source whose privacy also has some privilege attached to it.

With respect to union records and other outside organizational records, the Freedom of Information Act does not pertain to non-federal agencies. I think we would run into the same First Amendment problems that you have identified here and were addressed in the NAACP case.

As far as banks are concerned, I think ---

SENATOR FELDMAN: As to union records, if I am shaping up to work at the docks or I am a teamster at some trucking firm and it is a shape-up, say I am never called or I am called last because there is something in that record that is kept by the union office that is detrimental to me. I don't know it is in there, but upon investigation perhaps I could find out my union or teamster official has something there which is not so and I would want to correct it. This may be the reason that I am always the last one to be called on these shape-up jobs or not called at all.

MR. MARTINEZ: Senator, the union problem, per se, is a very difficult one. You know of the long history of legislative proposals that have attempted to regulate internal union affairs and the competing claims of associational rights that the union itself may have, vis-a-vis the individual member of the union. The absence of clear legal mandates, constitutional mandates, for fairness in the exercise of associational rights is a difficult problem which I suppose has always plagued the union movement.

I don't know to what extent legislation like you have proposed will get away with dealing with that problem. I think if I were a union member, I would feel it is a problem.

As far as banks and credit cards are concerned, I think there is a federal Banking Act with amendments being proposed that would apply to federally-chartered institutions that will get at this to some degree. Again we have competing claims. There are those who abhor the thought that checks are photographed or kept on microfilm and that kind of thing, despite the fact it is serving a public purpose, and would rather simply prohibit anyone from engaging in that activity.

My disposition toward that issue is that it is

very seldom the collection of data itself that is harmful, except to the extent it is inaccurate. It is more its use and dissemination really. And I think your bill has struck a proper balance in getting at that.

SENATOR FELDMAN: You mentioned Section 15 (b). I feel this is rather relevant; it is a statement that was made by Justice Douglas. You may want to comment on it. "The First Amendment was couched in absolute terms: Freedom of speech shall not be abridged. Speech has, therefore, a preferred position as contrasted to some other civil rights. For example, privacy, equally sacred to some, is protected by the Fourth Amendment only against unreasonable searches and seizures. There is room for regulations of the ways and means of invading privacy." Do you concur with that?

MR. MARTINEZ: There is no question about that, with the exception that I wouldn't want to limit my notion of privacy to a Fourth Amendment concept. It is quite clear that even in cases where information is voluntarily given in return for some privilege by an individual, he ought to be able even by way of contract, as it were, to put some limitation on its use.

SENATOR FELDMAN: Thank you very much, Mr. Martinez.

I now recognize Dorothy Schoenwald, American Civil Liberties Union.

D O R O T H Y D U G G E R S C H O E N W A L D: My name is Dorothy Dugger Schoenwald. I am Legislative Director of the New Jersey American Civil Liberties Union, a statewide, non-partisan organization of more than 10,000 members devoted to the protection of the Bill of Rights. Over the past decade the ACLU has actively promoted efforts to protect the privacy and security of citizens who are subjects of increasing

numbers of personal records compiled and maintained by both private industry and government. The ACLU has also provided legal representation to citizens who have been injured by various record-keeping practices.

On behalf of our membership, we strongly endorse the move by Senator Feldman and, hopefully, the entire State Legislature into the effort to protect the right of privacy of the citizens of New Jersey. In my testimony today, I would like to outline the basis for our concern over this issue and suggest a few critical amendments to the bill.

The ACLU believes that the right of privacy is one of the most important aspects of The Bill of Rights. We share the belief expressed long ago by Mr. Justice Brandeis in his dissent in Olmstead v. United States. In one short paragraph, he articulated the importance of the right of privacy and its relationship with The Bill of Rights. I quote:

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, his feelings, and of his intellect. They knew that only a part of the pain, pleasures and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone - the most comprehensive of rights and a right most valued by civilized man."

In short, our Constitution guarantees to each citizen a circle of freedom into which the government may not venture. Yet the increasing tendency of government and private institutions to collect, correlate and disseminate data on individuals threatens our ability to

preserve that circle of freedom. We have found that this increase in data collection on individuals, made possible in part by the recent growth of computer technology, is beginning to create a "record prison" for vast numbers of citizens. Public and private agencies have vastly increased the maintenance, sharing and dissemination of records of arrests not resulting in convictions; files and dossiers on citizens engaged in exercising their rights of free speech and assembly; medical and welfare records of the disadvantaged, the aged and other citizens who qualify for public assistance; bank records of persons and organizations depositing funds in banks; anecdotal record about children and young adults at every stage of the school system; and a wide variety of other personal information pertaining to virtually every aspect of the private lives of American citizens.

Data collection and dissemination practices tend to trap any citizen who gets caught by them, regardless of race or economic background. However, the impact falls most heavily upon the poor and racial minorities. The practice of law enforcement agencies of disseminating records of arrests not resulting in convictions, for example, is statistically twice as likely to result in the loss or denial of employment by inner-city blacks as by whites. In practice, data gathering and dissemination frequently works the way a tracking system works in a school: it makes assumptions about people on the basis of anecdotal information about their past, and then conditions the future of their lives on those assumptions. For this reason, it is often antithetical to the possibility of a free and open society which allows people the opportunity to improve their own lives.

Reports of individuals who have suffered severe damages as a result of the free flow of personal information

are plentiful. I have included in this testimony a few examples of abuse suffered at the hands of uncontrolled data banks, focusing primarily on the credit reporting agencies, perhaps the worst violator of privacy rights.

I will read a few of them:

A businessman, after orally promised a job with IBM in 1957, was refused employment after an investigation by Retail Credit Corporation. The giant of the reporting industry wrongly stated that the man had been the business partner of another man indicted for mail fraud.

Last year a professor's wife in Huntsville, Texas, lost her auto insurance because her credit bureau listed her as an alcoholic. She never drinks.

A Princeton University assistant professor lost her auto insurance in 1972 when Retail Credit Corporation informed her insurance company that she was classified a "morals risk." The reason for the classification was that she was living with a man "without benefit of wedlock."

The auto insurance of a Kensington, Maryland man was cancelled in 1969 because a credit investigator reported his house was "filthy."

As these examples dramatically illustrate, knowledge about an individual by those who will make decisions about his or her life gives those who know more power over that individual. A general purpose of any legislation to control the use of data banks is to give power back to individual citizens by returning to them control over information about themselves. A secondary purpose is to ensure the accuracy of information which the individual chooses to allow to circulate or which he or she is forbidden to control.

For citizens to affect the flow or accuracy of information about themselves, they must know what is circulating. S 3178 represents a sound attempt to turn

this generalized principle of privacy into statutory law. It would subject both government and business information systems to certain basic safeguards to encourage access to, accuracy, relevance and timeliness of information used to make decisions about individuals. The basic principles it impements have been recommended by many, including Frank Cary, Chairman of the Board of IBM. In a New York Times article, Cary said:

"First, individuals should have access to information about themselves in record-keeping systems. And there should be some procedure to find out how this information is being used.

"Second, there should be some way for an individual to correct or amend an inaccurate record.

"Third, an individual should be able to prevent information from being improperly disclosed or used for other than authorized purposes without his consent, unless such disclosure is required by law.

"Last, the custodian of data files containing sensitive information should take reasonable precautions to be sure that the data are reliable and not misused.

"Of course, one way of preventing misuse of personal information is to discourage its collection in the first place."

Despite our basic support of this legislation, the ACLU-NJ is greatly concerned about some of the omissions and specific exemptions from coverage in S 3178. The problems I will address we feel must be cleared if effective protection is to be afforded to the right to privacy.

The first problem is one of initiative. S 3178, as currently written, provides in Sections 6 (a), (b), (c) and (d) that an individual, upon request to an agency

or organization maintaining a data bank, must be informed of the existence and nature of any personal information, and within certain limits, the sources and recipients of the information. The individual must first request the information. We feel that very few will wish to incur the displeasure of the insurance and credit industries by exercising their rights under this provision. After all, credit is not a right, but a privilege. Furthermore, most people, not sufficiently aware of the kind of information collected and the broad dissemination practices, will feel no need to request access to their files. One week before a massive 30-day mass media Privacy Campaign by our New Mexico ACLU affiliate began, a random survey of Albuquerque citizens was made. 85.4 percent felt their privacy was threatened only "somewhat" or "not much at all." If the initiative for putting many of the protections of S 3178 into motion rests with a public not educated to data bank abuse, the Fourth Amendment may lose by default.

A better bill would require that everything obtainable by the obstreperous under S 3178, Section 6 (a), (b), (c) and)d) be sent at least once as a matter of course to every individual without a prior request. Here I guess I would concur with the Attorney General's comments that the costs may well be high, but they are certainly worth whatever protection we can extend to the right of privacy. Nothing would do more to police the data banks and bring abuses to the attention of the general public, than to require the information-gathering agencies and organizations to show each citizen, without waiting for his or her request, what information about him or her is being collected and disseminated. The ACLU strongly urges such a requirement as vital to providing a real solution to abuses of privacy rights.

A second problem we find in S 3178 is the consent requirements. S 3178 requires in Section 3 (c) and 11 (a) written consent of the individual prior to the maintenance, use or dissemination of any data on such individual. Parenthetically, it is doubtful how informed such consent would be without the provision I just suggested, without first knowledge of the kind of information that is collected. An essential element in the protection S 3178 seeks to afford is a requirement that agencies and organizations seeking a report on an individual must obtain consent prior to collection of such information, after explaining the scope and methods of the investigations rather than simply consent for maintenance and use.

Nor is there a provision for a withdrawal of consent. Individuals may not fully realize what they are consenting to until after consent is given and a record compiled. Upon review of the record, an individual may change his or her mind and should have the option of withdrawing future consent.

We see no need for the exemption provided in Section 15 (e), which would provide consent is not required for maintenance and use of information collected prior to passage of this Act. Much improper information is already on the files. 15 (e) would permit continued, unregulated dissemination of such information.

The third major area of concern to the ACLU, in addition to initiation of the flow of information between data bank and subject and the question of consent, is the total exemption of law enforcement agency data systems, Section 15 (a), from coverage of the Act.

Law enforcement agencies are run by humans and, therefore, are not perfect. The increasingly widespread use of computers in law enforcement (National Crime

Information Center, a national law enforcement computer hookup center, which New Jersey is a member of, provides immediate access to records nationwide) is quickly compounding that problem of imperfection. The dissemination of incomplete or incorrect information - arrest records not followed by conviction or without indication of outcome - in fact, labels people as criminals, thereby causing them to act as criminals. This practice is totally at odds with the concept of due process, that a person is presumed innocent until proven guilty.

Let me give again a few examples of law enforcement abuses:

William M. was arrested in 1965 and adjudged under a state youthful offender statute which provides that such an adjudication is not a conviction and that it should be sealed. (We have similar provisions in New Jersey.) Since then, he has tried to secure return of his fingerprints from the FBI. Most recently, he made such a request through a member of Congress and received a response from Clarence Kelley that it is FBI policy "to return fingerprints upon being advised that the record has been ordered sealed." That is what the State law provides. However, because Mr. M. is unable to get the local police department which submitted his prints to seek their return, the FBI holds on to them and disseminates them in a manner forbidden under the laws of the state in which the arrest and adjudication took place.

Another example - Calvin L. joined the Marine Corps in 1965. In August, 1969, he deserted and remained at large until he was arrested on January 10, 1973. He was taken to a military base in California and placed in the brig until March 23, 1973. At that time, he was given an undesirable discharge and released from military authority. He was never court-martialed and was told

that the desertion charges would not be prosecuted because of the discharge.

In June, 1973, he was a passenger in an automobile stopped by the Dallas police. The driver had some outstanding traffic violations and the police apparently ran a National Crime Information Center check and arrested him on a "hold" for the military. After hitchhiking, he was stopped by the Dallas police who again apparently ran a NCIC check, and was detained for over 24 hours on a military "hold" before being released. On December 3, 1973, Mr. L. was stopped by the Dallas police again because he was driving a friend's car with Ohio license plates, and no Texas inspection sticker. Again an NCIC check was made, and Mr. L. was placed in custody for four hours on a military "hold" before being released.

Law enforcement agencies should not be allowed to maintain and disseminate arrest records where there was no conviction, nor should law enforcement agencies be allowed to disseminate partial or incomplete information, nor should law enforcement agencies be allowed to disseminate information to employers. At the very least, we suggest Section 5 of this bill, regulating the internal administration of data banks, should apply to law enforcement agencies, as well as Section 3 (d), forbidding the collection of information about how individuals exercise First Amendment rights. A recent series of articles in the Star Ledger pointed up the violations of privacy rights, particularly in these two regards, within the law enforcement agencies themselves.

Furthermore, the definition in S 3178 of "law enforcement investigative data system" - that is data compiled on an individual in anticipation that he may commit a specific criminal act - seems to expand the statutory powers granted to law enforcement agencies to allow just this kind of dossier maintenance. Much better

language would be a definition of such system in the following manner: "information compiled in the course of conducting an investigation of an individual where there is reasonable suspicion that a specific criminal act has been or is about to be committed." We feel very strongly that the anticipation clause in the current language is much too broad and vague.

In all probability, law enforcement agencies will be able to come forward and describe instances in which crimes were prevented or criminals were apprehended because of the availability of such incomplete records. Similarly, it may be possible to put forward examples of jobs which no sane person would want to be given to people with particular kinds of records. Curiously though, the record of legislative hearings and court cases on arrest records lacks any actual cases where the things people feared actually occurred. But we also feel that the kinds of problems, for instance, in employment, with a bank robber applying for a job at a bank, and reasonably there should be this information known, could be taken care of through a law enforcement contact. The State or whoever holds the information of his arrest could supply this information to local law enforcement officials rather than the bank and risk the further violation of someone who has served his time in securing future employment. But we urge you again not to permit such examples ---

SENATOR FELDMAN: I would put him in charge of security for the bank.

MS. SCHOENWALD: Maybe.

(Continuing) --- such examples, even if they appear, to obscure the broad consequences of record dissemination practices. The United States disseminates arrest and conviction records more widely than any other country in

the western world. While there may be no proof of a cause and effect relationship, it certainly can be inferred from the facts.

Law enforcement data banks should be available only to other law enforcement agencies for law enforcement purposes only.

Before I end this testimony, a couple of points were raised by Bob Martinez that I would think the ACLU has an interest in and concurs with. On the 15 (b) question that was raised regarding First Amendment privileges for any files maintained, I think it is a legal technical point, but perhaps a distinction between First Amendment use of such information and a broad exemption for any organization with First Amendment functions might be a way to clarify that.

Two other small points, but I think somewhat important: One is that in your definition of what can and cannot be maintained in data systems, we would suggest that no uncorroborated information, no hearsay information, should be submittable to a data bank system. Another technical suggestion is on the composition of the Privacy Commission. We suggested at the federal hearings as well that no member of the Privacy Commission should have ties to any data maintenance system. This isn't to say that someone with computer technology and expertise should not be on, but that members of the credit reporting industry and other industries which specialize in data bank practices should not be members of that Commission which will review complaints and abuses.

SENATOR FELDAMN: Is that in your written testimony?

MS. SCHOENWALD: No, but I can write that and submit it to you. I was trying to be somewhat brief today.

I would like to end this testimony by emphasizing again the urgent need for the State Legislature to address the threat to privacy presented by uncontrolled

and inaccessible data banks. S 3178 as drafted does in fact provide substantial protections. The ACLU urges consideration of the points raised today in this testimony as necessary elements in that further protection.

Thank you very much. If you have any questions, I would be happy to answer them.

SENATOR FELDMAN: Your testimony was quite full. Your sentiments were made known and I want to thank you for coming.

MS. SCHOENWALD: We thank you for introducing this legislation.

SENATOR FELDMAN: I recognize Mr. Winterbottom, Special Assistant, Office of the President, Educational Testing Service.

J O H N A. W I N T E R B O T T O M: Senator Feldman, I would like to thank you for this opportunity to present the views of the Educational Testing Service on a piece of proposed legislation in which we have a very keen interest.

As you perhaps know, the Educational Testing Service is devoted to the production of a wide range of tests and examinations, most of which are used to assist educational institutions in making admission decisions, although the purpose of some of our tests does extend beyond that rather limited scope.

In addition to that, we have a very extensive research program which is based to some extent on the files accumulated as a result of our testing activities. We also have a modest instructional program whereby individuals come to our offices at our location in Princeton for purposes of being instructed in areas in which we have some degree of expertise.

I was interested in your opening statement, sir, because of the fact that it came home to me very strongly that the background against which this legislation is being presented has to do to a very large extent with concern over the possibly deleterious effect on individuals of data about them which reside in credit rating organizations.

I would like to emphasize that there are some very considerable implications in the legislation also for the educational community. I was interested in noting that so far as I could tell, according to the list of persons wishing to present testimony, that the Educational Testing Service was the only educational organization represted, at least on that list. There may be others here today, but I haven't been able to identify any.

We are, ourselves, an education organization. But, of course, there are others in the State and one thinks immediately, of course, of the universities and colleges and undoubtedly other organizations which have at least a peripheral interest in education and do maintain extensive data files.

So I think that in working toward legislation in final form in the privacy area, it is very important that the interests of educational institutions who do maintain data files be kept in mind.

The Committee is in possession of a written statement from the Educational Testing Service and I don't feel that further extended discussion at this time would be appropriate. I would, however, like to take just a few moments to comment by way of emphasis on a few of the points made in that statement.

First, as the holder of extensive files of information about many millions of individuals throughout the United States, many thousands of these being citizens

of New Jersey, we are very much in accord with the thrust of the proposed legislation. As data systems have increased in number, size and complexity, they have become more susceptible to abuse, to the possible detriment of individuals to whom the data apply. Careless management of such data systems or what may be worse, deliberate exploitation of them, may have injurious consequences for the individuals involved.

We, therefore, believe that it is a proper function of government to establish criteria and guidelines for the control of these systems, together with mechanisms to assure that legislative requirements will be met.

Second, despite an agreement with the spirit of the proposed legislation, we have some serious doubts that legislation by individual states is the best way to deal with these problems. The Educational Testing Service carries on its activities in all fifty states, as do many other organizations which maintain extensive data files. If numerous states pass legislation which is divergent in important respects, cumbersome and costly procedures will have to be set up within the organizations concerned to respond to the various requirements.

A recent communication from Congressman Edward Koch, Temporary Chairman of the Privacy Protection Study Committee at the federal level, set up by the Privacy Act of 1974, contains the following statement, and I quote:

"The Commission is to recommend to the President and the Congress by June 10th, 1977, the extent to which the requirements and principles of the Privacy Act should be applied to the information practices of state and local governments and organizations in the private sector."

We believe that it would be much preferable to wait and see what legislative proposals come out of the work

of the Commission and meanwhile to work with the Commission to ensure that the interests of the states are properly addressed.

Third, if New Jersey decides to proceed independently, there are two concerns which we believe should be kept in mind in developing legislation. One is the matter of cost. Organizations in the educational sector have few options but to pass increased costs of operation on to the students in the form of increased fees. If the expense of compliance with the proposed law is significant - if, for example, complex procedures for public notification and annual reporting are set up - the result might be another addition to the burden of educational expense already imposed on students and their parents.

The other concern has to do with a possible restraint on research which might result from an absolute prohibition against the exchange of identifiable data. In some cases, particularly in long-range studies where data are periodically added to a research file, name is often the only identifier whereby matching of data can be carried out. Identifiable data should be exchanged for research purposes only in exceptional cases, only when no other procedure will suffice. Also such exchanges should take place only when stringent safeguards to confidentiality are observed.

However, there are occasions when research of great social value can be executed only when it is possible to assembly identifiable data from several files. We believe that the door should be left open to permit such projects to be carried out.

Finally, the Educational Testing Service has been wrestling for many years with the problems of recognizing and protecting the privacy rights of individuals represented in our files. If it is decided to proceed with

the introduction of State privacy legislation, we would consider it a privilege to make our experience available to this Committee or to others responsible for drafting the legislation to the end of making it both effective and workable.

(See written statement by Educational Testing Service beginning on page 1X.)

SENATOR FELDMAN: I want to thank you, Mr. Winterbottom, especially for your help which you have said is forthcoming.

I don't intend to engage in a foot race with the federal government. June 10th, 1977, is the day that the Committee, of which Congress Koch is a member, will submit its report. But there can easily be irreparable damage between now and when the federal law will be implemented or strengthened, because Mr. Engman, Chairman of the Federal Trade Commission, at a recent committee hearing, testified that there is, "wholesale withholding of information concerning character, reputation or morals" of individuals that the individuals could not obtain from various data companies, in view of the fact that the federal law is either not being administered properly or there are weaknesses in the federal law. If the federal law were adequate there would be no such bill as S 3178 before us in New Jersey today.

I may be in a foot race. Who knows? This is a very sensitive and controversial issue.

MR. WINTERBOTTOM: May I ask a question? Is there any mechanism by which the states that are interested in independent introduction of privacy legislation could get together and concert their activities in this field so that the legislation and, I think perhaps even more important, the regulations that put it into force could have some uniformity across states?

SENATOR FELDMAN: Well, Professor Westin, who assisted my staff in coming up with this bill, has touched base with many states and many authorities, federal and state, throughout the nation. And we may very well be the beacon for other states to emulate. We are in constant communication with other states and we will continue to be. You know there is no pride in authorship. Many of our New Jersey laws are based upon similiar laws in other states. So we are forever reaching out for ways and means of strengthening 3178 and this is the purpose of the public hearing.

I do believe there will be a number of amendments that my staff will propose to the Judiciary Committee before we get this bill in final shape.

Again, many, many thanks for coming here today.

MR. SOKOL: As an addendum to what the Senator just said, in the preparation of the bill - and the research and drafting took some fourteen months - every bill that was considered by every state legislature in the country was read, whether it had been passed, was pending or had been defeated, in order to glean from them suggestions. S 3178 represents a synthesis of many of the ideas incorporated in the various bills of other states.

MR. WINTERBOTTOM: Is there any organization or body through which states do get together in order to concert their activities?

SENATOR FELDMAN: There is the Council of State Governments. That is the clearing house and we do keep in touch with them.

MR. WINTERBOTTOM: I think it would be very desirable if the New Jersey legislation, once completed, could be adopted by that organization as a kind of model bill so that other states coming up to this point might be encouraged to adopt it pretty much as it stands, if that would be possible.

SENATOR FELDMAN: Well, I hope so.

I want to bring to the attention of the Educational Testing Service that the Seton Hall Law School Legislative Bureau, represented here by Joseph Behot, has been very helpful. And that is a product of your own testing service.

Thank you, Mr. Winterbottom.

Lester Kurtz of the New Jersey Manufacturers Association will be our next speaker.

(Senator Feldman is advised by a person in the audience that William Dondero will represent the Association.)

W I L L I A M D O N D E R O: I am representing the New Jersey Manufacturers Association and its Committee on Industrial Relations. We welcome this opportunity to submit our views on the subject of Senate Bill Number 3178. My name is William Dondero and I am Director of Industrial Relations with Lenox China, Inc., and Vice-Chairman of this Industrial Relations Committee.

The New Jersey Manufacturers Association is a voluntary business organization with some 13,000 member firms, large and small, in every County in the State. Their representatives on this Industrial Relations Committee have expressed unanimous and sincere concern over the potential severe impact on normal business practice and the potential cost of this piece of legislation.

In order to assess the impact of S-3178 on firms engaged in business and industry, it is essential to understand how this issue gained impetus to the degree that private industry in New Jersey is now facing the regulation of all internal filing systems containing personal information.

Privacy became a public issue in 1965, when federal agencies attempting to create a Federal Data Center, which would combine or permit access to

a large number of individual data systems maintained amongst federal agencies. This caused a public out-cry, due to the creation of individual dossiers, containing all information on an individual gathered by various agencies.

Congressional investigations then continued to explore the collection and use of personal data by private industry, which resulted in creation of a Fair Credit Reporting Act, regulating credit reporting agencies and users of credit reports.

The Federal Statute was enacted in April, 1971, and has been named as the First Privacy Law, regulating a sector of industry.

The Federal Department of Health, Education and Welfare chartered a committee to study the impact of record-keeping and dissemination practices of the HEW Agencies. In 1973, this committee issued its report in book form, entitled: "Records, Computers and the Rights of Citizens", which created substantiation in the minds of many persons that there was a real danger in personal data collection and storage in computerized systems.

This was attributed in large part to the ability of such systems to store limitless record volumes for widespread dissemination through the use of sophisticated data communication equipment.

