

The original documents are located in Box 56, folder “Privacy - General (Includes House Republican taskforce report)” of the Philip Buchen Files at the Gerald R. Ford Presidential Library.

Copyright Notice

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Gerald R. Ford donated to the United States of America his copyrights in all of his unpublished writings in National Archives collections. Works prepared by U.S. Government employees as part of their official duties are in the public domain. The copyrights to materials written by other individuals or organizations are presumed to remain with them. If you think any of the information displayed in the PDF is subject to a valid copyright claim, please contact the Gerald R. Ford Presidential Library.

Some items in this folder were not digitized because it contains copyrighted materials. Please contact the Gerald R. Ford Presidential Library for access to these materials.

C.F.

FG 6-15-1

MEMORANDUM OF INFORMATION FOR THE FILE

DATE

10/8/76

LETTER, MEMO, ETC.

TO:

FROM:

SUBJECT:

Correspondence from Barry Roth's office dated Aug. 1974 - Aug. 1976 re the Domestic Council Committee on the Right of Privacy

Filed C.F. Overseize Attachment #257.

[Handwritten signature]



CORRESPONDENCE FILED CENTRAL FILES - CONFIDENTIAL FILE

OFFICE OF TELECOMMUNICATIONS POLICY
WASHINGTON

Phil,

You are probably in
the best position to appreciate
these concerns and
determine the proper
channels for action.

Charlie



OFFICE OF TELECOMMUNICATIONS POLICY

EXECUTIVE OFFICE OF THE PRESIDENT

WASHINGTON, D.C. 20504

August 9, 1974

ASSISTANT DIRECTOR

MEMORANDUM

FOR: Phil Buchan
FROM: Charles Joyce *CF*
SUBJECT: Privacy and Computers at the White House

The White House Computer Center (in the old EOB) presents some potential pitfalls as well as opportunities for President Ford in view of his close association with the privacy issue. These matters should receive early consideration.

A secure computer system was installed in the old EOB in 1971, primarily to meet national security requirements. However, it is available for all White House uses. I was designated White House Project Manager for the development and implementation of the system in 1969, and continued to serve in this capacity after moving to OTP in 1971. My role since then has been mainly to plan long term system growth and new uses, and to review and approve the allocation of project funds. Day to day operations are under the White House Communications Agency (WHCA).

Certain files have been put on this system by the White House which contain personal information. These are the Kardex and Presidential Contact files maintained by White House Central Files. These have been disclosed to the Ervin Committee. It would be easy to overlook the application of privacy safeguards to these files.

President Ford's contacts may already be entering these files. It might be wise for someone to review the need for, and contents of these files, so that a responsible and conscious decision can be made whether to continue them.

The desirability of keeping the White House Personnel Data Bank on a remote GSA computer should also be examined. This data bank contains a lot of personal information, and the

White House gets into it by calling up the computer through the telephone network. Security is therefore minimal and I think the system is a bad example from the privacy point of view. Moving it to the secure White House system would alleviate this problem.

Under the heading of opportunities there are uses of the computer which were considered but rejected in 1971 because they would only be useful if all Presidential material were included, and in 1971 this would have required a conversion of a three year backlog. For example, an automated index of Presidential statements would allow a rapid search of what the President has said on any subject, with literally thousands of key words as points of entry for the search. Applications like this are relatively painless when begun right away -- but involve massive problems once a backlog of manual files develops.

The desirability of an automated action status system should be reconsidered. A sophisticated system for this purpose has been in use by the NSC staff since 1971. It keeps track of hundreds