This report was not intended to be used as a standard for drafting privacy legislation. Yet, as with S-3178, it has, in fact, been so utilized.

Unfortunately, privacy legislation has sought to include private industry record-keeping operations despite the fact that the HEW Committee did not, as part of its operations, make an intensive study of the private sector; their assignment was to study and reach conclusions concerning the compiling and use of information on individuals by federal agencies.

The former Chairman of this Committee has indicated that using the HEW Report for drafting privacy legislation is utilizing the report for a purpose that was not intended, that in making the report, the commission created basic research conclusions from which additional studies could be made for the purpose of drafting privacy legislation.

In December, 1974, President Ford signed into law a Privacy Protection Act, which governed record-keeping practices of federal agencies. This Act was a result of four year's research by Senator Ervin's Government Operations Committee.

Senator Ervin's bill, which became in effect the Privacy Act, originally had included regulation of record collection and maintenance in the private sector. However, this was eliminated from the bill, it being the consensus of the Committee, that to attempt to legislate, as a privacy measure, the record-keeping procedures of private industry would be unwise, since there had been no intensive study of this area.

Dr. Allen Westin, a pioneer in assessing individual privacy standards, in testifying before the committee, cited the impracticality and dangers in trying to regulate and register many tens or hundreds of thousands of files of every kind (in the private sector).

Part of the privacy act creates the Privacy Protection Study Commission whose function will be to study the impact on federal agencies of the regulatory conditions of the privacy act, while at the same time studying the processes of private industry in collection, maintenance, processing and dissemination of personal information.

S-3178 failed to follow this same procedure, since the inclusion of private industry in this bill, before having made an intensive study of the numbers and uses of such information systems maintained by business in this state, has created a circumstance which can only result in tremendous additional operating costs and potential interruption and confusion of normal, legitimate business functions.

So here we see a Federal Bill, which had considered and rejected applicability to the private sector, being reintroduced on the State level with private industry included and with absolutely no evidence that the impact this piece of legislation will have on the cost of doing business in New Jersey was even considered.

Some of the specific problems our committee has observed, should this legislation become law, are as follows:

3.c. - "Each agency or organization shall obtain written consent of an individual prior to the maintenance or use of any data on such individual unless otherwise authorized by law."

By literal translation of this wording, an employer could not even establish a basic personnel or payroll file on an employee without his or her written consent. Nor could the employer use any of the file contents without written permission of the employee. Carried to its extreme, an employee subject to disciplinary action could unilaterally preclude his employer from using any of his employment history as justification of the proposed action. This would be an impossible situation for both Management and Union Representatives.

3.e. - Upon request the individual must be permitted to review his record and must be provided, at nominal cost, copies of personal records applying to him " in a form comprehensible to him."

There is no limitation expressed on the frequency with which an employee can request to see his record. With the open wording of "upon request" this could be done daily and be used to harass the employer. As far as providing data "in a form comprehensible to him", many employers, in conformance to other State and federal programs, have hired employees with both mental and physical handicaps which would make compliance with this requirement a virtual impossibility.

We had another one, Section 3 (g) which was addressed a little while ago, but I understand now does not apply to organizations, just to state and federal agencies. So I will skip that one.

These are but a few of the specific problems we see which cause us great concern.

In 1974, the Office of Management and Budget was requested to estimate the cost of the Privacy Act as it applied to Federal agencies. Their estimate of start-up cost was $100 million dollars the first year and some 1 billion to 1.5 billion over the succeeding five years. While these astronomical figures would not apply to New Jersey State Agencies nor to private industry in the State, substantial additional monies will be required by both the State and private industry should this Bill become law.

In closing, I would point out that our sister state across the river, the Commonwealth of Pennsylvania, had considered this identical piece of legislation earlier this year as House Bill 11. They, realizing that they had no idea of the cost impact such legislation would have on private industry, with the resultant negative effect on the competitive position of Pennsylvania business and industry, rejected this bill.

This is of particular importance to the members of the New Jersey Manufacturers Association, many of whom are small businessmen who are not economically able to absorb costs and administrative overhead and yet maintain a competitive posture with businesses in neighboring states.

With the number of protective instruments already available to employees, such as Union Representation, the Division on Civil Rights, Equal Employment Opportunity and even the Civil Courts, coupled with the rather critical fiscal position of the State and our severe unemployment problem, it seems to us to be totally unnecessary to impose this piece of legislation which can only result in increased taxation and in increased operating cost to business.

We respectfully urge your consideration of these remarks and the defeat of S-3178. Certainly, the private sector should be excluded from the Bill whose language contains so many provisions which are clearly inapplicable to business and industry. Drawing a parallel with the Federal government, any consideration of the private sector will be better served by thorough study, while any legislation passed is limited to the public sector as in the case of the Privacy Act of 1974. Further, we believe that one law,

governing the identical interests of citizens in the fifty states, is much preferable to individual state laws. We suggest that we let the Federal Privacy Protection Study Commission produce its report, based on which Congress can act in a manner which would put all states on an equal footing, so that New Jersey will not suffer further competitive disadvantage.

Thank you for this opportunity to express our views.

SENATOR FELDMAN: Well, there are abuses with any law. Even the repeal of prohibition brought about abuses. There was some excessive drinking.

I am a member of your Association. I want you to know that.

MR. DONDERO: Good.

SENATOR FELDMAN: I am very happy to be a part of the New Jersey Manufacturers Association. But I was concerned about the protection of individual rights when the idea of this bill came to me.

Now, if I were to apply to one of our department stores for credit, I would have to fill out a card and that signifies my consent to run a credit check on me. I have made application when I applied for this particular credit. So I think that would take care of one of your objections about written requests. There will be a proliferation of them going into various companies.

Number two, as far as excess work is concerned, all the information that now has been gathered is "grandfathered" in. It is new information that we are talking about. The work has been done now and doesn't have to be done all over again. Once the information is there, it is there. We just want to protect people from information that is not accurate. That is what

this is all about.

I know counsel has some questions he will be asking you to help us decide what amendments we should make to the bill after listening to you.

MR. SOKOL: Mr. Dondero, on page 4 of your statement in the examples you give as to the burden this legislation might place upon the private sector, you, firstly, talk about the written consent including personnel records. I think Senator Feldman underlined for you how that could be handled in a very innocuous and unburdensome way. Certainly, to use the analogy in the employee sector, when an employee signs up as an employee , he certainly can give as one of the terms and conditions of his employment his consent to you to establish a personnel file on him.

You make a statement here: "Nor could the employer use any of the file contents without written permission of the employee." I call your attention to Section 12 (a) of the bill on page 7,which specifically excludes the operation of officers and employees of an agency or organization who use that information in the ordinary course of business.

MR. DONDERO: "Officers and employees of that agency or organization. . .," yes; but you get into a union problem, let's say, and you get involved with people who are not part of your organization - you get involved with international union officers who are not part of the organization.

MR. SOKOL: Can you be more specific as to the kind of example you have in mind?

MR. DONDERO: A disciplinary case with an employee where an employee is discharged. It goes beyond the people in your immediate organization. It goes to

the international union level. It goes to maybe an arbitration case.

The employee under this wording could exclude you from using his file; he has to give you written permission to use it.

MR. SOKOL: You are saying where the union wants to get rid of an employee and the ---

MR. DONDERO: No, where the company wants to, vice versa.

MR. SOKOL: Why would an employee want to prevent his union from getting access to his file?

MR. DONDERO: To prevent the company from using the file. He has a history of bad conduct, say, and you cannot use it. Now what? He says, "I will not give you my written permission to use the file."

MR. SOKOL: Again couldn't this be handled in a routine way in terms of his consent to conditions of employment?

MR. DONDERO: Perhaps. I don't know whether it would stand up. But this wording says "establish or use" the file.

MR. SOKOL: I am saying you would meet the statutory requirement if you made part of the terms and conditions of employment prior consent and approval by the employee to use it for the purposes that you think you would have to use a personnel file.

MR. DONDERO: If that could be accomplished and conform to the law, yes. But the way it is worded now, each individual would have the right to deny you that use.

MR. SOKOL: We are talking about prior consent and I am submitting to you that furnishing you with prior consent as a condition of employment would meet all the statutory requirements in the law.

MR. DONDERO: You know as well as I, the employee is going to say, "Well, I had to sign that or they wouldn't have hired me in the first place." Right?

MR. SOKOL: But there is nothing in the law that says that is a violation of the law. We are not talking about compliance with the law. Having complied with this law, you are now no worse off or better off than you were before the law was passed. All of the rights you had before outside this law would still exist.

MR. DONDERO: We are quite concerned about the way this is worded because of the requirement that an employee give you permission to use his own file. That is one of our big concerns.

SENATOR FELDMAN: I just want to make a comment on Dr. Westin. You mentioned him in your testimony and said he felt the federal law was too burdensome and just couldn't work. Dr. Westin was to be here today to testify for the bill.

MR. DONDERO: I know that.

SENATOR FELDMAN: Unfortunately, a medical appointment came up and he could not be here. But he helped draft 3178. If you acknowledge him as one of the experts ---

MR. DONDERO: Yes, it would have been interesting to hear from him that he meant it to apply to private industry as well as these credit agencies, etc.

SENATOR FELDMAN: Actually he will read the transcript of your testimony and everybody's testimony. We are hoping he will make comments on it.

MR. DONDERO: Very good.

SENATOR FELDMAN: Thank you very much.

MR. DONDERO: Thank you for the opportunity.

SENATOR FELDMAN: Lewis Applegate, New Jersey State Chamber of Commerce.

L E W I S R. A P P L E G A T E, S R.:

My name is Lewis R. Applegate, Sr. I'm Director of Governmental Relations for the New Jersey State Chamber of Commerce and speak here today for that organization. As you may know, the State Chamber is a voluntary association of businesses and professions, large, and small, engaged in every conceivable type of economic, medical, educational and other activities in all corners of New Jersey.

The subject bill before you today -- the "Right to Privacy and Fair Information Practices Act" -- has antecedents that are worth reviewing. The Federal Department of Health, Education and Welfare sponsored a study early in 1972 to examine the issues of privacy. A comprehensive report on this was made in July, 1973 -- sometimes called the Ware Committee Report -- which contained many excellent recommendations, as well as a set of basic principles to be used as guidelines for protecting individual privacy. Those included the following:

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

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

-- 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.

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

-- Any 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 the data.

We do not take exception with such principles. However, they were presented as goals and not as a statement of present technological feasibility. Subsequent to the Ware Committee Report, a Domestic Council Committee on "Right to Privacy" -- chaired by, then, Vice-President Gerald Ford -- recommended that initial privacy initiatives should focus on the Federal Government and that Federal example and experience in this complex field should precede directives covering non-Federal governmental and private sectors. The same conclusion was also reached by the U. S. Congress in the course of developing the Privacy Act of 1974, which is now public law. The state and local governments, as well as the private sector, were specifically omitted from that legislation. In addition, a Privacy Protection Study Commission was authorized to assess the need for increased regulation of these organizations. This was done as a very positive step partly because the potential for invasion of privacy and the range of people covered was so great, partly because the subject was so

complex, and partly from a recognition that the impact on business and local governments could be substantial. We consider that to be a very prudent judgment.

We believe this to be a viable approach to the subject. This approach stresses the need to gain experience in applying personal privacy legislation to a specific portion of the public sector before attempting to develop such legislation for the private sector.

The reasoning behind this approach is that potential for invasion of privacy by the government is much greater than by private business. Of necessity, the government is involved in activities which require accumulation of sensitive personal data. Further, the purposes for gathering the data are both operational -- to perform a specific function such as paying unemployment benefits -- and regulatory, to ensure that no violation of the law occurs. Therefore, the desire of one governmental agency for access to the files of another can be quite strong, especially in carrying out the regulatory aspects of various Federal laws. By contrast, the existence and content of a data file in the business world is usually known by the individual and interchange with other companies is limited both by existing governmental regulation, by competitive conditions and by economics.

Our position, then, is that we support the principles of personal privacy. At the same time, we feel that attempts to impose these principles on the private sector through legislation can be quite costly and potentially operationally counterproductive for the simple reason that no one at this stage knows enough about the financial and operational impact of personal privacy legislation versus its effectiveness.

The Congress considered the vastness of these issues and reached the decision that application of "right to privacy" legislation to the private sector required much more study. The subject is so complicated and potentially so costly that a Privacy Commission was established to conduct a two-year study of all the ramifications involved.

Although we heartily subscribe to the concept of States Rights, we also believe that all consumers and citizens would be better served by a single Federal law covering privacy than by 50 separate and diverse state laws. Therefcre, our primary recommendation to this Committee is to give the Privacy Commission time to study the impact of the existing Federal law, to make recommendations with regard to cost effectiveness of various means of implementation, and in general to complete their job before applying any similar law, in some manner, to the private sector, particularly in New Jersey.

The citizenry's biggest concern with privacy and the private sector organization seems to be centered in the credit field; at least most of the publicity emanates from that activity. However, the Federal Fair Credit Reporting Act and other recent enactments and regulations now provide individuals a great degree of privacy protection. But, in the area of governmental files (criminal history, welfare, medical, taxation, vehicle registration, etc.) far greater abuse potential exists with minimal existing legal protections.

Therefore, if New Jersey's Legislature at any time feels that the Federal Privacy Commission is not doing its job well enough or fast enough or that individual citizens need additional privacy protection sooner, we suggest that legislation such as S-3178, modified to apply only to the

personal data systems of governmental agencies, could be enacted. Any such legislation should, of course, provide for a thorough evaluation of the cost/benefit facets of implementation.

In summary, we do not believe there is a need in New Jersey for immediate action which would justify the very substantial burdens that would be created by hasty implementation of personal privacy legislation covering private business. The result could be a substantial increase in business operating costs, which will eventually get passed on to the consumer, and a real danger that the legislation could have a disastrous effect on small businesses.

SENATOR FELDMAN: Thank you, Mr. Applegate.

Mr. J. Adelman.

MR. ADELMAN: If you don't mind, I would rather wait until later.

SENATOR FELDMAN: You are unique.

Then I will call on Joeseph Frankel.

J. J O S E P H F R A N K E L: Good morning, Senator. On behalf of the Prudential, I want to thank you for giving us the opportunity to testify here this morning.

I just submitted to you a copy of our testimony in this matter. I am not going to take the time to read my entire statement and I will be very brief.

I would like to echo on behalf of the company the statements made by Mr. Applegate and also by Mr. Dondero of the Manufacturers Association.

I would like to leave with the Committee though the thoughts of a particular company and how the bill as it is currently drafted might present problems for a company such as the Prudential.

I think it is important to note that there are

many business organizations such as ours which maintain information on a company or a national basis and that a state-by-state approach to the privacy problem - and I might add parenthetically that there are currently some 85 different bills pending in 35 states on privacy protection - will cause tremendous confusion and expense for business to the detriment, we feel, of the public. For example, our company, as you probably know, does business in all fifty states. We maintain records not only in Newark, which is our home base of operation, but also in Florida and in California. We have several large regional offices located in major United States cities, which also maintain records. It is our thought that if legislation such as this were to be passed, it would create severe problems for us because we would have to work out compliance criteria for all of the different states that might pass legislation of this kind and the constant reworking of our computer systems to accommodate each state's different criteria would result in great costs to our company and, consequently, to our policyholders.

The thought I want to leave with you is one of caution. Take your time. There is a lot of activity going on, as you have already mentioned, and you know about it. We feel that there is no more important problem than privacy, but we think it would be judicious for the Committee to take its time and to gain the benefit of the work that is being done at the federal level.

That is the thought I would like to leave with you, Senator; and we appreciate the opportunity to be heard this morning. Thank you very much.

(Written statement submitted by Mr. Frankel can be found beginning on page 20X.)

SENATOR FELDMAN: Mr. Frankel, I want to make it clear once again that it is only because the federal

government has been dragging its feet painfully over the years that I have felt some action was necessary in New Jersey. If the federal government would act --- and I agree with you that I would rather see uniform legislation affecting 50 states. There are many things I would like to see unified throughout the country. For example, welfare, in my opinion, is a national problem and not a problem which is local to New York, New Jersey and the other states.

I do hope that the federal government is going to move. But I have a reservation about their moving and we have to wait until 1977 just for a committee report and then the bills have to be enacted.

MR. FRANKEL: I appreciate that. There is an excellent article - I don't know whether Mr. Sokol has read it, perhaps he has - which I mentioned in my statement that has to do with this question. It is in the ABA Journal of July, 1975. It goes into the whole discussion of what the Privacy Study Commission is doing. I recommend it to you. I think it is an excellent article.

I appreciate what you are trying to do. On the other hand, piecemeal legislation all over the country, I think could result in many, many problems. That is our thought on the subject.

SENATOR FELDMAN: Thank you very much.

I will now recognize Mr. Lawlor, President of the New Jersey Savings League.

E D M O N D V. L A W L O R, J R.: Senator Feldman, we appreciate the opportunity to be hear this morning and present a statement on behalf of the New Jersey Savings League in connection with this bill.

The New Jersey Savings League is the trade association of savings and loan associations in New Jersey. Over 99 percent of the assets of the 248 associations

in New Jersey are held by the members of the League. Savings and loan associations in New Jersey hold approximately $12.7 billion in assets; and $10.1 billion of their assets are invested in mortgage loans, primarily on residential real estate. This amount is approximately equal to the total savings held by the Association. Savings and loan associations are the largest single lender on residential real estate in the State.

It would appear that as presently worded, Senate Bill 3178 would apply to savings and loan associations and other financial institutions which extend credit to members of the general public.

Section 2-i. defines organization as "... any individual, group, association, firm, partnership, trust, corporation, proprietorship or other legal entity not provided for in subsection a. of this section which is located within this State or which transacts any business within this State". (Subsection a. pertains to state or other governmental agencies.)

If the bill were passed in its present form, savings and loan associations, along with other financial institutions which are in the business of extending credit, would have to meet a number of ex-

tremely burdensome requirements under this act in order to obtain the necessary information to extend such credit. In many cases, such compliance would serve no useful purpose because these institutions already have similar requirements under existing laws or regulations. We are setting forth in this statement for the committee's consideration some of the things that savings and loan associations would have to do in order to be in compliance with the requirements of the bill if enacted. We hope that this will illustrate the importance of an amendment to the bill which would exclude financial institutions from the purview of the law.

Senator, if I may, I will go through it section by section as they apply to savings and loan associations.

Section 3-a.

Savings and loan associations would have to publish in a public notice the existence of their data system.

Such publication would be meaningless because the existence of such a system in a lending institution which deals primarily in home mortgage lending is self-evident.

Section 3-b.

Savings and loan associations would be required to, under this section, update personal information maintained.

This would be a waste of time and effort because the association has no use for the credit information beyond the time that the original loan application is made. The only reason the credit information is retained in a mortgage lender's file is for auditing purposes and for use by the supervisory authorities to ascertain that the savings and loan association complied with the law and was prudent in the making of the mortgage loan.

The Savings and Loan Act (C.17:12B-197) authorizes the Commissioner of Banking to adopt rules and regulations regarding the required records which must be maintained by an association in conjunction with its mortgage lending activities. The Commissioner's Regulation #3:37-1.4(b) requires associations to retain in their files a credit report and a financial statement made by the mortgagor at the time of an application for a mortgage loan.

Section 3-c.

Savings and loan associations, under this section, would be required to obtain written consent of each applicant to maintain credit information in their files, which we have pointed out is mandatory in conjunction with the loan.

Presently the Real Estate Settlement Procedures Act requires that a mortgage applicant be given a booklet at the time of the application in which all of his rights are explained and the procedure with regard to

the closing of the loan is explained, as well as the information that he will be given a disclosure statement. Then two disclosure statements are given to the applicant at the time the loan is committed upon, at the time of the closing, which explain to him the cost of credit. So the credit report is mentioned and he is aware of it entirely through the procedure as far as the application for the mortgage loan is concerned.

This practice would have no relevancy with respect to savings and loan associations because, in most cases, the mortgage applicant pays for the cost of the credit report and is informed of this cost at the time of application. He, therefore, is automatically aware of its existence. He also, as part of this application, must supply pertinent financial information which obviously will be retained in the association's file.

Section 3-e.

Savings and loan associations would be required, under this section, to grant an individual access to his record or to any information pertaining to him which is contained in their files.

The Fair Credit Reporting Act, which became effective April 21, 1971, (91-508, 85 STAT. 1114) already requires that savings and loan associations advise any mortgage applicant, whose applica-

tion has been refused for reasons of credit, of the name of the credit reporting bureau which supplied the credit information. The applicant, under that act, also has the right to make a written request within 60 days for a full disclosure of the nature of the information on which the decision was based. There would be no reason for the applicant to request this information if the mortgage was granted.

Senator, at this point, let me interject another thought, that savings and loans basically are not collectors of credit information. They are not credit rating organizations, but they are users of credit. The credit is used at the time of application in order to determine whether or not the applicant is a worthy applicant for that particular mortgage.

Section 3-f.

This section would require savings and loan associations to use information on an individual only for use as published in the public notice.

The only purpose of obtaining credit and financial information on a mortgage applicant is to aid the savings and loan association in making the determination as to whether or not a mortgage loan should be made to him. Therefore, this requirement would not be applicable to mortgage loan transactions.

We did strike out the section with regard to 3 (g) because that was clarified by these gentlemen.

Section 4.

The requirements in this section for making available, upon request of any individual, a statement of existence and character of a data system and notification of the commission of the existence and character of each existing data system would appear to apply to savings and loan associations.

This would serve no more useful purpose than notifying a mortgage applicant that the savings and loan association intends to appraise the property being offered for security of the loan to make certain that its value is sufficient to secure the debt. There is no logical reason to make this and the other requirements of this section applicable to savings and loan associations.

Section 5-a.

This section would prohibit savings and loan associations from disclosing credit information on an applicant to outside sources.

As a matter of practice, associations refrain from doing this because of the exposure to possible litigation resulting from possible release of incorrect information or violation of the confi-

dential nature of their business transactions with their mortgagors. In addition to this, section 117 of the Savings and Loan Act requires that a confidential relationship between a savings and loan association and its members be maintained.

The only time that savings and loan associations release this information is with the consent of the borrower.

MR. SOKOL: Is an applicant for a mortgage considered a member?

MR. LAWLOR: Not an applicant; but once he becomes a borrower, he is a member. An applicant is not a member, no. Once he becomes a borrower, he is automatically a member of the institution.

Section 5-c.

This section requires the maintenance of records showing the date, nature, and purpose of all access granted to the system or file and other disclosures of personal information made to outsiders.

This would not have relevancy to the typical mortgagor/mortgagee relationship because of the confidential nature of this information before mentioned and would be meaningless because once the credit information is acted upon, immediately following the application for the loan, there is no reason for granting access to it except for an audit or supervisory examination.

The other requirements of this section deal with the rules of conduct and instruction with people involved with the design and development of operation or maintenance of the system, etc.

This would be an equally inappropriate requirement for savings and loan associations.

Section 6.

This section contains safeguards to assure an individual, upon request, the right to information about the existence of the system, access to the system, the names of the sources of personal information, and other aspects of the use of the information in file, and the accessibility to the file to the individual and any person he may choose to accompany him.

All of the above do not fit the circumstances attendant to a mortgage loan transaction.

Sections 7. through 11. provide for: the opportunity of an individual to challenge information contained in the file; the responsibilities of the "organization", with respect to such a challenge; procedures for correction of incorrect information disseminated by the organization; the manner in which a dispute over the accuracy of information is to be handled in the file; restrictions on dissimulation of the information, etc.

All of these requirements have no bearing on savings and loan associations because of the manner in which they use the credit information of their applicants.

This measure may not have been intended to apply to savings and loan associations and other financial institutions, but there is every reason to believe that it does. For that reason, we respectfully urge the Committee to amend S-3178 to include among those "organizations" exempted from provisions of the act all savings and loan associations of this State and other financial institutions.

Senator, we have had our counsel draft some proposed amendments to the Act which, with your permission, I would like to submit for consideration by the Committee.

SENATOR FELDMAN: Mr. Lawlor, you have asked for amendments to the bill and you have asked that the savings companies in the Savings League which you represent be exempt. Do you favor the concept of the bill other than the part from which you request exemption? That is very unique because the Savings League generally wants to be included in everything, but now you have asked for an exemption.

MR. LAWLOR: Senator, we are not opposed to protecting an individual's privacy in any way. But we just feel

that as far as this bill is concerned, it doesn't have applicability to us. We are included in it and we would have to comply with it, which would be very costly.

SENATOR FELDMAN: I can appreciate that. I just wanted to get your feeling as one of the citizenry of New Jersey, if you care to answer, whether or not you feel that something should be done to protect the privacy of the citizens of our State.

MR. LAWLOR: I think where it can be accomplished without causing undue burden on the people who must comply with it, which ultimately would result in an additional hardship for the private individual, yes.

SENATOR FELDMAN: That is a fine benediction before lunch.

We will break for lunch. It is now 12:30 and I hope to resume the hearing at 1:30. Mr. Dudley North will be the first witness this afternoon.

(Recess for Lunch)

SENATOR FELDMAN: We will now resume our hearing. I'll call upon Mr. Dudley North, President of Hooper-Holmes Bureau to be the next witness.

D U D L E Y S. N O R T H: Good afternoon, Senator Feldman. I would like to briefly read a statement which we have submitted to the Senate Judiciary Committee. I believe we have furnished sufficient copies for all the members.

My name is Dudley North and I am the president of The Hooper-Holmes Bureau, Inc. Our executive offices are located at Basking Ridge in Somerset County.

The Hooper-Holmes Bureau, Inc. was founded over 76 years ago in New York City. Approximately 25 years ago, our corporate headquarters were relocated to New Jersey. Our company provides business information to the insurance, banking, credit card and direct mail industries, among others. We operate at 150 locations throughout the United States and Canada, employing 2,500 persons. In New Jersey, our business is conducted not only at our home office in Basking Ridge, but also in several other New Jersey cities. Our payrolls are approximately $2,000,000, paid to our 200 employees. We are the second largest company of our type in the United States.

We respectfully oppose the passage of S.3178. Federal legislation is the fairest way of regulating data systems as it provides a standardized compliance system for the data gathering industry. The Federal Privacy Act of 1974, which regulates U. S. governmental data gathering, created a commission which is to recommend what additional regulation of the private sector is necessary.

We submit that this commission is in the best position to evaluate the effect legislation will have on American industry. It will also be able to ascertain which data systems are already regulated by existing legislation. We believe that Senate Bill S.3178 is premature and unnecessarily duplicative of existing Federal statutes. For example, our present data system which includes consumer reports, is regulated by the Fair Credit Reporting Act. Much of this Bill, particularly Sections 6 and 7, duplicates the FCRA.

That Act which is conscientiously administered by the Federal Trade Commission, has proved to be efficient in regulating the consumer reporting industry including data gathering and disclosure. That industry opened its files to consumers in May of 1971 when the Act was passed and they have remained open.

Inadequate consideration has been given to the impact of S.3178 on the business community. Every business which keeps records of its accounts will be compelled to comply with Section 3 (c) requiring consent to use the information, Section 3 (g) requiring hearings and Section 11 requiring consent prior to dissemination. Every business will be compelled to comply with Section 3 (g) even if it does not disseminate the information. The cost of these procedures, which is excessive, will be passed on to the consumers by benefit grantors.

Such provisions should be reviewed in light of existing legislation to discover whether they create a cost without creating a justifying safeguard. Consumer reporting industry files are closely regulated by the FCRA. That Act gives the consumer the right to review his or her file, correct it, have information deleted, submit an explanatory or disputing statement, sue, recover compensatory and punitive damages and attorney's fees. Also, the FTC has the power to investigate complaints and to take appropriate administrative action. Experience shows that these remedies have amply protected the consumer while permitting the banking, insurance, credit card and many other industries to receive a free flow of information on which to make decisions. S.3178 threatens the viability of a number of businesses and, at least, creates the possibility of inflated costs for virtually all goods and services in the state because the bill would make the cost of business information inordinate.

The overbreadth of the bill is demonstrated by Sections 2 and 3. Section 2 (c) defines "data system" in terms of an "agency" as that term is defined in Section 2 (a). However, Section 3 (a) suggests that the term "data system" was meant to apply to "organizations" as well, as that term is defined in Section 2 (i). If that is the case, there are few businesses which keep records which are not includable in Sections 2 (c) and 2 (j) which defines the term "personal information". Please note that Section 2 (c) includes both

automated and manual systems. We respectfully submit that, even if that Section referred only to automated systems, the result of the passage of S.3178 will be extensive overkill. There is no business in this or any other state which does not keep payment records, many of which are now kept in automated files. Such records fall within Section 2 (j) and would be regulated by this Bill.

Section 10 seems to state that benefits may not be conditioned on the receipt of information covered by this Act. If that is the intent of the Section, the cost to consumers will be significant. People who have unfavorable credit records, for example, will probably not consent to their release to a credit grantor as provided in Section 11 (a). If that credit grantor is unable to refuse to confer a benefit on the basis of the consumer's refusal to release the record, the credit grantor will be compelled to create a fiction to reject the consumer or, more likely, to pass the increased cost of uncollected obligations on to consumers who do pay their obligations or to restrict the class to whom credit will be granted.

Section 11 (a) creates a costly compliance problem without creating a meaningful right for the consumer. No organization which orders reports prior to conferring benefits will approve an application without a report. The less onerous, more workable solution to the problem of protecting the

consumer while insuring the free flow of crucial business information is already provided by the Fair Credit Reporting Act. That Act insures that any applicant who is unable to qualify for a benefit because of the contents of a report must be told so and that the reporting company must disclose the contents of the file. Upon disclosure, the entire range of remedies, some of which were previously mentioned, are available. Experience has shown that these are ample, meaningful safeguards to the consumer.

Therefore, we respectfully urge you to reject S.3178 - at least in its present form. Far more study of the impact of such legislation on consumers and the business community is required. The Commission created by the Privacy Act of 1974 is in the best position to accumulate the data necessary to write effective legislation in this area.

We cordially invite all of you and your staffs to visit our facility in Basking Ridge so that we can provide you with more detailed information concerning our business. We would be glad to furnish you with additional information about our industry that you might require in considering S.3178.

SENATOR FELDMAN: Mr. North, I agree that the wording in parts of the bill is not as explicit as it should be, and it is not my intention as the sponsor of this bill to have one use this as a crutch or a shield when there is something in his background that should be known. So that is not the intent of the bill, and that certainly will be clarified.

Do you feel that the Federal law really embraces all facets of life that people should have protection on?

MR. NORTH: I feel strongly that the initial

application of the Fair Credit Reporting Act has provided consumers generally with the safeguards they require. It has taken both the consumer and the consumer reporting industry a few years to digest the administration of this legislation. In fact, I was quite disturbed this morning to have you mention that the Chairman of the FTC feels that there are severe abuses in the disclosure of information. This has not been our particular case. We have handled our disclosures, as the consumers requested them, in a forthright manner. In fact, we have gone beyond the law and actually permitted consumers to view the contents of our files as they pertain to them.

SENATOR FELDMAN: Of course, Mr. Engman was not talking about your company. He made a generalization about the status in the nation today, and he says, and I am quoting him, "there is often wholesale withholding of information concerning the character, reputation, or the morals of people." I want to know what's in there about me, and I just can't get an answer.

MR. NORTH: We feel that you are entitled to that, and the law covers it very well in that, if you are denied insurance, credit or employment because of information which a consumer reporting company such as ours has furnished to the potential insurance underwriter, credit granter, or employer, they must so inform you. At the same time they will inform you as to the name of the agency that provided the information and their address and telephone number in most instances. At that point, you have a responsibility to correct your record if it's wrong too. You may make an appointment and actually review your record with that consumer reporting agency. In many instances the consumer does find that the information is correct, but they just want to make certain that someone really made that information known. But, if on the other hand you feel that there is an error, we, or anyone in the consumer reporting industry, will reinvestigate the particular case, and then have a further disclosure.

If a correction is in order, not only will you be

notified but any persons to whom that information has been submitted will be notified. If, on the other hand, there is an unresolved dispute, your statement will be inserted into that file, and it will be incorporated with any information concerning you which is forwarded to a credit granter or an insurance underwriter, and so forth.

SENATOR FELDMAN: Let's say I am the holder of a credit card. Now, would you have in your files on Matt Feldman the restaurants that I patronize, what I might buy on a shopping spree with Mrs. Feldman, or what I might buy when we are on vacation on one of the islands, or the books I read, or the shows that I see? Would you have that kind of information?

MR. NORTH: No. And I don't believe--- To the best of my knowledge, there isn't a computer base or data base in this country that can maintain such records. The purpose of consumer reports in a computerized manner is for the approval primarily for credit; therefore, it would have only positive or negative credit experiences as they pertain to you. For instance, if you hold a major credit card and you pay your bills promptly, most credit bureaus would record that your average balance runs to "X" amount and that you pay promptly. If, on the other hand, you have a negative credit experience, in that you just didn't pay some bills, and they were turned over for collection, or that you consistently run at a very slow rate, that would also be indicated in the file. But that information would pertain to you as an individual, and would include only those credit experiences of those companies using that system. There is no file which is totally complete as to all credit cards and all banking institutions and so forth.

SENATOR FELDMAN: If you wanted that information, and you reporesented a firm that is not as ethical or high standing or as moralistically inclined as your company, could you get that information?

MR. NORTH: As an individual?

SENATOR FELDMAN: Yes.

MR. NORTH: No, sir, you couldn't. It would be necessary that you be a bona fide client, demonstrating a business purpose for your inquiry. In other words, reputable consumer reporting firms will not deal with individuals. They will deal with organizations.

SENATOR FELDMAN: If I started a data processing business, and I wanted to get data on my fellow legislators, where they went, who they talked with, what movies they went to see, could I get that?

MR. NORTH: I'm sorry, you wouldn't get it from our company.

SENATOR FELDMAN: Not from you. I'm asking you, would I be able to get that information?

MR. NORTH: Well, as a matter of fact, you couldn't get that under the law, because the FCRA indicates that you must have a demonstrated need for the information - in other words, there must be a business purpose for it - and you must sign a certification form indicating that it will be used for that purpose, and then penalties would apply should you not use it for that purpose.

SENATOR FELDMAN: All right, thank you very much.

MR. SOKOL: First of all, you may not have been here at the time, but just to reiterate for those who have just attended the afternoon session, Section 3-G is going to amended.

MR. NORTH: I realize that.

MR. SOKOL: Secondly, how do you get the data that is in your system now?

MR. NORTH: Well, if you are talking about the normal consumer reporting, it is contributed by users of the service. Are you talking about our computerized data base?

MR. SOKOL: Yes.

MR. NORTH: Yes, it would be contributed by the users of the service, the major credit card companies, the petroleum

card companies, department stores, other credit granters, and it acts, in effect, as an interchange.

MR. SOKOL: How do they get their information that they provide for you?

MR. NORTH: If someone has applied for an account, then they will run the inquiry through the file to determine if there is a prior credit history.

MR. SOKOL: To your knowledge, do any of these people ever take such application orally, or is it always done in writing?

MR. NORTH: I could not say for a fact, but I assume ---

MR. SOKOL: According to your experience.

MR. NORTH: In my experience, it has always been done in writing. You would have to sign a signature card.

MR. SOKOL: At the time that application is made, which is the initial point of entry of data to this system, couldn't the consent be given at that time and meet the requirements of this act?

MR. NORTH: If it were properly structured, yes. But that is the consent for us to divulge the contents of our file information ---

MR SOKOL: To use and disseminate.

MR. NORTH: To use for that particular purpose, right.

MR. SOKOL: If that was the case, obtaining consent in that manner, do you see that as imposing an unnecessary or undue hardship on you or the industry?

MR. NORTH: Not that particular individual facet, no, because I believe it is done in many instances at the moment. It is done for purposes of the FCRA in insurance. It is done in many facets, because it is required.

The Fair Credit Reporting Act requires what we call pre-notification. In other words, if a report is going to be required on you because you applied for a benefit, you are required to be pre-notified if it is an investigative consumer

report. That is done through a notice provision made as part of the credit application or insurance application, and it falls within the auspices

MR. SOKOL: Under the FCRA, you noted it provides for civil liability in case of a willful and knowing violation.

MR. NORTH: Yes, sir.

MR. SOKOL: If the consumer who has been injured in some way because of lack of compliance with the Federal law, the Federal Credit Reporting Act, chooses not to engage an attorney to pursue his civil remedy, what are his alternatives in order to get ---

MR. NORTH: In order to receive compensatory damages he is going to have to engage an attorney and go through a civil process. However, he has other remedies through the FTC on an administrative basis.

MR. SOKOL: He would have to apply to the FTC in Washington?

MR. NORTH: No, he has to make a complaint at the local regional office of the Federal Trade Commission and they will be in looking in our window to determine whether we are complying with the Fair Credit Reporting Act. But his remedy for civil liability is through the courts.

MR. SOKOL: Thank you.

SENATOR FELDMAN: Thank you very much. I will now call upon Mr. Armstrong.

P A U L L. A R M S T R O N G: My name is Paul Armstrong. I'm Regional Manager for State Government Affairs for TRW Incorporated. TRW Incorporated is a large organization with manufacturing and service facilities, some of which are in the State of New Jersey.

Because the consumer credit reporting agencies have been brought under this act over the past four years, I am addressing my remarks specifically to that, because there is a degree of precedence in the experience and the background as that act applies.

TRW Credit Data, a division of TRW Incorporated, shares with you the concern which has moved you to introduce legislation on the rights of privacy. However, we submit that the all encompassing regulations advocated in the proposed legislation would, if enacted, prove detrimental if not destructive, to the credit industry, without meaningful benefit to individuals in search of credit.

We acknowledge that a careful balance must be maintained between the "right to know" and the "right to privacy". A first and successful substantive effort was made in this area with the passage of the Fair Credit Reporting Act (Public Law 91-508) in 1970, effective April, 1971.

In addition to the Fair Credit Reporting Act, both Federal and State Governments have reviewed and enacted legislation directed at specific abuses by private industry. Examples of such legislation are:

The Equal Credit Opportunity Acts

The Unsolicited Credit Card Acts

The Fair Credit Billing Acts

Legislative Proposals on Fair Collection Practices

In our view, it would be impractical and unreasonable to submit private industry to further regulation without at least prime facie evidence that abuses exist.

TRW fully accepts and supports the concept of full responsibility and integrity for business in the collection and maintenance of personal information records.

However, in S 3178, we are greatly concerned by the inclusion in a bill obviously structured toward regulating the record-keeping practices of governmental agencies, by regulating the disparate and totally unknown numbers and types of personal information files maintained by businesses in New Jersey in conjunction with their legitimate operational or administrative needs.

The Federal Government has established a Privacy Study Commission to research the record-keeping practices of the private sector, rather then attempt to include private records in a statute regulating government agency data systems. This would appear to be a far more practical procedure then the inclusion of the private sector in S 3178.

It would seem impractical to subject the private economy of the State of New Jersey to the probable enormous, additional, administrative costs inherent in complying with requirements set forth in this proposed act.

An overview of the broad scoped requirements of the bill would indicate in addition to the financial costs, that compliance will certainly place New Jersey businesses in a competitive disadvantage with those located in other states; would tend to discourage the establishment of new businesses or the expansion of existing ones within the state and will vastly complicate present, legitimate and ethical business practices for the professions, retailers, manufacturers and service businesses.

The proposal of legislation which would control the collection and maintenance of personal data information by the business community without first having established indications that abuses exist or having defined specific areas in which abuses might occur can only serve to affect the business recovery and impact directly individual taxpayers.

TRW in commenting on the bill directs specific objections to the impact of this bill on consumer credit reporting, which is by comparison a very small industry, but is one which has been operating since 1971 under a statute, the Fair Credit Reporting Act, which has been termed the First Privacy Law. This law which fully endorses the concept of the free flow of vital credit information has impacted the industry, but has worked well. The conditions of S 3178 would place additional requirements that would severely restrict this free flow of information.

TRW specifically objects to requirements which would preclude collecting or transferring individually identifiable data to another system without obtaining the prior informed consent of an individual. These provisions would impede, if not eliminate, the free flow and exchange of credit information which is vital to our credit economy. Literally enforced, such provisions would require credit grantors to obtain an individual's consent prior to reporting account data to a reporting agency. Additionally, a reporting agency would be required to obtain consent prior to starting a file or making its file data available to an inquiring credit grantor.

Compliance with these provisions would be particularly onerous in an operation which generates any significant number of reports per day. It would be totally impractical in that credit grantors would no longer be able to request or receive credit reporting information by telephone or by remote teleprinter. These restrictions would definitely affect the time required to make credit decisions for consumers and result in astronomical increases in operating costs of credit grantors and reporting agencies in that reporting information exchanged in this manner currently represents (70%) or more of the total credit inquiries processed. Such increases in costs would serve no direct benefit to

the consumer as (90%) or more now obtain the benefits they seek with no problem and the existing Fair Credit Reporting Act provides adequate recourse to those consumers who do encounter problems. It should also be mentioned that compliance with the original Fair Credit Reporting Act came at no small expense to credit reporting agencies. Most incurred in excess of a (10%) increase in operating costs (in most cases more than their net profits), most of which had to be passed through to the users of such reports.

Congress recognized the need for free interchange of information in the consumer credit industry when they drafted the Fair Credit Reporting Act. They also recognized the fact that substantial increases in costs involved in changing long-established legitimate business practices would inevitably be passed on to all consumers.

Even more serious is the implication of the unfair and unjustified restraint imposed upon the individual seeking credit. The strictures placed on the credit application and granting process may impinge on the availability of credit for the "emergency" situation or the opportunity of an individual to purchase goods on a "temporary line" of credit, i.e., replacement of hot water heater, furnace, freezers, refrigerators, etcetera, where time could be a critical factor.

In addition, "personal data" is too broadly defined to be feasibly applied to a personal data system under the language of the proposed legislation, and would serve to hinder the further development of internal record-keeping systems currently maintained by the private sector for the direct benefit of individuals, i.e., payroll, billings, stockholders, employee benefit programs, etcetera.

Those who are genuinely concerned with the issue of the protection of personal privacy have three basic objectives, namely, that information be confidential, accurate, and current.

It is our firm belief that the Fair Credit Reporting Act has identified and met these objectives. We submit that the all-encompassing regulation advocated in the proposed legislation disregards the ethical responsibility of the industry and, if enacted, would result in crippling the credit system which has developed over the years to the advantage of the consumer, business, and the economy of this state.

SENATOR FELDMAN: Mr. Armstrong, do you really believe in the home rule concept? Too many of us cry out against Washington, against the bureaucracy: Big Daddy is doing everything for us; we ought to do it ourselves, home rule, New Jersey, municipalities.

Do you really feel that if New Jersey comes up with a bill that makes up for what is remiss in the national legislation -- by their own admission there are avenues that could be affected in the national bill -- do you think it would have a crippling effect on industry in New Jersey? I get concerned when I hear that, because I don't want to be part of the declining of New Jersey industrial goals and New Jersey industrial plans which could result in unemployment. I get bothered when I hear this, because I accept this seriously as I know you are presenting it here seriously.

I am concerned. I wonder, has it hurt Minnesota or New Hampshire or Utah? They have similar bills. They are weaker bills, but similar bills. Does it hurt the economic roots of these states?

MR. ARMSTRONG: I think it is too soon, Senator, to know. I know that the Minnesota bill, having become law last year, was very widely amended with many sections being eliminated. Apparently the first thing they ran into was the fact that the requirements of the act - which of course regulated state agencies - violated certain statutory requirements on these agencies as to confidentiality of information. Again, this is all third-hand information.

I can say this: I understand they set aside or were to appropriate $2 million to implement the bill which became law last year, a good part of which was to support a commission similar to that which is defined in this act. Under the amended bill which is now the law in Minnesota, they appropriated $25,000 for a study commission without the regulatory aspects.

SENATOR FELDMAN: That's for the public sector, not the private sector.

MR. ARMSTRONG: The private sector, Senator, was not involved in that bill to my knowledge, but essentially I think what we have to consider here is that this is an issue. It is an important issue. It is going to be an issue for years to come. We cannot remove that fact, unless it is assessed.

For example, the Fair Credit Reporting Act, in two years of study, defined the usage, content, and procedures of a credit file, or a consumer credit file in the case of credit data, which does not do investigative reports. They created the disclosure procedures which are quite similar to those contained in this bill, and they have worked, but they have worked at a great expense to the credit bureaus. We don't make an issue of this. This is a fact.

However, to make a point, they did not at the same time require the control legislation, and so on, of the billing procedures, the accounting personnel, and all the other records which are needed to operate those particular agencies.

SENATOR FELDMAN: Perhaps I can rephrase my fears, because the states that I have mentioned were concerned with the public sector and not the private sector.

MR. ARMSTRONG: Correct.

SENATOR FELDMAN: If I were a businessman in Minnesota, New Hampshire, or Utah, would I flee the State? This is the next step. They started in the public sector, and now they are moving into the private sector. To your knowledge, has there been one industry in any of these states - I think Minnesota may be more closely akin to us than the others because it has industry and it has farms ---

MR. ARMSTRONG: Well, since they do not actually attend to any requirement of the private sector in their present form--- First of all, I would have no idea, even if they did, that

there was a sudden decampment of business or individuals from the state. In talking to an individual that I occasionally see in Washington who is quite familiar with this particular act out in Minnesota, I was told a few months ago that it had created a great deal of confusion, for example, on the availability of educational records on the part of individual students, and some of the parents were up in arms because of this.

Essentially, Senator, I think what I am saying here is that to create for each individual data system as identifiable under the act - which is extremely broad-based - is going to create a dollar cost, not the least of which will be the cost of disclosure, as has been the fact with the credit reporting agencies.

You cannot, for example, simply hand someone a file or tell them about the file and assume that is the end of it. The credit reporting industry on a national level - and I'm talking about consumer credit reporting as opposed to the total industry which includes investigative reporting - has processed, as I understand it, some 10 million requests for disclosure at a cost of upward of $50 million over the past four years. This represents only one and a half percent to two percent of the reporting volume of the industry.

Now, I do not think that this will be true of every industry or every agency, but there is a definite dollar cost value in a privacy act or the Fair Credit Reporting Act, first of all, to avoid violations of the individual's privacy inadvertently. You cannot do it with existing staff.

I know in the reporting industry in order to establish a decent response to requests for these disclosures, every reporting agency had to hire additional staff - 10 or in some cases 20 percent of their total staff - from which no income derived but was the cost of doing business in order to properly handle disclosure requirments.

At TRW, because we are a computerized bureau, for example, we have found it simpler to identify the individual by asking him to authorize in writing the disclosure of his files, and generating off the computer a complete, in English, record of that file which we send to him after we have received the initial signed request.

This would not be possible for the smaller agencies or manual agencies. Nevertheless, we find that we are making sometimes as many as five disclosures of one initial request. We send them the file, and we ask them to return a copy of this in duplicate, marking any item which he feels is not either accurate or current. We then reinvestigate. We send him the contents of his records after it has been corrected. If he still has a question on any item, he may come back again; or, if he is again declined credit, even though we have made a total disclosure and an update on the basis of his own question, we will have still another disclosure procedure set up with the same individual.

SENATOR FELDMAN: You are one of two thousand credit bureaus?

MR. ARMSTRONG: That is correct.

SENATOR FELDMAN: Now, if 1,998 - and I include you, Mr. Armstrong - were like that, there would be no need for the bill.

MR. ARMSTRONG: Well, there is a bad misunderstanding of the function of the consumer credit reporting agencies. A consumer credit reporting agency is simply a vessel into which the credit granters deposit their credit records. They are merged together, and on request are then sent to the agency as they have an application on the individual. There is no judgemental process involved where we take part in any shape or form with the evaluation of the credit application. We are simply supplying information. We have a definite responsibility to have both accurate information and also have a facility which will give it as needed.

SENATOR FELDMAN: What I am impressed with is that your company supplies the information and will respond to an inquiry and make corrections.

MR. ARMSTRONG: I think you will find that with most of the industry.

SENATOR FELDMAN: Well, not according to reports we have received and the statements that have been made by the Congressional Investigative Commission.

MR. ARMSTRONG: Well, if I may add something to that, while all credit agencies are under the general title of consumer agencies, you have the investigative agencies which are doing a very vital job for the insurance perspective employees, where they must get some information concerning character and so on. Consumer reporting agencies are something entirely different. We store the information. Most of the information is secured verbally or by terminals which may be located in a bank or a store directly or from the data base itself under a cross-fixed technical procedure.

We do not have information as to the sort of thing you were talking about, where did you go, what did you do. It is simply a matter of transactional information reported by the various credit granters that use the service. As a condition of using the service they must make their information available. It would include, aside from that, public records such as suits and judgements, tax liens, and bankruptcies, all of which are supplied to the individual on request.

SENATOR FELDMAN: Thank you very much. Naomi Seligman.

N A O M I S E L I G M A N: Good afternoon and thank you for inviting me to testify. I was asked to describe what the function of our firm was before I begin, and I would like to do so.

We are a research firm who specializes in computer technology. Our work is conducted on behalf of a group of very large industrial companies, many of whom - and I think all of whom - do business in New Jersey. This does not include any company

whose primary business is the sale or transfer of credit data. I think that makes a difference. It does include much of major American industry, oil companies, steel companies and so forth.

I have a prepared statement which I have submitted to you. First I want to make clear that we agree that there is a need for the legal protection of the right to privacy for all citizens, including ourselves as individuals; and we do concur with the five basic principles enunciated in the HEW report. You have heard a number of these mentioned today, but I think with certain modifications your bill could protect these five principles. Let me go over the five principles.

"First, there must be no personal data record-keeping system whose very existence is secret.

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

Now, most major companies today will let, for example, their employees see their records.

"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.

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

"Any 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 the data."

These are the five basic principles contained in that HEW report.

For the most part, Senate Bill Number 3178 promotes these principles, and we agree with its intent. In several instances, however, the language fails to distinguish between the nature and purposes of personal data systems employed by government agencies, business generally, and third party data services. We feel that this failure to distinguish among the sectors may compromise the effectiveness of the bill and cause unnecessary disruption to New Jersey industry conducting routine, traditional, and totally legitimate activities.

Most personal data systems employed in business consist primarily of data taken voluntarily from an individual on the basis of his informal contractual relationship with the corporation, or accounting transactions which maintain the organization's financial relationship with the individual. These accounting/personal transactions may include payroll, stockholder dividend accounting, accounts payable, or accounts receivable. These records typically do not include data acquired from sources outside an organization; quite the contrary, they constitute a valuable asset which business guards as closely as other proprietary information on sales or costs.

We maintain that S.B. 3178 should recognize the difference between these internal, essentially accounting type systems, and the automated dossiers maintained by government agencies and by third party data services, such as credit bureaus. Not only is the need for regulation far less clear in terms of routine business practices, but the problems associated with certain aspects of compliance are considerably more onerous. While a government agency may gather data from a single questionnaire, an accounting-type personal system may reflect totals from hundreds of data records reporting hours worked, purchases, sales, and the like. The data may be routinely

handled on an account-by-account basis by many different company officers and clerks, without violating the legitimate right to privacy of the individual. In sum, there are substantial differences between routine business systems and those maintained by government agencies or third party data services.

We believe, further, that the business community will be able to meet the letter and spirit of the law if that law recognizes these distinctions in five specific areas.

1. The law should exempt all routine and otherwise legal uses, accesses, disclosures and transfers of personal data by and to those officers and employees of the organization which maintain the record and who have a need for the record in the performance of their duties.

2. The law should not require a record of each routine and recurrent accounting type input to the file so long as that input is processed entirely with the organization maintaining the file.

3. The law should totally exempt small, manual employee files maintained informally by department or section managers for their own personal use. These are not part of the organization's evaluative process and, in fact, the organization will very likely be unaware of their existence. Further, the registration reports required for such systems would impose an immense and unnecessary reporting burden on both the organization and the state.

4. The law should permit an organization reasonable time to respond to a request for access of a record, within the limits of technology and the existing clerical staff.

5. Although this point is less critical in the case of Senate Bill 3178, public notice should probably not be required of systems and records more often than there is a new use of personal data outside the routine or internal processes of an organization. Further, if such an external use already exists, notification should be required only if new categories of persons are included or if there has been a qualitative change concerning the personal information content of the record.

PROPOSED CHANGES IN LANGUAGE

Page 1, Section 2(c), Line 10:

...or disseminated by an agency on more than 1000 individuals;

Page 2, Section 2(i), Line 31:

...located within this State or which maintains a data system on any citizen of New Jersey;

Page 2, Section 2, Insert following Line 40:

"Routine internal use" includes the collection of accounting transactions from within the organization, the processing of data by the organization or its administrative agents and the access of data by those officers and employees of the organization which maintains the data, who have a need for the record in the performance of their duties.

Page 2, Section 3(c), Line 13:

...unless authorized by law or excluded under Section 12 of this Bill, or when defined as routine internal use.

Page 3, Section 3(g), Line 31:

Each agency shall hold public hearings...

Page 3, Section 4(b), Line 5:

...act becomes effective and whenever required by Section 3(f),

Page 5, Section 5(e), Line 23:

Establish appropriate and generally feasible administrative,..

Page 5, Section 6(f), Line 23:

...uses and disclosures made routinely or...

Page 5, Section 6(f), Line 24:

...or excluded by Section 12.

Page 6, Section 7(c), Line 9:

Accept and include in, or relate to, the record...

Page 6, Section 7(e), Line 17:

...inform past recipients of that information within the past year of its elimination or correction.

Page 7, Section 12(a), Line 3:

...officers, agents, and employees...

Page 8, Section 15(d), Line 13:

...for employment or promotion with an agency...

Page 8, Section 16(a), Line 1:

Any agency or organization that willfully...

SENATOR FELDMAN: Ms. Sligman, you have given us invaluable assistance, and I want to thank you very much.

MS. SELIGMAN: Thank you. I would be happy to provide anything else.

SENATOR FELDMAN: Mr. Collins.

J A M E S F. C O L L I N S, JR: Senator Feldman, I am very happy to be here this afternoon and have the opportunity to share with you and your associates and your hard-working staff some observations of mine, representing the observations of the company I am with, Johnson & Johnson.

I am James F. Collins, Jr., Director of the Management Services Division of Johnson & Johnson. I am a professional in the field of computer systems and have responsibility for such activities throughout the company.

Johnson & Johnson has 22 major locations in New Jersey employing approximately 11,500 people.

As a matter of principle, our company agrees that there is a clear need for the legal protection of the right to privacy of all citizens, including ourselves as individuals.

Some historical background on the right to privacy issue may be helpful.

In 1972, the Federal Department of Health, Education and Welfare initiated a study to examine the right of privacy issues. A comprehensive report on this was issued in July, 1973, sometimes called the Ware Committee Report, and entitled Records, Computers, and the Rights of Citizens. This report contained many recommendations, as well as principles to be used as guidelines for protecting individual privacy. These recommendations

were presented as goals, however, and not as a statement of present technological feasibility. Subsequent to the Ware Committee Report, the Domestic Council Committee on the Right of Privacy, recommended that protection of the right of privacy should start in the Federal government and that Federal example and experience in this complex field should precede study and legislation covering the non-Federal governmental and private sectors. The United States Congress in enacting the Privacy Act of 1974, reached the same conclusion by specifically omitting state and local governments as well as the private sector from coverage. However, the 1974 Act did direct a Privacy Protection Study Commission to assess the need for regulation of those sectors. This was done as a very positive step partly because the potential for invasion of privacy and the range of people covered was much greater at the Federal level, partly because the subject was so complex, and partly from a recognition that the impact on business and state and local government could be substantial.

Recognizing that the cost-effectiveness and the ultimate impact of the Federal Privacy Act of 1974 on Federal agencies has yet to be determined, I wish to emphasize that Johnson & Johnson strongly supports the principles of personal privacy. However, the subject matter, as complex as it is when applied to the Federal governmental sector, is infinitely more complex when applied to the other levels of government and the

private sector. A measure of the complexity and difficulty in this problem is suggested by the definition of the term "personal information" contained in Senate Bill #3178. This term "means any information that identifies or describes any characteristics of an individual." This encompasses virtually any or all transactions involving individuals. Such personal information, and the dissemination of it, should and must be protected from unauthorized use. However, the very scope and magnitude of such a protective policy as applied to such an enormous amount of information is not a simple one to define.

Therefore, I would respectfully propose that Senator Feldman and the other sponsors of the bill consider the creation of a study commission composed of legislators, members of the executive branches of state, county and local government, and representatives from industry to carefully analyze the subject of data privacy as it affects all levels of government and the private sector of New Jersey, to include the following questions:

1. Are there abuses in the collection of and dissemination of personal information on citizens by government agencies and organizations of the private sector located in the State of New Jersey?
2. Do these abuses differ within the public sector and the private sector?
3. If there are abuses in either sector, should the State of New Jersey be involved in the prevention of such abuses and in what manner?

4. If state government regulation is deemed appropriate, what exemptions and exclusions are appropriate for what types of governmental and business activities with respect to personal information and other data on citizens?

These questions are only by way of example and are not intended to limit the scope of this study.

Any regulation should exempt the routine internal use of all data including personal information, gathered for and disclosed to those authorized employees of an organization who either maintain such data and personal information or who have a need for it in the performance of their duties.

It is my belief that such a study commission if properly constituted and staffed will be able to effectively evaluate and use the work of the Federal Privacy Protection Study Commission and the Federal Domestic Council Committee on the Right of Privacy, the work of the Congressional Committees presently considering proposed Federal privacy legislation which would cover the private sector, as well as proposed amendments to the Federal Privacy Act of 1974, and use its own special expertise to insure that the rights of the private citizen, in his rightful quest for privacy, are appropriately and efficiently protected.

SENATOR FELDMAN: Thank you. We had a quasi-study commission. It wasn't an official one, but it was headed by Dr. Alan Westin. I am sure you are aware of Dr. Westin. He was quoted earlier today as one of the leading proponents of legislation affecting the protection of privacy or the strengthening of privacy. We looked into the other states that had intended legislation or had legislation on the books such as Arkansas, New Hampshire, Minnesota and Utah, as well as the Federal group, so we did make an exhaustive study.

However, I am very pleased to know that you, representing one of New Jersey's foremost industries, that is nation known, do favor the protection of the privacy of American citizens. I want to thank you very much. We do want to thank you for your time and your comments and for your moral support.

MR. COLLINS: I am very happy to have had the opportunity to pass our views along, and we would be most happy at any time to offer any cooperation or assistance possible in the study and development of legislation so that it would have maximum effectiveness but minimum adverse impact and minimizing the costs and the redundant costs. Thank you.

SENATOR FELDMAN: I recognize Mr. Venta. Is Mr. Venta here?

MR. VENTA: Senator, I appreciate the offer. This is my first experience speaking before a committee such as this, and I can see that I am not as well prepared as I might be. I would like to decline at this time.

SENATOR FELDMAN: If you want to send in a written statement, Mr. Venta, that would be appreciated.

MR. VENTA: I would like to thank you for the offer. This has been an experience, and I do want to thank you. I think it is better that I decline and act as an observer.

MR. SOKOL: Mr. Venta, do I take that to mean, then, that you would like not to include the written statement you

have submitted in the record? There will be a published record of these proceedings.

MR. VENTA: I would like to include my written statement, plus, if I may, send in a short memorandum with regard to a couple of suggestions I have would affect state agencies such as the Real Estate Commission. I think that I might be able to offer a suggestion or two that would be at least worthy of consideration, but I am really not prepared in the manner in which my predecessors obviously have prepared themselves. They have put a great deal of time and effort forth. I thought it was going to be more of an informal nature. I'll just act as an observer and perhaps send a memo to you.

SENATOR FELDMAN: We will keep the record open for at least ten days, in case someone wishes to send in some supplemental testimony. It has to be in within ten days. Is that fair enough?

MR. VENTA: Yes. Very good, thank you. (See pages 28x & 30x)

SENATOR FELDMAN: Is Mr. Adelman here?

J A Y A D E L M A N: Thank you, Senator Feldman. I do not have a written statement. I really just wanted to react, at least to some limited extent, to the bill itself. I think some of the questions that I would have raised have already been answered.

SENATOR FELDMAN: Jay, I know you and many of us know you, but will you please give your full name for the record.

MR ADELMAN: I'm sorry. Jay Adelman, Executive Director of the New Jersey Food Council. The main reason that I am particularly concerned about this legislation on behalf of the food chains of the State is the bearing that it might have on lists that are maintained - in many cases by computers - of shoplifters. In reading through this legislation, it would appear that the supermarket chain would be required to make the presence of that list known to everyone whose name appears on that list, and to give that person the right to challenge the fact that the name appeared.

I don't think that was the intention of the legislation. And based on your statement explaining the legislation, I would not have gotten that impression. However, this is a common practice, and certainly it is true not only of the supermarkets, but I think of many other organizations as well.

We would hope that this type of a listing would be excluded from the provisions of the bill. I am not speaking here about when lists are traded off to other companies. They don't do that. This is maintained strictly by one organization, within that organization, and it would have bearing on any future dealings with customers.

Similarly, lists of this kind may not be kept so much on shoplifters, but those who have been discharged for theft, or some other crime. In some cases there may even be examples of employees who have confessed to something and conceivably no charge will ever have been brought, and the employee is just discharged. Well, that name might well be kept on a permanent record.

Again, we would hope that this bill could be so amended, so that type of list would not be affected. I don't think it was intended to be within the pervue of this legislation. We would hope not, in any case. We think this is totally legitimate in terms of the normal operation of a business.

SENATOR FELDMAN: Mistakes are made in the greatest of corporate giants. But if one is unjustly accused of shoplifting, and his name is maintained on a list such as you are talking about, would that list be disseminated to other companies which are similar to that company?

MR. ADELMAN: No, it isn't.

SENATOR FELDMAN: That is what I wanted to know.

MR. ADELMAN: I am speaking of a list of one organization - and I hate to single out any one company - that has found many people shoplifting over a period of time. Those people may be prosecuted. If they are prosecuted, their names

are maintained in a permanent record, and it is that record that I am alluding to.

SENATOR FELDMAN: I am referring to the other cases where mistakes have been made.

MR. ADELMAN: In other cases, it is quite conceivable that a shoplifter might confess to having shoplifted. He might say, "I did shoplift; I took $100 worth of merchandise," and conceivably the store will not prosecute, or it may begin prosecution and drop it. But they have the record of confession.

SENATOR FELDMAN: How about where there is no record of confession?

MR. ADELMAN: I don't know of any list of that kind. That is not what I am alluding to.

SENATOR FELDMAN: I just wanted to clear that up.

MR. ADELMAN: As a matter of fact, I think they bend over backward not to maintain lists of that kind because that indeed could get into the very right to privacy that this bill covers. Of course, we are in accord with that aspect 100 percent.

I wonder if I might ask this: I came in late this morning, and I gather you did address the question of public hearings.

SENATOR FELDMAN: This is a public hearing.

MR. ADELMAN: No. I'm referring to public hearings that would be required under section 3.g. of the bill.

MR. SOKOL: That only applies to government agencies.

MR. ADELMAN: Would there be such a requirement? We received an inquiry from a large manufacturer.

MR. SOKOL: No.

MR. ADELMAN: But that is not clear as the bill is now written.

MR. SOKOL: Right. There is an error in the bill.

MR. ADELMAN: Okay.

MR. SOKOL: The bill now reads, "Each agency or organization shall hold public hearings as to the purpose and

operation of . . . a new data system . . ." It will include only each agency defined in the law as "a public agency," and organizations defined in the law as "the private sector" will be excluded when the bill is amended.

MR. ADELMAN: Another point I should make - this is a perfect opportunity for it, and I wouldn't want to pass it up---

SENATOR FELDMAN: Are you going to announce some sales? (Laughter)

MR. ADELMAN: Nothing of that kind. Those come on Wednesdays. (Laughter)

There has been a considerable amount of comment about the new automatic check stands that certain supermarkets have begun using and others will soon begin using. These, of course, are all operated on computers. There are many who seem to feel that these computers are going to give the supermarkets an opportunity to maintain lists of shoppers, lists of shopping habits, etc. That is not the intention of these systems, the electronic scanners, and, of course, nothing of the kind will be done. It has not been done by those who are using the scanners, and it will not be done by those who are going to use them. Certainly, then, the right of privacy will in no way come into play here. Thank you for giving me the opportunity to clarify that point.

SENATOR FELDMAN: The list of names that I have read is the official list of those who indicated they wished to testify. Is there anyone else who wishes to comment at this time?

(No response.)

In that case, I want to thank those of you who have been with us today. This is a most important piece of legislation, and you can rest assured that what has been said here will not be taken lightly by me as the sponsor, my staff, or the Judiciary Committee. This is serious business and serious legislation, and it can have a far-reaching effect and impact on our daily routines and activities. What you did say, therefore, will be taken seriously and studied thoroughly, and amendments will be presented.

The hearing is adjourned.

SUBMITTED BY JOHN A. WINTERBOTTOM

Statement by the Educational Testing Service
concerning the Right To Privacy
and Fair Information Practices Act

The Educational Testing Service appreciates this opportunity to present its views on a subject which is of growing importance to the citizens of this state and to numerous organizations that operate within its boundaries. The multiplication of data systems, their increasing potentiality for interaction with one another, and the consequent possibilities for putting data to uses that could not be foreseen by the individuals concerned and that may, in fact, be detrimental to their own best interests--these considerations make it desirable that uniform standards governing the protection of identifiable, personal data be instituted and enforced. We are, therefore, very much in accord with the intent and spirit of the New Jersey Privacy Act. Indeed, we have given a great deal of thought to precisely those issues which are addressed by the Act and, over the past several years, have developed and refined a set of policies and procedures governing the collection and retention of data within our own organization. These are embodied in a policy statement entitled "Policies and Procedural Guidelines for Control of Confidentiality of Data," a copy of which is attached to this paper.

The Educational Testing Service, established in 1947 as a nonprofit educational institution with its main office in Princeton, N. J., engages in three general categories of activity. First, it conducts large-scale testing and data-gathering programs for a variety of purposes--admission to colleges and to graduate and professional schools, the estimation of financial support needed by students to permit continuation of their education, the measurement of academic achievement at the elementary, secondary, and college levels, and

the licensing and certification of individuals for practice in various trades and professions. Second, it carries on a wide-ranging research program seeking answers to a variety of important educational questions. Third, it provides instruction in a number of areas in which its work in measurement and research have given it special competence. The scope of its activities is suggested by the fact that its tests are taken by 3 to 4 million individuals annually, that its research budget for 1974-75 was about 8 million dollars, and that some 800 individuals from this country and from abroad completed instructional courses during the past academic year.

Activities of this character and this magnitude necessitate the generation of extensive files on individuals, many of them citizens of New Jersey. The primary purpose of such files is to provide a record base for the support of a wide variety of services to students and educational institutions. A secondary, but very important, function of the files is to provide a data base for research. We have long recognized the need for maintaining our data files under conditions of strict confidentiality, for permitting students to know what their files contain and to amend them when they are inaccurate, and for providing to students a large measure of control over the circumstances under which their files are released. In 1972, well before the passage of the Federal Education Rights and Privacy Act (Buckley Amendment), the Educational Testing Service had developed a set of internal guidelines, referred to above, which codified and improved its policies and practices regarding the control of student data. These guidelines, in updated form, continue to shape our practices with regard to confidentiality, student access and right to amend, and consent to release.

While we do agree in principle with the Act and feel that, by virtue of the policies and procedures embodied in our guidelines, we are largely in conformity with the requirements of the Act, we would like to offer several observations pertaining both to specific provisions of the Act and to its general implications.

1. Section 4b, p.3 requires that organizations annually "notify the commission and give public notice of the existence and character of each existing system or file." As it applies to data systems, this requirement would create no problem, assuming that the term "data system" refers to the organization's general capability for collecting, storing, and utilizing data. If, however, the term "file" is intended to refer to each set of data stored for a particular purpose, an unreasonable requirement for reporting might result. We have literally hundreds, perhaps thousands of such files, extending all the way from the very extensive files amounting to millions of entries retained in connection with the College Entrance Examination Board programs down to minuscule files containing data on as few as 50 individuals collected for various research projects. It would be a most time-consuming and expensive procedure to report individually on all such files each year.

   A preferable procedure from our point of view would be to require reporting on the organization's data gathering capability as a whole, general descriptions of each of the major operational files, and categorical descriptions of other types of files such as those used for research purposes.

2. Section 12b, p.7 permits disclosure of personal information to a third party without specific consent when the information is to be used as a "statistical research or reporting record, and is to be transferred in a form that is not individually identifiable." We are gratified that the drafters of the legislation have

been sensitive to the need of researchers for data, much of which is retained in files falling within the scope of the legislation. We agree, too, that, whenever possible, the data should be transmitted and used in anonymous form.

We would like to point out, however, that there are some research studies, particularly follow-up studies, in which pieces of data are added to the file over a period of time and in which name may constitute the only available identifier whereby new data can be matched with what is already in the file. Such longitudinal research is important in understanding factors influencing the educational growth of individuals and in developing means by which the educational process can be made more effective. We would like to see a provision whereby, for such studies, data may be transmitted and used in identifiable form, under proper safeguards.

The Buckley Amendment was revised during the stage of public discussion in such a way as to provide for the release of identifiable data without specific consent for research purposes, "if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations [conducting the research] and such information will be destroyed when no longer needed for the purposes for which it is conducted."

We would like to see a policy which a) requires that data transmitted for research purposes be anonymous

if the requirements of the research do not necessitate the use of identifiable data and b) permits the transfer and use of identifiable data when necessary for the research in question, providing the researcher undertakes to limit access to the data to persons required by the nature of the research to have such access and agrees to destroy the identifying data when the research has been completed.

3. There are a number of requirements imposed by the Act which have the potentiality, depending largely on how they are administered, of substantially increasing the cost of doing business for the organizations concerned. Among these are the requirements for public hearings, for notice to the Commission regarding the nature of data systems and files, for notice to the public, for right of access and modification of files, and for appeal to the Commission. Educational institutions have already begun to conform with many of these requirements in the process of complying with the Buckley Amendment, but the New Jersey Act goes significantly beyond Buckley, especially as regards notice. Insofar as additional expense is incurred as a result of such requirements, nonprofit educational organizations such as the Educational Testing Service, various institutions of higher learning, and others, would have no choice but to pass the additional cost on to the students. We hope that, in setting up regulations and procedures governing these requirements, the issue of cost will be kept in mind so that any increase in expense to students can be kept to a minimum.

4. Over the past two years, actual and potential privacy legislation affecting educational institutions has been generated in quantities which may well cause some uneasiness among the administrators of such institutions. The Buckley Amendment has become law; the Federal Privacy Act of 1974, while directly applicable to public agencies, applies by extension to institutions with which those agencies deal; the Koch-Goldwater bill, if enacted, would specifically extend the Privacy Act of 1974 to the private sector; finally, several states, including New Jersey, have passed or are considering the passage of privacy legislation of their own. When institutions are subjected to such a flood of uncoordinated legislative requirements, the possibilities for confusion and inefficiency multiply. In the case of an organization like the Educational Testing Service, which is active in 50 states, the multiplication of divergent privacy and confidentiality requirements among the various states carries with it the potentiality of vastly increasing the difficulty of doing business.

Several alternative courses of action might be suggested, any of which would do much to minimize the difficulties foreseen above. a) The states might leave to the federal government the responsibility for coordinating the production of uniform legislation governing confidentiality and privacy in data systems. The Koch-Goldwater bill promises to fulfill this function and, if appropriately influenced by the states during its formative period, could be made to embody all or most of the features the states would find desirable.

b) If the states choose not to follow that path but wish to create their own legislation, it would be highly desirable if as much coordination and uniformity of requirements could be achieved among them as is possible. Perhaps the council of governors could be utilized for this purpose or perhaps an interstate conference specifically on this issue could be instituted. c) A third possibility would be to encourage discussion within the Education Commission of the States. The Commission is an organization representing 45 states, including New Jersey, which fosters cooperative action on common educational problems. Perhaps it could be persuaded to take a role of leadership in this matter.

5. While the discussion above covers a number of matters on which we felt it appropriate to comment at this time, there are other provisions of the Act that are dealt with in rather general terms and about which we might like to comment at some future time, depending on how they are interpreted in the administration of the Act. We hope that, if need be, there will be opportunity for discussion of such matters with the Commission provided for in the legislation.

In conclusion, we would like to reemphasize that we are in agreement with the broad purposes of the New Jersey Privacy Act as we understand them--namely, to prevent injury to individuals which may result from the misuse of information residing in data systems, to provide the individual with a larger measure of control over data in such systems, and, finally, to make possible the continued use of such data for ends which will benefit both the individual and the public interest. We have

had a good deal of experience in coping with the problems that arise from efforts to achieve these ends within our own organization and would be glad to work with the committee responsible for drafting the legislation or with the proposed Commission on Privacy, Freedom of Information and Public Information in the development of sound legislation in this field.

Educational Testing Service
Princeton, New Jersey

July 16, 1975

Policies and Procedural Guidelines for Control of Confidentiality of Data

Educational Testing Service

October 1974

Policies and Procedural Guidelines for Control of Confidentiality of Data

Definitions

A major goal of ETS is to provide to individuals and to institutions services involving the collection, processing, storage, retrieval, and dissemination of information about individuals and about institutions--information that is potentially useful to individuals in making wise personal decisions and to institutions in making sound judgments in their handling of educational and institutional problems. The information involved in these processes is herein referred to as the ETS data files.

Another major goal of ETS is to conduct research that is intended to increase understanding of such phenomena as human learning and development and that may ultimately result in the development of new or improved techniques and materials for application in such areas as classroom instruction, evaluation of progress toward educational goals, counseling of students, and decision-making by school administrators. The information involved in these activities is herein referred to as the ETS research files.

Confidentiality of Data about Individuals

Policies

1. Individuals shall not be asked to provide information about themselves unless it is potentially useful to those individuals or unless it serves the public interest in improving understanding of educational processes and of human learning and development.

2. ETS affirms the right of individuals to privacy with regard to information about them that may be stored in the ETS data or research files. This right extends both to processed information, such as scores based on test item responses, and the raw data on which the processed information is based.

3. ETS recognizes that information provided by individuals for a designated purpose should be used for another purpose only with the

individual's informed consent, except when the information in question is released in a form that cannot be identified with any individual.

4. ETS encourages the widest possible range of legitimate uses of the information in its data and research files in order to help in solving important personal, educational, and social problems, as long as the right to privacy of individuals is assured.

5. ETS acknowledges its responsibility to safeguard the information in its data and research files.

6. ETS shall continue to strive for the highest attainable level of accuracy in recording, processing, and transmitting information in its data and research files.

7. ETS shall decline to collect or maintain in its data or research files any information that in its judgment cannot be adequately protected from disclosure. At the request of the appropriate governing body of a program, ETS shall remove from its data files any information deemed to be of a confidential nature obtained or stored primarily for purposes of that program that that governing body feels cannot be adequately protected from disclosure.

8. ETS shall continue to work closely with sponsoring organizations for whom ETS acts as agent, in developing and maintaining policies and procedures for the protection of individuals and organizations with regard to confidentiality of information in ETS files.

9. Nothing contained in these policies and procedures shall be construed to prohibit transfer to another organization data collected by ETS on behalf of that organization, provided that that organization has adopted policies and procedures that adequately protect the confidentiality of that data.

Procedural Guidelines

1. Adequate procedural safeguards will be instituted

and monitored, including the following:

a. Information directly identifiable with an individual shall be released from the ETS data or research files only with the informed consent of that individual.

b. Any individual has the right, on payment of a reasonable fee, to request or authorize the disclosure of information from his ETS data file to any recipient he names, providing that such release is not prohibited by other ETS or program policies and does not violate rights to privacy of other individuals; and ETS is obligated to comply with such requests to disclose information.

c. Identification of the requester, through signature, social security number, and ETS data file number, or other appropriate method, shall be made a necessary part of any request for information from the ETS data files. However, in an emergency, when it is clearly to the benefit of the individual, an authorization by telegram or telephone may be acceptable. By prior agreement, authorization by a designated agency or institution may also be acceptable. The individual shall in such instances be informed that the disclosure has taken place, and to whom the information was disclosed, unless there is prior agreement to the contrary.

d. There may be occasions when an individual is deemed not competent to make judgments for himself because of legal minority, illness, or other considerations; in such cases, information about him shall be released from the ETS data files only with the informed consent of the individual's parent, guardian, or spouse.

e. Procedures enabling ETS to produce and maintain a continuous record of all transactions involving the ETS data files, showing all reports of information from the files with dates and identification of requesters and of recipients of information, shall be instituted

as soon as technological developments and economic considerations permit.

f. All ETS programs shall be reviewed periodically to assure conformity with ETS policies and procedures for disclosure of information.

2. Safeguards shall be built into every aspect of the processing systems, to the extent that is appropriate, reasonable, and feasible.

3. ETS shall not participate in any time sharing, network, data bank, or other electronic data processing or storage system involving units outside ETS unless it is satisfied that the confidentiality of data can be adequately safeguarded.

4. Any individual has the right at any time, on payment of a reasonable fee, to receive for his review the information about him in the ETS data files. The individual has the right to correct errors in personal or biographical data and to request verification of test scores or other processed information based on tests, questionnaires, and/or school records.

5. Steps shall be taken to encourage recipients of information from ETS data files to adopt standards regarding anonymity, confidentiality, and privacy that are equivalent to those of ETS.

   a. Symmetry between security procedures employed by ETS and other organizations is desirable.

   b. Attempts will be made to encourage user groups to develop and disseminate their own standards of conduct with regard to privacy.

   c. Suitable forms shall be developed, for such uses as registering candidates and reporting information, such that users of ETS services are fully informed of conditions for release of information and asked to agree to similar conditions in their own release of this information.

   d. ETS may at its discretion refuse to release confidential data from its file to individuals or organizations that have failed

to demonstrate an adequate ability to control further dissemination of information.

6. Procedures shall be developed for systematically eliminating from the ETS data files information that because of the lapse of time is judged to be of minimal value in helping to solve personal, educational, or social problems.

   a. Information of a highly subjective nature might be judged to become obsolete in a shorter time than more objective items of information.

   b. Information about young children might be judged to become obsolete in a shorter period of time than comparable kinds of information about adults.

   c. In the case of data that are of potential value for research or survey purposes, the purging may consist of destroying the link between name and information rather than destroying the information itself.

7. Information from the ETS data files may be used for research purposes without the consent of individuals, provided that the information is treated in such a way that it cannot be identified with an individual by any person, including clerks and computer personnel as well as research investigators.

8. Individuals shall be identified in ETS research files only by code numbers. Information linking the code numbers to names shall be kept in a secure location separate from the data. Names shall be retained only as long as necessary for such purposes as follow-up studies, collating new data, or reporting processed information to subjects, after which the names shall be destroyed.

9. Measures of performance based on unvalidated or experimental situations or tests, whose interpretation is therefore questionable, will not be reported to subjects, or to the institutions providing the subjects, if there is danger that misinterpretation of the information would be harmful to those individuals or institutions. Stipulations regarding non-issuance of such reports should be made and

agreed to by participants, in advance of the data collection.

10. An Advisory Committee on Confidentiality of Data, representing the general public and the users of ETS services (including both individuals and institutions), shall be established to check on ETS procedures and to advise ETS concerning its policies and procedures relevant to privacy, anonymity of individuals, and confidentiality of data.

11. Research investigators must conform to the procedures and requirements of the ETS Committee on Prior Review of Research with regard to control and confidentiality of data.

12. Subsequent to the completion of the data-collection phase of a research project, subjects should not be expected to provide additional data for a follow-up study unless their original informed consent to serve as subjects was based on information that a later request for data would be made, or unless the follow-up study has been approved by the ETS Committee on Prior Review of Research.

13. Requests for information in ETS data or research files, for research purposes, from individuals or agencies outside ETS shall not be granted unless identification of subjects is removed and unless the project has been approved by the Committee on Prior Review of Research of the institution represented by the individual or agency. If the person or agency requesting the data wishes to make a follow-up study requiring a new request to subjects for information, the request should not be granted without explicit approval of the Committee on Prior Review of Research of the institution represented by the individual or agency, and the endorsement of the ETS Committee on Prior Review of Research. If the institution represented by the individual or agency does not have a Committee on Prior Review of Research, then the ETS Committee on Prior Review of Research should evaluate the project.

14. Appropriate steps should be taken where necessary to gain legal support for the policies and procedures here outlined and to make information about specific individuals and institutions immune to subpoena. If release of information is required by court order, a

written protest shall be filed, all pertinent individuals and institutions shall be informed of the circumstances and the nature of the information divulged, and legislative redress should be sought.

Confidentiality of Institutional Data

ETS recognizes an obligation to protect the confidentiality of data about institutions as well as about individuals. However, there are differences in the issues and relationships involved that make it necessary to develop different standards and procedures for institutions than for individuals: (1) In many instances the information about an institution is not supplied by the institution itself but by the individuals (e.g., students or candidates for admission) who are or may be affiliated with the institution. (2) The institutions involved are already in the public arena by virtue of the services they offer, and public knowledge about the institutions generally speaking is desirable for the society. (3) Institutions, unlike individuals, are organizations possessing substantial power and influence, and they are able to protect themselves, if they wish, by bargaining with regard to the conditions for supplying information or assisting in arrangements to obtain data from individuals.

Policies

1. ETS will strive to protect the confidentiality of data supplied by institutions to the extent that such confidentiality does not conflict with the rights and welfare of individuals or of the public's need to be informed.

2. ETS will endeavor to reach agreement with institutions in advance, and on an ad hoc basis, with regard to confidentiality of data supplied to ETS by the institutions.

3. If the data are supplied by individuals rather than by institutions directly, there is less obligation to protect the anonymity of the institutions.

4. In the event that an ETS staff member feels obliged to release information about an institution contrary to prior agreement, or in the absence of an agreement to do so, approval must first be obtained by that staff member from the appropriate ETS advisory committee (the Advisory Committee on Confidentiality of Data or the Committee on Prior Review of Research) before doing so. In the event that ETS collected the information in

the name of a sponsoring organization while acting as its agent, approval of the sponsoring agent would be required as well.

Procedures

Student Registration Forms

For programs involving individual student registration, a statement similar to the following shall appear in the bulletin of information, or whatever publication contains registration forms:

> "The release of your score reports from ETS is governed by an ETS policy that information about an individual contained in ETS files shall be released only with the informed consent of that individual. The transcript request form provided constitutes such a written authorization. Your submission of the registration form indicates your acceptance of these conditions."

The student registration form for individual testing programs shall then contain a statement such as this:

> "In submitting this form, the candidate accepts the condition set forth in the bulletin of information concerning the administration of the tests and the reporting of scores."

Transcript Requests

Transcript requests form a transaction under the initial agreement and shall contain no further reference to the ETS policy. Institutions or individuals receiving scores under the program shall be asked to sign statements such as a below.

Institutional Testing Program Scores

In the case of programs that offer tests ordered by institutions, a statement such as the following shall appear in the program handbook that is sent to faculty or administrators:

> "Scores reported through this testing program are governed by an ETS policy that information about an individual or an institution shall be released only with the informed consent of that individual

or institution. This policy has two immediate implications for institutions participating in this program: (1) Information about the institution gathered through this program will not be released in any form attributed to or identifiable with the institution unless ETS has received written authorization to do so; (2) Information about individuals gathered through this program is released to institutions only after an institutional representative agrees to the following conditions:

"a. The institution will keep such data on a secure basis, and will restrict access to such information about individuals to those who have been authorized by the individual to see the information.

"b. The institution will forward such information about individuals to other institutions or organizations only upon written authorization of the individual.

"It is suggested that, where appropriate, institutions obtain a general written authorization from students to the effect that certain faculty members and others who are directly concerned with the student's education have access to this information. The signature of an institutional representative on the order form for this program constitutes an agreement to the conditions above."

The order form then shall contain this statement:

"We agree to adhere strictly to the procedures outlined in the handbook for: (1) administering the tests, (2) protecting their security, (3) returning all test materials and reports, and (4) insuring the confidentiality of information about individuals.

Implementation

Policies and guidelines such as the above are likely to be ineffective if they are merely printed and distributed to staff members. In order for the guidelines to be effective, an agency is needed that has responsibility and authority to investigate periodically the operations and materials employed by each ETS program from the standpoint of compliance with the guidelines, and for reporting the results of its investigations to the

appropriate administrative officers of ETS.

1. A standing Committee on Confidentiality Guidelines shall be appointed to monitor ETS programs from the standpoint of compliance with the Policies and Procedural Guidelines for Control of Confidentiality of Data.

2. The committee shall have a rotating membership that is broadly representative of the various divisions of ETS, including the program divisions.

3. The committee shall have a working staff that is competent to assist in the development of procedures for monitoring operational practices and to use those procedures in obtaining from each operational program information that will be useful in appraising degree of compliance with the guidelines.

4. Schedules shall be set up for periodic reappraisals of each ongoing program; proposed procedures for new programs should also be appraised as they are developed.

5. Reports shall be prepared by the committee to communicate its findings and recommendations to the appropriate program directors and vice presidents.

6. The committee's duty shall be only to report and recommend; it will be the responsibility of the officers and program directors to initiate any actions based on the appraisals.

7. The committee shall be responsible for reevaluating the policies and procedures from time to time and proposing revisions as deemed appropriate to the officers of ETS.

Educational Testing Service
October 1974

SUBMITTED BY J. JOSEPH FRANKEL

STATEMENT OF THE PRUDENTIAL INSURANCE COMPANY OF AMERICA
BEFORE THE NEW JERSEY SENATE JUDICIARY COMMITTEE - AUGUST 11, 1975
RE: NEW JERSEY SENATE 3178

Mr. Chairman, on behalf of The Prudential Insurance Company of America, I want to thank you and the members of your Committee for the opportunity to testify.

First, I want to compliment Senator Feldman and the co-sponsors of Senate 3178 for concerning themselves with the protection of individual privacy. There is no more important topic. Those of us at Prudential share your concern and are doing as much as we can to protect the rights of each individual.

Mr. Chairman, while supporting the intent of this legislation, there are matters pertaining to this bill which should be brought to the attention of the Committee.

As you know, a great deal of activity has been taking place on both the Federal and state level in the area of Privacy Legislation. On the Federal level, the 1974 Privacy Act created the Privacy Protection Study Commission. In an article in the American Bar Association Journal of July, 1975, the role of the Privacy Protection Study Commission is described as determining whether the 1974 Privacy Act is an effective instrument for safeguarding personal privacy and whether the Congress should look favorably on similar legislation affecting state and local governments and the private sector. Through study and review of a wide range of public and private records systems, as well as analyses of the relationship of these systems to constitutional rights, potential abuses, and standards established under the act, the commission will form conclusions, make general recommendations, and propose changes in laws or regulations.

Mr. Chairman, in light of the report to be made by the commission, I would urge this Committee to recommend that before any action is taken on Senate 3178, the recommendations of the Privacy Study Commission be carefully evaluated.

It is important to remember that many business organizations maintain information on a company or national basis and that a state by state approach to the privacy problem (and there are currently some 85 different bills pending in 35 states on privacy protection) will cause tremendous confusion and expense for business to the detriment of the public. For example, our Company does business in all fifty states. We maintain records dealing with our products in Florida, California, as well as New Jersey. Since we have several large regional offices located in major United States cities, we also maintain many records in these offices. If legislation such as this were to be passed in the various states, it would create severe problems for a company such as ours since compliance criteria could differ from state to state, and the constant reworking of our computer systems to accommodate each state would result in great costs to the company.

I have mentioned costs several times, and in reviewing Senate 3178, there appears to be several sections, namely 3a, 3c, 3f, 3g and 4b, which would be burdensome from a cost standpoint and ultimately produce a greater cost burden on the public.

In summary, we would recommend to the Committee a posture of continued concern with the problem of individual privacy. We would urge the Committee to recommend that a reasonable period of time be taken before enacting legislation in New Jersey so that the recommendations for dealing with this problem on a national level can be evaluated which will inure to the benefit of the general public and industry of the State of New Jersey.

21X

J. Joseph Frankel
Assistant General Counsel

THE HOOPER-HOLMES BUREAU, INC.
170 MT. AIRY ROAD • BASKING RIDGE, N. J. 07920 • (201) 766-5000

JOSHUA A. KALKSTEIN
CORPORATE COUNSEL

August 18, 1975

Hon. Matthew Feldman
790 Grange Road
Teaneck, New Jersey 07666

Re: S.3178

Dear Senator Feldman:

Mr. Dudley S. North, President of Hooper-Holmes, has asked me to thank you for the courtesy with which you and your staff received his testimony regarding the captioned bill on August 11, 1975. He has also asked me to respond to a number of your statements and those of your staff, for the record.

We noted your reluctance to wait for the completion of the work of the Privacy Protection Study Commission created by the Privacy Act of 1974 as well as your reluctance to leave the protection of the privacy area to the Federal Government, in general. We also noted your heavy reliance on the Chairman of the Federal Trade Commission's statement, apparently referring to credit bureaus and consumer reporting agencies, that "We found that there is often wholesale withholding of information concerning character, reputation or morals."

Hooper-Holmes and TRW, two of the largest companies in their respective fields, disputed the accuracy of that statement.

(For the record, Hooper-Holmes is not a credit bureau, but rather a consumer reporting agency as that term is defined in the Fair Credit Reporting Act.) Your response was that perhaps we were in strict compliance with existing laws, but that our remarks did not account for the remaining credit bureaus across the United States.

We respectfully submit that your remarks demonstrate that more background research by your staff is required. Apparently, no one from any area of the business community participated in drafting the bill. We submit that it is demonstrable that Mr. Engman's statement is inaccurate. (You might be interested to know that the Federal Trade Commission will, this year, be called upon to demonstrate the accuracy of that statement in its litigation with the Retail Credit Company.)

We dispute Mr. Engman's statement as it applies to us and the consumer reporting and credit bureau industries. The following illustrates the general situation in credit bureau operations:

> The reporting agencies don't claim that their operations are error-free. They do claim that substantive errors are involved in only a tiny fraction (far less than 1% of the millions of reports they maintain.) An Associated Credit Bureau's survey of its nearly 2,000 member bureaus in 1972 showed that 1,713,000 consumers reviewed their files, most of them because they had been turned down for credit. About 74,000 or 4%, placed statements in their files disputing an entry. Probably no more than about 5% of all consumer reports involve any kind of problem, whether it be a simple miscue (a wrong birth date, for instance), a disputed item (a past due notice on a charge you think should be eliminated because the product broke down) or a completely erroneous entry (such as a nonexistent account on your record). CHANGING TIMES, The Kiplinger Magazine (August 1975) at 44.

The article also states that credit bureaus are advised to show copies of the report to consumers. Hooper-Holmes also follows this practice although it is not required by the FCRA.

In 1974 our Reporting Division made over 2,000,000 reports throughout the United States. It made 1,130 disclosures to consumers and issued 128 corrected reports. Last year we made 22 disclosures in New Jersey and issued 2 corrected reports. Virtually none of the corrections were of a dramatic nature. Our mistakes are minimal because of the sanctions provided in the Fair Credit Reporting Act coupled with our desire to be fair and accurate. We submit that when all the facts are in, you will conclude that our performance is typical of that which can be expected from the other members of our industry.

We do not expect you to shape legislation based either on our testimony or our experience alone. On the other hand, we believe it unreasonable to predicate legislation on Mr. Engman's remarks without testing their validity. For this reason, among others, we aver that your legislation is premature.

This contention is supported by the nature of the questions asked of Mr. North at the hearing by counsel. The Fair Credit Reporting Act is a relatively new and fairly complex statute. It is difficult to deal with unless one has practical experience with it involving either compliance or administration. Accordingly, the committee's counsel could not be expected to have the working knowledge of that law and how it regulates the consumer reporting and credit bureau industries, which is

required to judge its effectiveness. Both the record of the hearings and the text of S.3178 suffer from this lack. Legislation as pervasive in effect as S.3178 would be, should not be reported out of committee without the fullest investigation of all the facts.

We disagree with your contention that the Federal Government has dragged its feet in the privacy area. The appointed commission, we feel, represents a prudent manner by which to gather information and reflect on its effect. The issues addressed by the Commission were virtually unknown ten years ago. The recognition of privacy itself is in a relatively early stage of development as far as the law is concerned. However, if you feel it necessary to proceed without that commission's results, it is advisable, as Mr. Collins of Johnson & Johnson recommended, to create a New Jersey Privacy Commission to develop the facts for our state. Such a committee might contain representatives from the academic, legal, legislative and business communities and others that you deemed appropriate. We believe that our experience with the Fair Credit Reporting Act would be valuable to the work of such a commission and, therefore, offer our services. At the very least, we would like the opportunity to meet with the Majority Counsel and the Legislative Counsel to discuss in detail the operation of the Fair Credit Reporting Act, its sanctions, safeguards and efficacy.

The necessity for further discussion is underlined by your remarks at the conclusion of Mr. North's statement in which you

recognized the validity of our contention that the language of the bill was in some instances inconsistent and did not always accurately express the bill's intent. Additionally, counsel's remarks regarding the study that went into the bill and the fact that the bill was a synthesis of bills and acts considered or enacted in other states indicate that these syntactical and contextual problems were not always apparent to those of your staff who did the actual drafting. Once again, we suggest that these problems at least partially stem from the fact that no information was sought from those in the business community who, like us, live with the Fair Credit Reporting Act on a day to day, practical basis and who find that the Act's sanctions and safeguards are meaningful and effective.

We emphasize that we are the second largest company of our kind in the United States. If our experience shows, which it does, that the Act is effective and that Mr. Engman's remarks do not apply to us, study is required to isolate those entities to which Mr. Engman's remarks do apply and to find out why the Act is ineffective as to them. Our opinion is that Mr. Engman's remarks are inapplicable to our industry in general.

S.3178 has created the opportunity to address many of the complex issues which are raised when personal privacy is discussed. Most entities in and out of the business community recognize the sanctity of the American citizen's right to limit the access of others to information regarding his personal affairs. The basic issues in recognizing and protecting this

right are how to do it effectively and how to define the right where the citizen's entry into the marketplace requires access to information. Those are challenging issues. We respectfully submit that a committee hearing on a bill which requires additional research is an inappropriate forum for dealing with the complexities involved. This is especially true because all of your co-members on the Judiciary Committee were unable to attend.

We believe we can be of assistance in resolving the problems discussed above. We offer you, your counsel, and the Judiciary Committee the benefit of our experience.

Respectfully,

Joshua A. Kalkstein
Corporate Counsel

JAK:eg
Encl.
cc: Congressman Peter W. Rodino, Jr.
Senator Anthony Scardino, Jr.
Senator John M. Skevin
Senator Raymond Garramone
Senator John J. Fay, Jr.
Senator John A. Lynch
Senator Alexander J. Menza
Senator Martin L. Greenberg
Senator James S. Cafiero
Senator Anne C. Martindell
Senator Joseph Hirkala
Senator James P. Dugan
Senator Raymond J. Zane
Senator Joseph A. Maressa
Senator Barry T. Parker
Senator John F. Russo
Senator Stephen B. Wiley
Senator Raymond H. Bateman
Mr. Paul Armstrong
Ms. Gayle Mazuco
The New York Times
Star Ledger
Trentonian
Trenton Times

TRANSCRIPTION

Honorable James P. Dugan - Senator
Honorable Robert C. Shelton, Jr. - Assemblyman

Dear Senator Dugan and Assemblyman Shelton:

I understand public hearings will be held during July on S-3178, A-1188, A-1466, and A-3133, all of which are bills that will affect the public's right to obtain information from governmental agencies. I would like to attend each of the hearings and to reflect my views in my capacity as a State employee as well as my capacity as a citizen of New Jersey. I, therefore, ask that you direct my appearance at the hearings. Should you be unable to direct my appearance as an employee, I will appear of my own volition and on my own time as a citizen. I make this request because I have been denied the right to obtain public information these past four years from such agencies as the New Jersey Real Estate Commission and the Dept. of Civil Service. To make matters worse, the Real Estate Commissioners and Secretary - Director Regan have demoted me two grades and are trying to fire me for insubordination and unbecoming conduct because I have released public information to the public.

The Commissioners, particularly those who represent the political interest group known as realtors, have been in violation of the U. S. Freedom of Information Act, the N. J. Right to Know Law, the N. J. Administrative Procedures Act, and the very Real Estate License Act it is incumbent upon them to enforce. Those Commissioners who represent the political interest group of realtors must feel invulnerable and encouraged to act as they do because of the power they wield. Surely, they are considered untouchable and beyond criticizm by many elected officials as well as well known New Jersey newspapers who recognize realtors as a source of political power and/or income.

I also make this request because I believe I can contribute positive suggestions of benefit to the public. I have enclosed some samples of correspondence which help to illustrate the problems one can encounter in seeking information as a citizen, or in trying to make information available to the public while acting as an employee of New Jersey. The correspondence dealing with civil service was generated when I was cheated out of a job by Dept. of Treasury officials even though I had the highest score on the Civil Service test - I am a veteran of 21 years service, I have a disability rating, and I was certified to the position. Please note - one of the letters

was signed by Governor Brendan Byrne and the other by Chief Examiner Druz. Both letters speak of public records being attainable by way of subpoena duces tecum.

Now, surely, any record that has to be obtained by subpoena duces tecum is not a very public record readily available to the public. However, that is a shade better than the real estate commissioners who have instituted the use of a secret report which is not described in the Administrative Procedures Code nor is any procedure established for obtaining copies of the report by interested and affected broker applicants.

Upon reflection, I not only ask that you direct my appearance, but I also ask that you direct the appearance of the Real Estate Commissioners, the Chief of Civil Service, and last, Jack Regan, Director of the Real Estate Commission.

Yours truly,

Innocenzo M. Venta, Jr.
12 Colonial Ave.
Princeton Junction, N. J. 08550

Encls.

cc: Senator Alene Ammond
Senator James Cafiero - re: Mr. Regalbuto
Senator Wayne Dumont - re: Mr. Gregory De Vita
Senator Anne Martindell
Public Advocate Comm. Stanley Van Ness
Ms. Estelle Kuhn - Americal Civil Liberties Union

P. S. Please overlook the handprinting - Director Regan will not allow letters of this nature to be typed and will not forward them to addressees when routed through him as he has directed.

August 15, 1975

Honorable Matthew Feldman
c/o Ms. Gail R. Mazuco
State House
Trenton, New Jersey

Dear Senator Feldman:

I am writing in reference to Senate Bill S-3178 and our conversation of August 11, 1975. Thank you for offering me the opportunity to submit suggestions on the bill.

I indicated at the hearing and to Ms. Mazuco that I did not object to excluding from the record several of the letters that were enclosed with my initial letter to Senator Dugan on the subject of S-3178 and Assembly Bills A-1188, A-1466, and A-3133. Upon reflection and after reviewing my correspondence, I decided it would not be a wise idea to exclude the letters in question. I decided the letters were relevant and at the least illustrative of the problems a citizen and employee could encounter in obtaining or giving information from a state agency. Unless there is some overriding reason of which I am not aware, I would, therefore, appreciate having the letters included in the record.

I consider the privacy of the public and the public's right to obtain information to be essential elements in a successful democracy and therefore wish I could spend more time on this subject. Unfortunately, time is limited because of the press of other things. Nevertheless, I have a couple of suggestions which I offer for consideration. For example:

a. Appoint a Public Information Officer (P.I.O.) at department, division and bureau levels, and lower levels where necessary. The responsibility of the P.I.O. should be to insure that public information is made available to the public.

b. Appoint a civil servant as P.I.O. rather than a political appointee who is subject to political pressures.

c. Provide for the protection of a civil servant who releases public information to the public. For instance, do not allow reprimands, suspensions or removals from office to take affect before a fair and impartial hearing is held.

d. Require all agencies to identify in their administrative codes the types of information available or types not available. Information not available to the public should be clearly identified with justifiable reasons and only as approved by the Governor.

e. The administrative code of each agency should contain definitive instructions on how information is to be obtained.

f. The proposed law under S-3178 should relate to (and perhaps take the place of some) laws such as : The Administrative Procedures Act, The New Jersey Right to Know Law, Federal Freedom of Information Act. Along this line, the concept of the Sussman decision ought to be incorporated in the law.

g. A section of the law ought to be devoted to the types of information gathered by state agencies prior to issuing a license to a citizen.

h. Require an annual report from each public information officer. The report should cover such things as: types of information requested by and made available to the public; what problems were encountered; total monies received; suggestions received from the public.

i. Establish a firm date by which each state agency must codify its rules under the Administrative Procedures Act on the subjects of public privacy and the public's right to public information.

j. Provide for penalties of commissioners, political appointees or civil servants, who obstruct, inhibit, or through non-feasanle fail to obey the law. This is important lest you find other agencies doing as the New Jersey Real Estate Commission has done. The Real Estate Commission has ignored the law for some fifty-five years. New Jersey Law under 45:15-8 mandates as follows: "...all records kept in the office of the Commission under the authority of this article shall be open to public inspection under regulations prescribed by the Commission." The spirit as well as the intent of the law has been deliberately ignored by the Real Estate Commission.

Yours truly,

Innocenzo M. Venta, Jr.
12 Colonial Avenue
Princeton Junction, N.J. 08550

cc: New Jersey Real
Estate Commission

STATEMENT BY RUTGERS UNIVERSITY CONCERNING
S-3178, "RIGHT TO PRIVACY AND FAIR INFORMATION
PRACTICES ACT"

Privacy, confidentiality of records, and fair information practices are of concern to all members of the University community and so it is with great interest that Rutgers takes this occasion to comment on Senate Bill #3178.

In the main, such legislation should be warmly greeted by the public institutions and citizens of New Jersey. The extension of personal rights and the protection of personal rights from abuses in data collection, storage and dissemination are now recognized to be of similar importance to the First Amendment rights guaranteed for citizens.

Senate Bill #3178 clearly belongs to the growing family of privacy legislation and, as such, has some of the characteristics of the best of this work -- as well as the defects of other legislation in this field.

The University has had rather liberal privacy practices in the past decade and is in general conformity with the spirit of the contemporary privacy legislation. The proposed legislation, however, contains numerous ambiguities and defects which need comment. Further, as part of a general trend in the privacy rights area, this legislation must be examined in the context of the requirements of the rest of the legislation.

1. Ambiguity of Terms; Confusion of Terms

Throughout the legislation, perhaps due to the complexity of these issues, the language shifts from specialized mechanical, data-collection usage to ordinary usage in key terminology. This ambiguous use of terminology is puzzling in places and interferes with the meaning -- creating possible contradictions -- in some sections.

Examples of the problems include:

The use of the terms system and file in several different ways: Section 1c defines data system as the "total of components and operations". Section 1d defines file as a "record or series of records ... which may be

maintained within an information system". Information system goes undefined, but here file becomes ambiguous. File can mean, in ordinary language, the manila folders held in a health center, or it could mean a "file" of students' names, listed by county address, in the Registration system.

Section 4 requires that we give public notice of these files. To give public notice of each record (as in a manila folder or a transcript card) would be cumbersome enough. To give public notice of "files" as they are defined for computer system purposes would be nearly impossible (and extremely expensive). "Files" are often short-lived, assembled for single purposes and are then dismantled. To use the word to refer to something concrete is misleading in some cases.

Maintenance is another problem. In computer parlance, maintenance is correction. In ordinary parlance and in some parts of the proposed legislation, maintenance simply means "keeping". Thus maintenanceas used in Sections 3a&d is a different matter than "maintain" in Section 5b&c and still a different matter than maintenance in 5d and the "challenge and correct" provision of 6h. Perhaps the best way of solving this problem is to be clear on the meaning of the word by distinguishing between keeping and correcting.

The language needs to be clarified in order for the law to make sense and in order for the applicability of some of the provisions to be known. Particularly with respect to the public announcement and notification practices, a preferable procedure, in Rutgers' view, would be to describe the data-gathering and manipulation capacities in general. This could be accompanied by a sample list of major areas where records are kept.

It is not clear from the law what level of description and of what detail would be necessary to meet the requirements of Section 3a. Further, does Section 3c imply that if a student refuses to give consent to having his or her name in, for example, a registration system that Rutgers is barred from requiring this from the student as per Section 10? In a University being enrolled [e.g., enjoying the benefit of the University] entails being in a registration system. Similarly, being an applicant entails filing an application and being "on" an admissions system.

The complexity of writing legislation with a multiplicity of jargons and usages and an intention to protect rights is appreciated by the University. Nevertheless, there are matters here which need sharper definition.

2. Applicability of the Law

It is not entirely clear from the legislation just what or whom is covered or protected by the proposed law. The synopsis of the law identifies "New Jersey residents" as the protected class. The content of the proposed law seems to impose requirements on agencies and businesses within New Jersey without restricting the applicability of the law to New Jersey residents. Other sections of the law (notably 11b) seem to imply that the law (or the principle it advances) must be in force in all agencies and businesses having official interaction with New Jersey residents or those agencies or businesses in New Jersey doing business outside the state. Section 11c seems to extend the provisions of the law to all "recipients" of information on New Jersey citizens. (It is not clear that a state can make a law governing the internal affairs of corporations or institutions in another state.) Finally, the "Statement" on page 10 resorts to a protection of "New Jersey residents" once again -- which raises the issue of the applicability of this law to, for example, non-resident students at Rutgers. This is an area needing clarification.

3. Conflicts with Other Legislation

Rutgers is concerned about the possible conflicts between (and among) this law and the so-called Buckley Amendment already passed by the Congress (and with numerous other examples of legislation [e.g. Koch-Goldwater] proposed to deal with similar problems).

To expect compliance with numbers of different laws on the same subject is unrealistic if one considers the potential for conflict and confusion created by a multiplicity of legislation.

Further, in a time of great budget crisis for public institutions, to satisfy the various assurances, notification, publication and information-dissemination requirements of this spate of legislation is duplicative of costly personnel effort and time. Ultimately, the costs of these efforts will come from the protected class (or the sub-part of that class currently paying tuition and fees). This will only add expenses while not advancing rights appreciably.

A preferable solution would be some national coordinated effort (perhaps through the Federal government or through the nation's governors) to extend privacy rights uniformly.

4. Prior Restraints and Security of Records

Section 6 grants access to inspect personal information and seems to ignore the restraint imposed by the confidentiality of information received prior to the effective date of this legislation. Common Law concerns would seem to conflict with the intent of S-3178, here. The 6d provision does not seem to fully address this issue since it refers to "statute" requirements.

Further, Section 6d allows the confidentiality of the source (and presumably the content of a file) to be maintained, but states that the "nature" of the source of information may be released. This would seem to be a problem in that to reveal the nature is sometimes to reveal the source (as in law enforcement agency ...). Here it seems that an opportunity for abuse is permitted to continue.

Section 6g grants the right to obtain duplicate copies of records. Once again, this section is ambiguous in computer parlance since a file is rarely the record of a single individual and hence its release could abrogate the confidentiality of other persons. More serious threats are posed to the security of institutional records by having copies of individual records "in circulation". In essence, the University believes that the security of records is jeopardized if copies of records are permitted to be in circulation. How will "leaks" or abuses be determined or attributed if the security of records does not remain the obligation of the institution? The University favors the right of inspection, opposes the distribution of copies and urges that the legislation should reinforce a private person's right to subpoena records should this become necessary.

5. Public Hearings

Section 3g requires that:

> "Each agency or organization shall hold public hearings as to the purpose and operation of its data system before such agency begins collection, maintenance or dissemination of personal information in a new data system or a data system whose use of information has materially altered. Notice to the public of the hearings shall be given 30 days prior to such hearings..."

Aside from the ambiguity in the word "maintenance", the proposed law fails to specify just what the purpose of the public hearings is, who has a right to "object" to a proposed "data system", upon what grounds the objection can be made, how such a notice of hearings is to be accomplished for non-state agencies or political subdivisions, and under what circumstances a decision to begin a data collection effort can be reversed. Further, there is no way to determine what "materially alter" means in this section.

Section 3h seems to be tautological, and where it makes a statement "nor shall any organization...operate a data system that violates the rights of individual protected by this act", it seems gratuitous.

In order for this whole area to make sense, a number of the above questions need to be answered. While Rutgers supports the principle of openness with respect to data collection efforts, the relevance of this principle to the proposed rules seems negligible. All in all, hearings which have no defined purpose or opportunity for action of any kind are, at least, cumbersome and somewhat mystifying.

6. Rights to Challenge Content

While the thrust of this section on individual rights to challenge records is laudable and largely consistent with current University practices, there are two problem areas:

a. Verifiability - Section 7b requires that information "which can no longer be verified" must be eliminated.

This poses serious problems for the University. For example, a person's transcript is a record and in many cases the only record of academic

performance. We have thousands of records for which professors creating the record are no longer here, and, in many cases, no longer living. The information on transcripts is, at some point, unverifiable — since it stands as the sole record. In a timely way, any record may be challenged as inaccurate. But no record is strictly verifiable. The verifiability criteria poses a real dilemma for Universities.

b. Correction - The requirement of Sections 7c&d may be incompatible with computer storage systems. Further, since no reasonable restraints are placed on individual rights here, the opportunity for abuse by individuals is not restricted.

7. Cumbersome Notification Requirements

Probably more than any other institution, Universities are record-keepers. In modern education the record itself becomes the "test" for degree candidacy. Since Universities are also communities somewhat unto themselves, they contain many separate parts. Data collection efforts range from academic records, to health, psychological, advising, admission, financial aid, accounting, employment, pension and on down the line. All are included in the proposed act. Assuming the ambiguities about "file", etc. are clarified, to publish the "existence and character" of each record and to meet the requirements of 4b&c would constitute a massive effort.

Ironically, many of our records are routinely given to students, such as term grade reports, financial aid need determination and calculation, and accounting records. Consequently, it seems wasteful to tell a student that he or she has a term grade report, where it is, under whose control, etc., since the student receives copies of this information routinely.

Rutgers suggests that these requirements are so extensive that they pose serious problems in meeting them for the conscientious institutions. Further, the opportunity for exception from these requirements (as in 15c) on the grounds of "the public interest" is ambiguous. Those most needing protection may go unprotected while the rest of society labors under unreasonable requirements.

If a Commission is created, isn't it preferable to wait until complaints on information matters are received prior to requiring this extensive effort. In order to effect compliance, a "complaint-generated" basis seems to be more practical. It seems unlikely that the Commission with a modest number of employees could possibly evaluate the thousands of reports which would be received by it annually if this legislation is enacted. With limited resources, Rutgers suggests that emphasis should be on investigation of complaints and the enforcement of the law for habitual offenders.

8. The Proposed Commission

With the requirements of the proposed legislation, it seems more than obvious that a Commission is needed. It has been suggested earlier that the Commission and its employees will probably have more than enough to do just receiving and recording information on an annual basis -- setting aside the need to hear cases, make policies, etc. There are several questions which need to be asked about the Commission's make-up, authority and powers.

1. What criteria were used to determine the size of the Commission? The opportunity for an adequate diversification of interests and expertise does not seem to be accommodated by the limited number of five members.

2. Section 21 specifies the Commission's purpose, but seems to place no restraints on the Commission nor does it specify a procedure whereby an act by the Commission can be determined as consistent or inconsistent with the law itself.

3. The cost of having an effective effort in this area is probably rather large. Does it not make sense to reduce such expenditures where the same or similar enforcement of privacy rights is accomplished by the courts and other government agencies (like HEW, in the case of education)?

Conclusion

The difficulties inhering in attempts to extend new rights which we all acknowledge to be of seminal importance are enormous. Where eloquently succinct laws have the advantage of establishing the bones of a principle -- the flesh must come from the courts. Where the flesh comes with the bones, the problems loom initially.

The experience which Universities have recently had with the Buckley Amendment and the changes which HEW is making to the regulations may be instructive in this New Jersey effort. Attached is a copy of the Rutgers' comments on that legislation -- parts of which are relevant to S-3178.

The protection of privacy rights is important and needed. It is hoped that the foregoing will help move us all towards that objective. Rutgers looks forward to working with the legislature and its committees to further this goal.

Rutgers University
Office of the Vice President for Student Services
August 1975

Attach.

RUTGERS UNIVERSITY *The State University of New Jersey*

VICE PRESIDENT FOR STUDENT SERVICES
New Brunswick, New Jersey 08903
Tel. 201-247-1766

March 18, 1975

School Records Task Force
Mr. Thomas S. McFee
Room 5560
Department of Health, Education and Welfare
33 Independence Avenue South West
Washington, D.C. 20201

INSTITUTIONAL COMMENTS ON FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

Dear Mr. McFee:

Contained herein are the general comments and questions by Rutgers University on the Proposed Rules promulgated by HEW pursuant to Title IX of Public Law 90-247, as amended, added by section 513, Public Law 93-380 as amended by Senate Joint Resolution 40, 1974.

1. General Agreement and Endorsement

Rutgers certainly endorses the principles and purposes which are embodied in the legislation. The proposed rules, as written, go a considerable distance towards clarifying the original legislation and its intent.

2. Items Needing Example or Definition

a. In Section 99.6 (c), the phrase "any other services or benefits from an agency or institution" is employed respecting the non-coercive stance which institutions must take respecting a students opportunity to waive access rights. Examples of the "services and benefits" would be useful. If a professor were to refuse to write either an informal course evaluation (not a requirement or a grade) or a letter of recommendation unless the student waived the right of access, would the institution be in violation of this section?

b. Placement personnel have raised "definitional" questions concerning Section 99.39 (a). While the problem does not directly concern Rutgers, is the intent of this provision to limit access to the addressee only (as in Personnel Office, X Corporation), or may that person transfer the material to appropriate "third parties" for a decision?

c. We fail to understand the use, desired denotation, or purpose of the word "except" in Section 99.37 (c). Please clarify.

3. Consent

Once again, our difficulties with consent do not involve current matriculants so much as they involve the "placement" offices who perform services for students after their departure from the University. Section 99.31 seems to require that the student must specify "(c) the names of the parties (to whom) such records will be released."

Often students accumulate a dossier, indicate that they are available for employment, and ask that their dossiers be considered for "anything that comes up." Also frequent is the practice of a professional placement officer offering a list of potential applicants to a prospective employer.

Even with the student on campus, to follow the requirements strictly would be burdensome, time consuming, and costly. For graduates, often remote from the campus, these requirements create enormous problems and may very well act to the detriment of the person protected by the Law.

Rutgers suggests that the consent provision be rewritten, either, (1) to exempt counseling and placement offices from its provisions, or, (2) to permit general ("blanket") consent agreements between students and agencies within the University designed to serve them.

4. Copies of Records to be Provided

Protecting the integrity of institutional records is of great importance to Rutgers. Consequently, there is no small concern at Rutgers regarding Section 99.32, especially as it relates to 99.39 (prohibition or release to third parties). With the requirement that Rutgers provide and release copies of information to students, what controls are there on the opportunity for misuse of the materials to the disadvantage of the institution? How could official records be distinguished from other ones, if copies of the records are readily obtainable by students? Must each office having records possess and use a "seal" or some emblem which identifies the document as official?

While Rutgers has no specific recommendation to make here, clarification is asked. Could the Law stand without the "copy" provision, since the right to review and inspect is retained, as is the

right of subpoena?

5. Directory Information

The University expects to issue a pamphlet to detail its record policy and to reflect the provisions of the Law. Section 99.40 requires that institutions "give public notice" of information to be issued as directory information and to "allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent."

Rutgers lists more than 45,000 students in its directories and answers hundreds of telephone solicitations for "directory" or public information each year. While it is expected that the provisions of the Law will be made public, to enforce this particular regulation will add substantial burdens in both staff time and dollars.

Further, this requirement presumes that no enrollment information about particular individuals is public information. What is the legal basis for this presumption?

Must the opportunity for withholding directory information be open to just students (if, in fact, the home phone number were actually that of the parent)? What is a reasonable period of time?

6. Notification by Educational Institution

Section 99.5 requires systematic annual notification of students of the requirements of the Law. While Rutgers understands that "what is reasonable for a one room school house would not be reasonable for a University", HEW has failed to specify what would be acceptable for a University. Rutgers has over 20 divisions enrolling over 45,000 students. Many thousands of graduates and persons having been matriculated at the University also exist and seem to be subject to this Law.

To inform students of these rules will be costly and difficult enough (given paper costs and the threat to end the second class postage rate). To inform alumni and others who have been associated with Rutgers may very well be impossible.

The extensiveness of the requirements, e.g. "names and position of the official responsible . . . the persons who have access . . . policies regarding destruction," etc., will make it very difficult to perform this notification task accurately and in the form specified.

A description of compliance is essential in order that Rutgers may meet its legal obligation without tying up resources needed elsewhere in this time of budget constraint.

7. Access

Analogous to our question as to whether it is possible to grant a "blanket" consent, is it possible to waive one's right of access to a file, in perpetuity? This is not a recommendation but a query as to whether an individual may sign "broad" waivers or must he or she sign individual waivers for each particular letter of recommendation, application for award, etc.?

Does Section 99.12 (c) (2) refer to employment counseling and placement?. If so, we need a clarification as to how it does. If not, we need to have some indication of what "employment" refers to in this section.

The foregoing comments and suggestions are submitted for your review. In order that we may begin to implement the provisions of the Law, a response from you on our specific questions would be helpful. Finally, let me say that, during the dark period just following the passage of the Buckley Amendment, my conversations and the information provided by individuals at HEW helped us to keep our institutional composure. For this service, I wish to register my appreciation.

Sincerely,

William David Burns
Assistant to the Vice President
for Student Services

WDB:srp

STATEMENT ON BEHALF OF
STANLEY C. VAN NESS, PUBLIC ADVOCATE
IN SUPPORT OF S-3178

S-3178 would impose much needed controls on the collection, maintenance, and dissemination of personal information on New Jersey citizens by governmental and private institutions. I strongly endorse this bill and urge its passage.

The right to privacy is the bedrock of democracy. A free people cannot long tolerate serious encroachments on their fundamental right to privacy. Yet, the last few years have seen a proliferation of data banks by governmental and private interests. For example, in the summer of 1974, the United States Senate Sub-Committee on constitutional rights reported that 54 federal agencies maintained 858 data banks on individual citizens and had over one billion records. The Federal Bureau of Investigation maintains approximately 200 million fingerprint cards; state and local agencies, including law enforcement agencies, have hundreds of millions of records. Schools, hospitals, and credit bureaus maintain extensive personal information files. The Medical Information Bureau, which serves the insurance industry, has medical and psychiatric records of 13 million people.

The fact is that information about almost every individual in this country is contained in thousands of computerized files. Our precious sphere of privacy is slowly being whittled away. Moreover, the disclosure of erroneous and misleading information about an individual has serious implications. This trend will continue unless something is done quickly. S-3178 is indeed a powerful weapon with which to reverse this alarming trend.

Any good privacy bill must have as a minimum a provision requiring notification to and consent of the individual prior to the maintenance or dissemination of any data on such individual. S-3178 has this and, indeed, many other salutary features. Included among these are provisions requiring public notice as to the nature and purpose of the data or information system; access to and right to inspect the system; a meaningful opportunity to correct errors; and strong criminal penalties for willful violations of the act.

Although on the whole I am very much in favor of this bill, I do have some suggestions and criticisms. The provisions relating to the activities of law enforcement agencies leave something to be desired. Paragraph 15(a) totally exempts the "permanent and investigative data systems or files" of law enforcement agencies. Moreover, under paragraph 14, the consent requirement of the bill does not apply to disclosure from one law enforcement agency to another. I realize that the exchange of complete and accurate criminal justice information among law enforcement agencies is necessary and indispensable to effective law enforcement. It must be remembered, however, that the disclosure of misleading, inaccurate or irrelevant data from police files can have a devastating impact on an individual's life. I believe that S-3178 should have specific provisions which appropriately limit the dissemination of arrest, conviction, and non-conviction records. In this regard, I note that A-2336 and A-2339 are now pending in the Senate. These bills, relating to expungement of arrest and conviction records, would complement S-3178.

Paragraph 3(d) prohibits information gathering on individuals who exercise their first amendment rights unless "authorized by law or regulation." This

exception is vague and probably too broad. At the very least, the term "regulation" should be deleted.

Paragraph 7 permits an individual to appeal directly to the commission on privacy if that individual cannot resolve a dispute regarding information in a file. Many individuals may not avail themselves of this appeal mechanism because of their reluctance to become involved in formal proceedings. It might be desirable to appoint a mediator, attached to the committee, who would attempt to resolve all disputes, if that dispute was not resolved in the first instance by the individual and the institution that gathered the information. This mediation procedure would occur before appeal to the committee. Mediation might also serve to filter out disputes of a minor or frivolous nature, thereby reducing what might otherwise be a serious backlog of cases before the commission.

I appreciate the opportunity to submit this statement, and I hope that S-3178, with some modifications, meets with swift passage.

STATEMENT ON BEHALF OF
SNELLING AND SNELLING OF PLAINFIELD, NEW JERSEY
BEFORE THE JUDICIARY COMMITTEE OF THE SENATE
STATE OF NEW JERSEY

PRESENTED BY MRS. ANNE T. GARDNER C.E.C.
Legislative Representative

Snelling and Snelling is a franchised network of over 500 employment services located throughout New Jersey and the United States. At this time, there are 36 Snelling and Snelling employment agencies located in the State of New Jersey, providing jobs for New Jersey residents and qualified, capable employees for New Jersey businesses. I am an owner of Snelling and Snelling franchises in Plainfield and Edison, New Jersey, and am a member of the National Legislative Committee of Snelling and Snelling, Inc., the franchisor corporation. I am accompanied by Robert P. Style, Vice President and General Counsel of Snelling and Snelling, Inc., which is located in Paoli, Pennsylvania.

The purpose of my presentation is to oppose Senate Bill 3178 as that Bill would apply to the operation of private employment agencies in the State of New Jersey and urge that the activities of these employment agencies be exempted, from the sections of the Bill.

During the past few years, a legitimate concern has arisen regarding the intrustion of government and business on the basic right of privacy of citizens. It is, I am certain, at least partially as a result of this concern, that Senate Bill 3178, which would create a Commission on Privacy,

Freedom of Information and Public Information, has been proposed.

It is not my purpose here to contend that this concern is an unnecessary one, because I share the view that the right to privacy is an important right, and the State of New Jersey has a legitimate interest in protecting its citizens from violations of that right. However, I am also concerned, both as a businessperson and as a citizen, with the necessity of providing job opportunities for the citizens of New Jersey, and I believe it should be a legitimate state concern not to unduly interfere with a vehicle through which those job opportunities are provided.

It is my position, and the position of Snelling and Snelling, that, sections 3,4,and 5 of the Senate Bill 3178, if applied to the private employment agency profession, would add little to the protection afforded our citizens against violations of their privacy, but might seriously infringe upon the ability of private employment agencies to continue to provide job opportunities for these citizens. I, therefore, urge that private employment agencies be exempted from many of the requirements of these sections of the Act, and further urge the adoption of an amendment to the legislation which would state "Sections 3,4 and 5 of this Act shall not apply to organizations licensed as employment agencies by the Division of Consumer Affairs of the Department of Law and Public Safety."

Sections 3, 4 and 5 of the Act all are designed, it appears to me, to prohibit the accumulation and dissemination of data regarding an individual without that individual's knowledge, consent or approval. Such a concern is not relevant to the operations of private employment agencies. The private employment agency is compiling data on applicants who contact its offices at the direct request of those applicants, in order that the skills of the applicant can best be presented to prospective employers. The private employment agency, unlike credit research organizations, does not earn any money from the mere compilation or dissemination of the data, but only earns its fee if it is able to use that data to market the skills of the applicant. The applicant desires that the private employment agency compile data on him or her, directly aids it in doing so, expressly consents by his own contact with the agency to the compilation of the data, and hopes and expects that the employment agency will use that data for the applicants benefit.

Essentially, therefore, Senate Bill 3178 imposes the following duties upon employment agencies in Sections 3, 4 and 5 thereof:

1. Employment agencies would be required to disclose to applicants that they will be compiling data concerning the, even though the fact that this data is compiled is obvious to every applicant who contacts the agency.

2. Employment agencies shall be required to identify those to whom disclosures of personal information are made even though these disclosures are made at the direct request of and in order to provide a service to the person about whom the information is being disclosed.

3. Employment agencies shall be required to disclose to applicnats that information which it maintains in its files concening them, even though the great majority of that information has come from the applicants themselves.

All of the above burdensome requirements, as well as the other technical requirements of Sections 3, 4 and 5 are designed to protect the applicant against a procedure which is set up solely for his own benefit. Employment agencies do not compile data on individuals unless that individual, by contacting its office to apply for employment, has indicated th willingness for that data to be compiled concerning him.

I also sbmit that the Federal Fair Credit Reporting Act sufficiently protects those who use the servies of employment agencies from any abuses of the information contained in the employment agency's files. This Act specifically requires disclosures, upon the written request of the applicant, of the information in the applicant's file concerning him, and require that the applicant receive the opportunity to correct that information. Essentially,I submit that the Fair Credit Reporting Act gives the applicant who deals with employment agencies all the protection which he or she needs.

In summary, as applied to private employment agencies, sections 3, 4 and 5 Senate Bill 3178 will only serve to impose technical procedural burdens in the way of organizations which are acting on behalf of those who seek to gain meaningful employment and remove themselves from the welfare of unemployment compensation rolls, or those who seek to improve their current economic situation. In our economy, anything which interferes with these activities should be rather closely examined. I believe that a close examination of Senate Bill 3178 will show that our citizens will receive necessary protections by exempting private employment agencies from Sections 3, 4 and 5 of the Act, and urge the enactment of such an amendment.

NEW JERSEY ASSOCIATION OF PRIVATE EMPLOYMENT AGENCIES

60 Parkway Drive, East East Orange, N.J. 07017 201-676-6688

August 8, 1975

The Honorable Matthew Feldman
Senate of the State of New Jersey
The State House
Trenton, New Jersey

Dear Senator Feldman,

Thank you for the courtesy of hearing testimony from myself as representative of the New Jersey Association of Private Employment Agencies.

Our Association represents approximately four hundred and fifty of the approximately six hundred and fifty licensed agencies presently licensed by the Private Employment Agency Section of the Division of Consumer Affairs of the Department of Law and Public Safety. We are the spokesmen for those private agencies whose primary business is the locating of employees for companies and of jobs for applicants which employment is intended to be of a permanent nature. We do not represent services engaged, primarily, in the placement of temporary employees, contract engineers or laborers, or professional services such as nurses registries, etc.

Under the provisions of P. L. 1951, c. 337 (C. 34:8-24 et seq) all licensed private employment agencies are required to maintain records and data files on individuals for the purpose of securing employment for them. All such agencies must meet licensing requirements of the Department of Law and Public Safety and these records are subject to regular and unannounced inspection by the Private Employment Agency Section of the Division of Consumer Affairs.

All such employment agencies are presently under the official control of the Department of Law and Public Safety.

We believe that sections 3, 4, 5, and 11 of proposed Senate Bill 3178 will impose an unnecessary duplication of administrative control on our industry. By its nature, this is an industry in which most companies are small (less than ten employees in all) and for whom a duplication of necessary record keeping would present a costly and difficult task for several reasons, not the least of which are basic differences between existing law and the proposed law.

Employment agencies maintain their records with the knowledge, cooperation, and consent (verbal or written) of those on whom the records are kept. These records are maintained for the sole purpose of assisting the persons referred to in them to find new or bettered employment. The vast bulk of their contents are supplied to the agencies by the persons referred to in them. Those portions which

are not obtained from the individual but from other sources are strictly and explicitly controlled by the United States Fair Credit Reporting Act of 1971. This law specifies that certain consumer reporting agencies (which includes employment agencies by definition) must first obtain the written permission of the person involved before instituting an investigation of previous employment or other specified items of information. This law further requires the agency to disclose the complete nature and scope of information which is received in this manner to the person involved upon request of that individual.

For all of these reasons, the New Jersey Association of Private Employment Agencies believes that certain portions of Senate 3178 should not be required of our industry and respectfully suggests that the following paragraph be inserted between paragraphs 15(b) and 15(c) of the law:

> ¶Sections 3, 4, 5, and 11 of this Act shall not apply to organizations licensed as employment agencies by the Division of Consumer Affairs of the Department of Law and Public Safety.

We congratulate you and your fellow sponsors on the intent and scope of the bill in question as a demonstration of your regard for the right of citizens to their privacy.

I am prepared to submit whatever additional information is needed and can be reached during business hours at (201) 487-0900.

Enclosed with this letter, you will find the statement of Mrs. Anne T. Gardner, CEC, Legislative Representative of Snelling and Snelling, Inc., the major franchisor of private employment agencies in this state, relating to the same subject.

Respectfully,

Eugene C. Batkin

Eugene C. Batkin
Certified Employment Consultant

Legislative Chairman
New Jersey Association of Private Employment Agenc

ECB:hs

SUBMITTED BY
RALPH A. DUNGAN
CHANCELLOR OF HIGHER EDUCATION

STATE OF NEW JERSEY
DEPARTMENT OF HIGHER EDUCATION
TRENTON, NEW JERSEY

OFFICE OF THE CHANCELLOR

STATEMENT ON THE IMPACT OF BILL S.3178

The Department of Higher Education supports the purposes of the bill but believes that immediate action may have negative personal, administrative, and fiscal effects, if careful consideration is not given to the impact of this legislation. Precipitate action on the Federal level resulted in the Federal Privacy Act of 1974, a bill which has been characterized by Federal agency officials as a "compromised hodge-podge" and an ineffective piece of legislation which, it has been predicted, will be "piecemealed to death" in order to rectify its internal inconsistencies. This is not an approach we would like to see emulated on the State level.

The collection, maintenance and dissemination of personal information in the Department of Higher Education is carried out primarily by the student financial aid offices (State Scholarships, Educational Opportunity Fund, Student Loans) and this statement, therefore, focuses on the effects of S.3178 on the operation of those offices.

Section 3(e). "Each agency....maintaining a data system or file shall upon request by any individual to gain access to his record or to any information pertaining to him....permit him to review the record....". The actual paper files containing personal data in each of the student financial aid offices are presently open and accessible for anyone to inspect and amend his or her own file. Current practice is to disclose verbally or to show actual records to the individual who inquires or to a person designated by the individual. Access then is not a problem, but the cost of complying with the latter part of Section 3(e) "....and have a copy made of all or any portion thereof in a form comprehensible to him...." would be prohibitive. Some personal data on scholarship and loan applicants are on computer tapes, while some are in the paper files. In order to provide the student with a copy of all information in a comprehensible form, an entire series of computer programs would have to be re-written at an estimated cost of several hundred thousand dollars to provide this service on a routine basis.

The records include information on parental income which some parents do not wish to share with their children. This problem has been anticipated on the Federal level with the result that the Privacy Act specifically exempts the financial records of the student's parents from inspection by the student.

In order to be consistent with Federal legislation, it is therefore suggested that Section 3(e) be amended to include the following language:

> "Students have the right to inspect and review their educational records except for the financial records of the student's parents."

Sections 5(c) and 6(c) require each agency and organization to maintain an accounting of the date, nature, and purpose of all other access granted and to assure that an individual can know the identity of all recipients of information about him.

In order to comply with these provisions on a routine basis, the Department of Higher Education would have to hire additional staff and re-write computer programs as mentioned above.

Section 11(b) states "No agency or organization shall disseminate personal information unless: .... the recipient of the personal information has adopted rules in conformity with this act for maintaining the security of its information system and files and the confidentiality of personal information contained therein;". Putting the burden of proof on each agency or organization to assure conformity on the part of the sharer of the information could lead to restricting the availability of information needed from or by schools, lending institutions, Federal or other State agencies. In the case of student loans, such a requirement would have a harmful effect on the loan office's relationship with credit bureaus, making it difficult to locate those who default on loan payments and to collect monies owed to the State of New Jersey. Extra expense and staff needed to trace outstanding notes could again result in additional costs of over one hundred thousand dollars.

Section 26. "This act shall become operative 90 days after its enactment." Because of the considerable re-programming required by the Act, and the resulting expense, at a time of serious fiscal constraint, it would be impossible for the Department of Higher Education to comply with all the provisions of the Act within present appropriations.

In order to gauge the eventual impact of the provisions of this legislation, it is the Department's recommendation that the Legislature conduct a statewide survey prior to legislative action by using a questionnaire such as the one attached which Senators Koch and Goldwater (H.R. 1984) sent out to selected private organizations and state and local governments as a part of Federal committee consideration. Only with such information at hand could more informed estimates of statewide effects be reached that would allow accurate appropriation estimates for this Bill.

In sum, the Department supports the objectives of this Bill, but cannot endorse all technical aspects of the Bill until more information is obtained on its effects in terms of time and resources required for implementation.

August 11, 1975

5. Listed below are the ten principles of privacy. For each check:

Column A - If your organization or firm presently practices the principle
Column B - If you believe that your organization could easily implement the principle
Column C - If you believe that your organization could not implement the principle because of cost, time, or operational considerations
Column D - If there are technical, administrative or legal problems and limitations.

PRINCIPLES OF PRIVACY	A	B	C	D
1 Permit any person to inspect his own file and have copies made at reasonable cost to him				
2 Permit any person to supplement the information in his file				
3 Permit the removal of erroneous or irrelevant information and provide that agencies [organizations] and persons to whom material had been previously transferred, be notified of its removal				
4 Prohibit the disclosure of information in the file to individuals in the agencies [organizations] other than those who need to examine the file in connection with the performance of their duties				
5 Require the maintenance of a record of all persons inspecting such files, and their identity and their purpose				
6 Insure that the information be maintained completely and competently with adequate security safeguards				
7 Require that when information is collected, the individual must be told if the request is mandatory or voluntary and what penalty or loss of benefit will result from noncompliance				
8 Require that the person involved in handling personal information act under a code of fair information practices, know the security procedures, and be subject to penalties for any breaches				
9 Permit anyone wishing to stop receiving mail because his name is on a mailing list to have that right				
10 Prohibit agencies or organizations from requiring individuals to give their social security number for any purpose not related to their social security account, or not mandated by federal statute				

* Recognizing that your organization may handle differently employee, client, or other records, you may wish to make additional copies of this page

Specify type of record

Congress of the United States

House of Representatives

Washington, D.C. 20515

KOCH-GOLDWATER PRIVACY SURVEY OF SELECTED PRIVATE ORGANIZATIONS AND STATE/LOCAL GOVERNMENTS
1975

Organization _____

Address _____

_____ Zip Code_____

Organization contact

Name _____

Title _____

Telephone Number _____

1. Describe your organization, specify type, function, and major objectives.

2. Indicate the approximate number of employees _____

3. Indicate if your organization uses, collects, handles, or disseminates records which contain individually identifiable personal information (manual/automated). If computers are used to handle these records indicate percentage of their use as well as mode of operation.

- Type of Records -	Number of Records	Computer Operation Batch	On-line	ADP In-house	Supported by Service Bureau
(a) employee records (includes payroll, health, etc.)	___	___	___	___	___
(b) client/student records	___	___	___	___	___
(c) other records: specify (i.e., investigative, sales, credit, mailing list, statistical)	___	___	___	___	___

4. If the enclosed Public Law 93-579 were to apply to your organization's operations, what problems do you foresee. (If needed, use additional sheets for your comments.)

RICHARD C. McDONOUGH
Attorney-at-Law
20 WEST LAFAYETTE STREET
TRENTON, NEW JERSEY 08608
(609) 393-3700
(201) 755-4033

TO: MEMBERS OF THE SENATE JUDICIARY COMMITTEE

FROM: RICHARD C. MC DONOUGH, LEGISLATIVE COUNSEL
RETAIL CREDIT COMPANY

RE: SENATE BILL NO. 3178

DATE: JULY 28, 1975

On behalf of Credit Bureau, Inc. I would like to offer the following statement in opposition to Senate Bill No. 3178. Credit Bureau, Inc. is in the business of facilitating transactions between consumers seeking to buy goods and services on credit, and a merchant who wants to provide the goods and services to the consumer - providing the merchant can reasonably expect the consumer to make good on a "promise" to pay on mutually agreed upon terms based on the consumer's past pay record.

To illustrate, daily our New Jersey customers buy tires, refrigerators, televisions, clothes - all on "credit." They need these items and others now but want to pay for them over an extended period of time. A quick check over the telephone by the merchant with the local credit bureau usually allows this businessman to confidently sell these to the consumer on credit.

Our files are computerized to better serve our merchant customers who in turn are constantly striving to better serve the consumer. No longer can a consumer point to a local department store and suggest that a potential creditor ask the credit department of the store to testify as to the consumer's past pay record. That department store may have their credit files in Chicago, New York or Houston.

Because the idea of buying on credit had become such a fundamental principle in the American way of life, a special study committee was charged with analyzing in detail the role of "credit" in our economy.

The National Business Council for Consumer Affairs was thus created by an Executive Order on August 5, 1971. In a Summary Report, "Financing the American Consumer," the Sub-council on Credit and Related Terms of Sale stated that:

"Consumer credit, in adding substantially to the buying power of consumers, has affected both the level and structure of consumer demand. This increased consumer demand, in turn, stimulates the production and distribution of goods and services on a mass scale, thereby providing greater employment opportunities, high income levels, and lower unit cost to the consumer."

The study goes on to say:

"Over-extension of consumer credit usually results when the credit grantor errs in his judgment of, or ignores, the applicant's ability to pay, or when the applicant himself over-estimates his repayment ability.

From the credit grantor's point of view, these decisions often depend on reliable credit information. Some legal limits have been placed on the use of credit information, and proposals have been offered which would add further restrictions. Consumer rights should be protected in this area, but it should be noted that a continuing trend in this direction can be harmful to the consuming public if it results in greater credit over-extension, or in the curtailment of credit availability."

A specific recommendation was that:

Government agencies at all levels should avoid actions which unnecessarily erode consumer credit information systems.

It continued:

"Operation of a rational and efficient consumer credit system would be impossible without this information. Over-extension, and even bankruptcy, would rise as the accuracy of this data decreases, so all reasonable precautions should be taken to insure its quality.

In this context, provisions should be made for consumers to easily identify and rectify any errors in their personal file. In addition, the confidentiality of the data should be carefully preserved to respect the consumer's right of privacy against unauthorized use of credit information."

Even prior to the Sub-committee report, Congress, after years of carefully investigating the consumer reporting industry, established in law procedures aimed at giving protection to the consumer but at the same time would protect the free flow of business information needed to base business decisions so vital to the consumer in today's credit economy.

Thus, the Federal Fair Credit Reporting Act was enacted in April, 1971. This law sets up specific procedures designed to both meet the needs of commerce for consumer credit, personal, insurance, and other information, and in a manner which would be fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy and proper utilization of such information.

The Fair Credit Reporting Act, which became effective April, 1971, provides:

1. That a reporting agency may issue a consumer report only in connection with a legitimate business transaction involving the consumer. Further, the recipient of the report must have certified his need for the report and certified that the report will be used for no other purpose.

2. That a consumer is notified - in writing - when an investigative consumer report is requested and notified of his right to get full disclosure of the nature and scope of that investigation.

3. That whenever an individual is denied a benefit, or pays more for the benefit, because of information supplied by a consumer reporting agency, he is notified of the fact and supplied with the name and address of the agency.

4. A reporting agency may not report adverse information, except bankruptcy information, for more than seven years.

5. That a consumer, at his request, has the right to complete reporting agency disclosure of all consumer file information pertaining to him.

6. That a reporting agency must reinvestigate any file information that is questioned by the consumer.

7. That any information that cannot be reconfirmed by the reporting agency must be deleted from its files and a corrected report must be sent to previous recipients of the information.

8. That a consumer has the right to make a written statement concerning reconfirmed information which he has questioned, and that the statement must be included in all future reports that are issued which contain the questioned information.

9. That the law provides legal remedies to the consumer for willful violations of the Act by a consumer reporting agency.

Enclosed are certain materials that I have extracted from the CONGRESSIONAL RECORD concerning the original Federal Fair Credit Reporting Act (FCRA) including presentations by Senators Proxmire, Javitz and Williams, and the actual summary of the purposes which the Senators felt would be achieved by passage of the FCRA in 1970.

The FCRA took effect in April of 1971 and is administered by the Federal Trade Commission (FTC). In 1973, the FTC made certain recommendations for changes in the FCRA which were introduced by Senator Proxmire on August 3, 1973 as Senate Bill 2360. Thereafter, the Sub-committee of Consumer Credit of the Committee of Banking, Housing and Urban Affairs of the United States Senate conducted hearings on S-2360. This bill included provisions to permit the consumer to physically inspect his credit file and to receive a written copy of all the information in the file and also required the users of credit information to inform the consumer of the reasons for his credit rejection in writing and to give a copy of any credit report supplied to the user to the consumer.

Thereafter, after additional hearings, the Sub-committee had its "mark-up" session on November 27, 1973 at which time Senator Brock noted that the FTC had not prosecuted any suits for violations of the FCRA and suggested that this failure indicated that there were few, if any, violations. He also felt that the requirement for written notification would deny access to the market place to many consumers. Senator Brooke indicated that many of the amendments contained in S-2360 had been considered in the original bill and rejected, and he felt that to move in the direction of supplying printed copies of the reports to the applicant was premature since all indications to him were that the present act was working well. Senator Sparkman agreed with Senator Brooke as to the premature character of such severe amendments and agreed with Senator Brock that the FTC had not documented its case - that new legislation was necessary. At that session, a Motion was made to table S-2360, which was carried 4-2.

I bring these matters to your attention to acquaint you with the fact that the Congress has been keeping its eye on the performance of the industry under the FCRA and will continue to do so, when and if the regulatory arm, the FTC, can demonstrate to Congress that the present bill is not working and that amendments are necessary to protect the consumer.

On behalf of my client, Credit Bureau, Inc., we strongly endorse this position. We have testified in Washington, both before Congressional committees and the FTC, to make clear our position with respect to the implementation on a

continuing basis of the FCRA. Credit Bureau, Inc. feels the FCRA is working well, the balance between consumer rights and privileges and the needs of the credit industry are maintained by the law in its present form and amendments like S-2360 or S-3178 are unnecessary.

By way of background, S-3178 appears to draw heavily from recommendations made by the Secretary's Advisory Committee on Automated Personal Data Systems, established by former Secretary of Health, Education & Welfare, Elliott Richardson.

A review of the Committee's charter and recommendations clarifies the fact that the report actually was not intended to suggest actual language suitable to be incorporated directly into legislation - but rather to serve as a guide to the information of public policy in the general management of personal data systems. The Director of the Study Commission, Willis Ware, actually stated in subsequent hearings on a bill which similarly drew from the Studies' recommendations, that the private industry was not covered and if it, in fact, was covered, could have serious economic impact and could result in tremendous costs with no known benefits.

We must strongly object to any requirement which would bar the transference of "personal data" without obtaining prior informed consent of an individual. This unnecessarily restricts the free flow of business information which is so vital to our economic well being.

The detailed registration and notification requirements suggested by S-3178 place unnecessary restrictions and subsequent penalties on even the most routine accumulation of information of even say employees of a firm and such provisions would in no way benefit the individual consumer who depends upon his personal and professional background to assist him in obtaining credit, insurance, advancements in employment, etc. The further requirement that specific sources of information on file be disclosed to consumers will similarly grind to a halt the free flow of business and other information. Such was the case when the United States Congress passed into law a bill which required sources of information contained in school records (letters of recommendation, etc.) to be disclosed to an individual student. It was strongly pointed out by the educational community that if this were the case, no professor or educational administrator would detail his personal feelings as to recommendations for graduate school, specific courses of study, etc. This led HEW to propose regulations which protected such sources of information and does point out that legitimate sources of information must be protected if the quality of the information is to remain free and not diluted to everybody being "average." The same argument applies as to copies of files being made available to individual consumers which similarly could disclose sources of information. Both of these provisions - revealing of sources of information and providing copies of files - are contained in S-3178. Both have been proven as highly restrictive to the flow of business information since it seems illogical that a person would provide information - both favorable and otherwise - if their identity could become routinely known by an individual consumer.

To summarize, we must take the position that S-3178, if consumer reporting agencies are not excluded, will so unnecessarily restrict the free flow of business information so important in our credit oriented society that it would actually work to the detriment of the consumers within our state by eroding the business as we know it today.

Since there is currently adequate federal law covering "consumer reporting agencies," we strongly urge that an amendment be included in this bill which makes it quite clear that S-3178 does not relate to "consumer reporting agencies" as defined by existing laws.

While credit bureaus both inside New Jersey and outside its boundaries may or may not utilize computers to communicate with merchants that may or may not keep their business records also in computers, legislation should not, in our opinion, be designed which limits in any way the basic and sole purpose of a credit bureau - which is - to facilitate transactions between consumers and business.

Enclosed please find a copy of a brochure which was prepared for use by consumers to help them understand their rights under the Fair Credit Reporting Act. I trust it will answer most, if not all, of your questions. Of course I will be happy to discuss any additional matters which you feel need further explanation.

Finally, I would like to take this opportunity to extend a formal invitation to all members of the committee to visit one of our facilities in this State to see how the credit reporting business operates and how we perform our duties and obligations under FCRA. I shall call you in the near future to see if we can agree on a mutually convenient date to visit with us. I am mindful of your very busy schedule and every attempt will be made to meet with you at your most convenient and least time consuming opportunity.

Atlantic Richfield Company Statement

New Jersey Assembly Bill No. 3338
"Right to Privacy" and "Fair Information Practices Act"

The Federal Department of Health, Education and Welfare sponsored a study early in 1972 to examine the privacy issues. A comprehensive report on this was made in July, 1973 - sometimes called the Ware Committee Report - which contained many excellent recommendations, as well as a set of principles to be used as guidelines for protecting individual privacy. However, these were presented as goals and not as a statement of present technological feasibility. Subsequent to the Ware Committee Report, a Domestic Council Committee on "Right to Privacy" - chaired by, then, Vice-President Gerald Ford - recommended that initial privacy initiatives should focus on the Federal Government and that Federal example and experience in this complex field should precede directives covering non-Federal governmental and private sectors. The same conclusion was also reached by the U. S. Congress in the course of developing the Privacy Act of 1974, which is now public law. The state and local governments, as well as the private sector, were specifically omitted from that legislation. In addition, a Privacy Protection Study Commission was authorized to assess the need for increased regulation of these organizations. This was done as a very positive step partly because the potential for invasion of privacy and the range of people covered was much greater at the Federal level, partly because the subject was so complex, and partly from a recognition that the impact on business and local government could be substantial. We consider this a very prudent judgment.

Atlantic Richfield Company supports strongly the principles of personal privacy, especially as they are stated in the Ware Committee Report. The deliberation behind the Privacy Act of 1974 led to what we considered to be a viable approach to the subject. This approach stresses the need to gain experience in applying personal privacy legislation to a specific portion of the public sector before attempting to develop such legislation for the private sector.

The reasoning behind this approach is that the potential for invasion of privacy by the government is much greater than by private business. Of necessity, the government is involved in activities which require accumulation of sensitive personal data. Efforts to minimize the cost of government have also encouraged interagency exchange of information. Further, the purposes for gathering the data are both operational, to perform a specific function (such as, paying unemployment) and regulatory, (to ensure that no violation of the law occurs). Therefore, the desire of one governmental agency to access the files of another can be quite strong, especially in carrying out the regulatory aspects of various Federal laws. By contrast, the existence and content of a data file in the business world is usually known by the individual, and interchange with other companies is limited not only by existing governmental regulation, but by competitive conditions and economics.

A data file in the business world ordinarily has a single purpose, such as paying dividends to stockholders, and the cost of accessing the file (for other than its normal operation) restricts such accesses to those which can be justified economically. Further, there is no economic incentive for providing to the operators of one data file, say a stockholder records group, information available in another data file such as a lease royalty holder's file.

If legislation such as A.B. 3338 had to be applied to Atlantic Richfield on a Company-wide basis, it could greatly increase the probability that the "right to privacy" could be compromised rather than protected. An example could involve a typical Company employee who has employment records, medical records, a thrift plan account, a credit card account, is a stockholder and could have records in several other files, each of which are widely dispersed in the Company and serve a specific business purpose. Although a major expenditure would be required, regulation such as A.B. 3338 would probably force the Company to bring together all this information in one central location in order to make it available to the data subject, to control access, and to provide the mandated records and controls on input and disclosure. As any expert could testify, there is no way that a person with adequate knowledge and incentive could be prevented from gaining access to this information, once it is aggregated in a central location.

Atlantic Richfield Company does not have the kind of centralized data control center which compliance with disclosure, notification and file access provisions would necessitate. With the present system of widely dispersed files, each business function retains only that information about an individual that is needed for its own operation.

Although the bulk of the records including personnel files are in Los Angeles, Atlantic Richfield Company records on production leaseholds (for paying royalties) are in Dallas, stockholder records are in Los Angeles, credit card records are in Atlanta, and employment records are widely dispersed. The potential for exposure of any significant amount of personal data is very limited because of this geographic dispersal. If forced to centralize these files in order to comply with provisions such as those contained in A.B. 3338, this very important privacy protection feature is destroyed.

Another major problem would relate to use of service organizations. As an example, Atlantic Richfield Company does not handle its own credit card billing. This is performed for the Company by a service bureau in Atlanta. While this is unique in the petroleum industry, the concept of using service bureaus for file processing is quite common in business, especially in small businesses. Doctors, for example, are regular users of such services for billing, and many small businesses have their payrolls handled by service bureaus. The complications involved in developing legislation to cover the personal privacy aspects of service bureau operations, also suggest a go-slow attitude in applying such legislation to the private sector.

From study of just a few major systems which could be defined as containing personal data, it has been found that the cost would be in the millions of dollars if the provisions of A.B. 3338 were to be applied to the entire Company. This assumes that it is actually technically feasible to comply with it as written, although this assumption is open to question. However, there is no question that application of the proposed legislation to the private sector would require major changes in business systems and procedures, and these changes increase rather than decrease the possibility for unauthorized access to personal data maintained in data files.

In summary, Atlantic Richfield Company supports the principles of personal privacy and has taken strong steps internally to ensure that Company operations are carried on with these principles in mind. At the same time, the Company views

attempts to impose these principles on the private sector at this time through legislation as costly and potentially operationally counterproductive. Too little is known at this stage, by anyone, about operational impact of personal privacy legislation versus its effectiveness.

We strongly recommend that A.B. 3338 be changed to exclude its application to the private sector by eliminating any reference to "Organization" in this legislation. Atlantic Richfield Company supports the principles advocated to HEW by the Ware Committee; but much more research is needed, such as that authorized by the Privacy Act of 1974, in order to identify the problems and the needs so that legislation is properly balanced.

Atlantic Richfield Company, therefore, advocates that personal privacy legislation be limited in application to selected agencies in the public sector, and that any attempt to apply it to the private sector be deferred until further experience is gained with that type of legislation.

There does not seem to be a need for immediate action which would justify the very substantial risk created by hasty implementation of personal privacy legislation covering private business. The result could be a substantial increase in business operating costs, which will eventually get passed on to the consumer, a strong possibility that the legislation will increase rather than decrease opportunitites for unauthorized access to personal information, and a real danger that the legislation could have a disastrous effect on small businesses.

7/14/75

Attachment

BASIC PRINCIPLES OF INDIVIDUAL "RIGHT TO PRIVACY"

(From Ware Committee Report - July, 1973
U.S. Department of Health, Education and Welfare)

- There must be no personal data recordkeeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- 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.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any 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 the data.

Statement of Senator William V. Musto regarding Senate Bill 3178 ("Right to Privacy and Fair Information Practices Act"), presented to the Senate Judiciary Committee at a public hearing held August 11, 1975

The legislation that you are considering today is very timely, and the problem to which it is addressed is a very urgent one. That problem arises from the alarming possibilities inherent in modern data-processing techniques. It is now possible to store a great quantity of data in a very small space, and to retrieve it in a very short time; to correlate, for whatever purpose desired, separate items gathered at widely separated times and places and, it may be, for very different purposes. Perhaps even more ominous is the ease and rapidity with which the computer, abetted by the xerox machine, can reproduce and disseminate the information entrusted to it.

Of course, it is a commonplace to say that technology, in itself, is neutral -- a commonplace that has been applied to every potentially dangerous invention or discovery from flint-and-steel to the atomic bomb.

It must not be forgotten that modern information technology has also an enormous potentiality for social benefit. Such technology increases our ability to identify, analyze and understand conditions, problems and opportunities. It enables us to make more accurate and efficient decisions as to the allocation of resources. Fundamental to all such benefits is a general broadening of the data base; the technology now enables us to make sense out of vast conglomerations of data which in

years gone by would have been too unwieldy for accurate and systematic manipulation by unaided human capacity.

Appetite keeps pace with digestion. The more data we can usefully employ, the more we seek, gather and record. From this enormously increasing appetite for information, conflict arises; for the individual from whom, and about whom, the information is sought tends to resent, as we all do, inquiries that seem to pry into his personal affairs. He will recognize the rights of an employer, a lender, a tax collector and such persons to have certain questions truthfully answered; but there are limits, and those limits need to be defined.

We also become more dependent upon our data systems in the making of decisions -- both general decisions as to governmental or corporate policy, and particular decisions affecting the rights, obligations and benefits of individuals. This dependency has its good side: the more hard facts we can bring to bear in a systematic and accurate fashion, the more likely are we to make correct decisions. But there is a corresponding risk; for if we depend upon the analytical machinery, we must be sure, first, that the data we put into it and retain in it are accurate and complete, and second, that the analytical criteria programmed into the system are valid. Otherwise, we may not only make errors, but we may also commit injustices.

The sponsors of this legislation that you have before you have accurately perceived that safeguards must be erected against

the indiscriminate and uncontrolled employment of data systems. With that premise I can agree, and I suppose we all can. But between a laudable purpose and a well-worked-out piece of legislation there are, as you know, many intermediate steps, some of them rather tricky, and not a few pitfalls. This is especially true of legislation such as this, which is innovative. I think we can identify some areas in which additional work is needed on the bill before you.

In general, this bill shows some of the marks of that excessive enthusiasm which is not uncommon in first attempts to deal legislatively with newly perceived evils upon which a great deal of attention and alarm have been directed without having come to a clear focus. There are broad and sweeping definitions, designed to identify the areas where control is needed, but too broad for the purpose; powers of control and enforcement are granted in a large, unspecified manner; procedural requirements are excessively elaborate.

First, let us consider the enforcement mechanism set up in sections 18 through 23 of the bill. There is established a commission, to be known as the "Commission on Privacy, Freedom of Information and Public Information." It will consist of five members, unpaid, serving staggered three-year terms, appointed by the Governor with the advice and consent of the Senate. It is specified that no more than three of the members may be of one political party. To comply with the Constitution, this Commission

is allocated to the Department of Law and Public Safety, but, as section 18 goes on to say, "notwithstanding said allocation, the commission shall be independent of any supervision or control by the department or by any board or officer thereof."

One signal indication of enthusiasm for a new program is to set up a new and independent agency for its administration. There can be various reasons for this, the most common of which fall under the general rubric of keeping the program "out of politics." In this case, no doubt, it was thought that, inasmuch as all the established departments of government are involved in the use of data systems, it would be advisable to keep the overall supervision of data systems out of the direct chain of command in any department.

So the bill provides for a pro-forma compliance with Article IV, Section IV, paragraph 1, while arranging for its violation in practice. We might, for a moment, reflect upon the wisdom, born of experience, which led to the inclusion of that provision in our 1947 Constitution. Experience showed that the proliferation of "independent" boards and commissions did not, in fact, keep "politics" out, but merely complicated the political considerations tremendously, while obfuscating the assignment of responsibilities upon which democratic decision-making depends.

Furthermore, what is the point in establishing a non-political commission and then requiring that one party shall always have a majority on it?

Section 18 specifies that the dominant party shall never have more than a one-vote majority on the five-member commission. It will never be less, either, you may be sure.

It might have been more consistent to adopt the arrangement of the Election Law Enforcement Commission, which is a four-member board split evenly between the two major parties. But that brings up a recurrent dilemma: when the membership is evenly divided, there is the danger of deadlock; when unevenly, there is the danger of partisanship.

In any case, the Commission will have discharged most of its responsibilities when it has appointed a full-time executive director, legal counsel and hearing officers. These non-tenured officers will do most of the work, assisted by a staff of classified Civil Service personnel.

I might point, out, parenthetically, that the role of the "hearing officers" provided for in section 19 is not clearly defined. I assume, in view of the unpaid status of the commissioners, that the actual work of conducting hearings will fall upon these officers, with the commissioners merely reviewing and approving their findings. The bill itself, however, does not clarify this. The existence of the hearing officers is provided for, but their duties are not specified; section 20 provides that it shall be the "duty of the commission" to hold hearings and to impose penalties or order the cessation of "unfair information practices," and that findings of fact "made

by the commission" shall be conclusive.

For all practical purposes, it appears that the executive director might have been appointed directly by the Governor, without the mediation of the commission, and might have exercised himself the rule-making an other powers assigned to that body. He is only one person, to be sure; but a majority of one may be as effectively 1-0 as | 3-2. And inasmuch as there is a provision for automatic review by the Superior Court of the commission's "final" decisions, a larger body does not seem to be needed as a safeguard against arbitrary exercise of power.

There are, however, a couple of arbitrary powers apparently accorded to the commission which deserve comment.

First, section 20, in giving the commissioner the duty to hold hearings on complaints of "unfair information practices," not only empowers it to order the discontinuance of such practices, but also empowers it to "impose penalties where appropriate." What penalties? What is the meaning of "appropriate"?

If we turn back to the penalty sections of the bill, sections 16 and 17, we find two classes of penalty, civil and criminal. Section 16 provides criminal penalties. They apply only to individual "employees" of data-gathering organizations or agencies, and they provide for fines of up to $1,000 and imprisonment of up to one year. In section 17, organizations, private or governmental, that violate the provisions of the act are declared to be liable for nominal, actual and punitive damages

to "any individual aggrieved"; and the same section also enables such an individual, or the commission, to apply for an injunction against the unfair practices complained of.

It seems to me that the language of these penalty sections clearly requires judicial, not administrative, action. The commission may in some cases appear before the court on behalf of the aggrieved individual; but it does not appear to have any authority to impose any of these penalties on its own initiative.

I return to the original question: What are the "appropriate penalties" contemplated in section 20? Either the phrase means nothing at all, or it is a clue to the disappearance of an administrative penalties section which has dropped out of the bill draft, or it is an attempt to delegate a vague and extensive punitive power to the commission.

Another arbitrary power seems to be granted under subsection c. of section 15, which deals with exemptions from the provisions of the bill. The subsection states: "An agency or organization may be exempted from any provision of this act by a showing of need to the commission, if such need is required by the public's interest or by law."

I can discern no adequate guidelines to what is meant by "the public's interest" in this context.

Control over exemptions from the coverage of the bill may be of some importance by reason of the broad way in which that coverage is laid on to begin with.

The bill applies to any "data system" maintained by any "agency" or "organization." Under the series of definitions in section 2, an "agency" is any arm of State or local government, and an "organization" is any other entity, including an individual; while a "data system" is any means of collecting, storing and using "personal information." And "personal information" is, to quote in full, "any information that identifies or describes any characteristics of an individual, including, but not limited to, his education, financial transactions, medical history, 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."

Now these various definitions are by no means selective. Suppose, for example, that I, finding myself short of lunch money, borrow five dollars from a friend, promising to repay it the next morning. To be sure I don't forget, I make a little note of it, and put it in my wallet next to the bill.

Now observe that, under subsection i of section 2, I, as an "individual," am, ipso facto, an "organization." I have recorded information "that identifies or describes any characteristics of an individual, including ... financial transactions." To do so, I have made use of my note pad and pencil as a recording device, and my wallet as a receptacle

for data storage; all of which are the "total components and operations, whether automated or manual, by which personal information . . . is collected, stored, processed, handled or disseminated by an agency."

(Actually, as we have seen, I am, as an individual, an "organization," not an "agency." But I believe the omission of the latter term in subsection c., as just quoted, is probably an oversight or misprint.)

Now, by writing out that little memorandum and tucking it into my wallet, I have established and maintained a "data system" within the meaning of the bill. In doing so, I have committed a couple of "unfair information practices". To begin with, I have not held a public hearing as to the purpose and operation of this data system before I began the collection and maintenance of personal information in it. I should have done this, and given 30 days public notice of the hearing. (Section 3, subsection g.)

Furthermore, under subsection a. of section 3 I have committed another "unfair information practice" because a notice of the "existence and character" of my "data system" has not been published and filed with the commission, containing the several items of information specified in subsection c. of section 4.

Under section 17, I can be sued for a minimum of $1,000, regardless of the amount of actual damages (if any) and whether punitive damages are "appropriate" or not. The Commission on

Privacy, Freedom of Information and Public Information can haul me before it for a hearing and, pending that hearing, get out an injunction to prevent me from going on with this unfair information practice.

Whether I am liable to any criminal penalties is a more difficult question. Section 16 provides such penalties for "employees" of an "organization" only. From the definitions in section 1, subsection i., I know that I am an "organization", but whether I, as an individual, may be considered an "employee" of myself as an "organization" is an almost metaphysical question on which the terms of the bill offer no interpretive guidance.

Of course, you may say that the example I am analyzing is somewhat fanciful -- that no such stir will, in practice, be made over such a innocuous memorandum. But I think that a statute, or prospective statute, should be capable of being construed in accordance with the plain meaning of its own terms, without yielding such fanciful results.

Besides, we may easily conceive of less trivial examples. Every business has to keep many records which would come under the coverage of this act. Accounts payable, accounts receivable, payroll and personnel records -- all such basic records qualify for coverage under the act. Every business firm in the State, whether corporation, partnership or sole proprietorship would be compelled to publish notices, hold public hearings and provide a complete array of administrative safeguards and review procedures with respect to each such category of records.

Read sections 4 through 8 of this bill, and make the imaginative effort of visualizing the practical effects upon the business procedures of, say, a corner grocery store that handles numerous small charge accounts, or a free-lance carpenter or plumber with a long and fluctuating list of clients and suppliers.

Note, too, that while a small business run as a sole proprietorship or a partnership is an "organization" for purposes of what records it must keep, it (or each partner in it) is also legally an "individual" (or "individuals") entitled to the protection of record-keeping by others. If, for example, the free-lance carpenter purchases supplies from a supplier which is a partnership, his accounts payable contain "personal information," within the meaning of the act about the partners while their accounts receivable for the same transaction contain "personal information" relating to him. He and the supplier must comply with the provisions of the bill which are designed to protect each against the other.

Furthermore, even putting aside the obvious consideration that the procedures mandated by the bill are obviously ponderous and impracticable for all but government agencies and large corporations whose record-keeping is of an extensive nature, it seems to me that this bill concentrates too single-mindedly upon the proposition that "personal information" is, or ought to be, the personal property of the individual to whom it

pertains. But I do not think this can be legitimately said of the very broad definition of "personal information" that we find in subsection j. of section 2 of this bill. Broadly viewed, this bill seems to attempt to confer upon every individual a very sweeping power to prevent any other individual from making use of any information whatever that pertains to him -- with one significant exception, and that is the power retained by government to abrogate the individual's power for its own purposes. For example, subsection c. of section 3 states: "Each agency or organization shall obtain written consent of an individual prior to the maintenance or use of any data on such individual unless otherwise authorized by law." In other words, we tend toward the creation of a government-controlled monopoly upon information.

I think the right of non-governmental organizations and individuals to gather and use such information as they see fit ought to be subject only to the condition that they refrain from using such information to the damage of any individual. All prior restraints, established by government, over what data may be gathered seem to me to be inherently dangerous. They have the same relationship to the protection of privacy that government censorship would have to the prevention of libel. With respect to libel, our State Constitution provides that "Every person may freely speak, write and publish his sentiments on all subjects, being responsible for the abuse of that right."

I think a like principle applies to the protection of privacy -- that all persons should have a right to inquire and seek information, including personal information, being responsible, however, for any abuse of that right.

I think that there should be very severe penalties, and very strict liability, for any person or firm responsible for careless, incompetent or malicious use or transmittal of personal information which may damage an individual. But I do not think that elaborate legal restraints and procedures which introduce certain inhibiting hazards into all gathering of personal data are the best way of restraining the abuse of such data.

There are, as you know, numerous governmental and private agencies and organizations which gather certain personal information for the direct purpose of determining an individual's eligibility for benefits or liability to obligations -- from qualifying for welfare payments to setting credit limits or fixing insurance rates. In this particular type of data gathering I think there is one form of restraint that may appropriately be placed upon the gatherer -- namely, that, wherever practicable, such information should be gathered directly from the individual concerned, and, in any case, with his full knowledge of what information is being sought, from whom and for what purpose.

But to return to the bill which is actually before you, I

would summarize my objections by saying that it appears to be too ambitious, too broad in scope and insufficiently precise in its provisions. Its definitions are too general, its applicability too inclusive, and its procedures ponderous and impracticable. It needs considerable re-working to give precision, clarity and force to the valuable ideas upon which it is based.

common cause NEW JERSEY

28 WEST STATE STREET, RM. 910, TRENTON, NEW JERSEY 08605 ☐ 609•396-1150

STATEMENT ON S. 3178
BEFORE SENATE JUDICIARY COMMITTEE
BY WILLIAM S. SINGER, LEGAL AFFAIRS CHAIRMAN,
NEW JERSEY COMMON CAUSE

Common Cause welcomes the invitation of the Judiciary Committee to offer our observations on S. 3178. Although the reach of this bill does not fit squarely within the ambit of our legislative program, Common Cause must congratulate its sponsors for drafting and introducing this legislation. As individual citizens and as citizens organized to seek open, accountable government, we appreciate the bill's intention to free the flow of information.

S. 3178 focuses its scope on allowing individuals to learn the source and the quality of the information being collected, maintained and disseminated about them. It is particularly praiseworthy that the legislation covers not only government instrumentalities, but expands its coverage to private agencies distributing similar data on individuals. The sense and the need for including private organizations cannot be disputed.

Common Cause believes that permitting each individual to secure data on himself recognizes that in a properly functioning free society, individual action should not be prohibited or discouraged. One cannot depend on a sometimes awkward bureaucracy to protect a person's rights as diligently as the individual will. Furthermore, recourse to a more informal hearing before the Commission created by this bill, again allows individuals to act without resorting to a more cumbersome and costly court challenge.

Although Common Cause supports this legislation and would welcome its passage, S. 3178 does not satisfy fully the core issue. It is true that information collected and maintained on individuals should be available to those persons. Yet that sort of data comprises only one component of the desired goal of a full, free flow of information from government to its citizens. The federal government recently made strong strides in this direction in its passage of the Freedom of Information Act of 1974. We are only beginning to witness the full impact of that legislation on the national processes.

The New Jersey Legislature is now considering another bill which would offer citizens of New Jersey equal access to the information held by its government. Passage of A. 3133 would accomplish this goal. Although the direct ills sought to be cured by S. 3178 are not specifically treated in A. 3133, the bills are complementary. Both pieces of legislation propose to loosen the flow of information; both bills establish a commission to oversee the accomplishment of this goal (although it should be noted there is no appropriation for this commission in S. 3178). Certainly this committee should be impelled to consider both bills as part of a legislative scheme to meet the urgent need to treat this area. Certainly the committee should consider joining the two commissions as the range of their charges is almost identical. There is no reason why the bills could not be consolidated in a unified, rational legislative package.

Common Cause supports S. 3178. But Common Cause sees the bill as one component of a larger issue; an area which could be more fully and more decisively treated with more comprehensive legislation as A. 3133.

Mazuco

DEPARTMENT OF BANKING MEMORANDUM

From: CLIFFORD F. BLAZE, DEPUTY COMMISSIONER Date: August 6, 1975
DIVISION OF ADMINISTRATION & OPERATIONS
To: GAYL R. MAZUCO, RESEARCH ASSISTANT
SENATE JUDICIARY COMMITTEE, ROOM 219, STATE HOUSE

Re: S-3178

On July 15, 1975 you were informed that I would appear before your committee on August 11, 1975 to give this Department's feelings on the above captioned Senate Bill. You are advised that we have decided to submit this brief memorandum in lieu of appearing in person.

No doubt the committee will be made aware of the ambiguity and unnecessary pervasiveness of the subject bill by other persons. For this reason we have set forth only the two major debilities as they apply to this Department.

I. EXEMPTION

There are in the bill as now drafted certain exemptions which innure to "law enforcement agencies" which are agencies empowered by law to investigate and make arrests for violations of law. We believe that these sections should be amended to include certain functions undertaken by this Department.

More specifically, this Department is charged with the examination of financial institutions for soundness and safety. The examination reports which result are made confidential by statute. A section in these confidential examination reports deal with the competence of bank management and any suspected or discovered violations of law.

It would appear that the instant bill would cover the above. We submit that such a procedure could negate the effectiveness of this most important area of inquiry.

When our examiners discover evidence of a possible illegal practices, the proper law enforcement agencies are notified. Thus, we act as an investigative arm of these agencies. Therefore, we believe that this segment of our duties should have a similar exemption.

II. ADMINISTRATIVE PROBLEMS

The Committee will no doubt be told that the passage of the instant bill could well result in unbelievable administrative expense. We believe that the purposes of the bill do not justify the expense, at least as it applies to this Department.

Carrying out the ambiguous and pervasive terms and requirements of S-3178 could well necessitate or justify the hiring of two or three persons, not to mention the problems concerning the created paperwork and storage thereof.

For purposes of emphasis only, we call your attention to the following reductio ad absurdum. Paragraph 3c requires that we obtain written consent of an individual prior to the maintenance or use of any data on a person. Paragraph 1c defines a "data system" as including a person's name. Thus, before we could file a letter signed by or mentioning an individual we would have to have his written consent. However, the written consent would contain an individual's name which may well technically require a consent with a name which would ...." This never ending cycle can be compared to the mirrors on opposite walls in a barber shop.

In closing, our recitation of comment b above should be taken not as a belittling of the apparent intent of the bill, but one example supporting our position that the bill is so pervasive and unweildy as to make its application and effect burdensome not only on state agencies as our own, but upon any entity or individual who maintains any records which refer to another.

C.F.B.

CFB:bvv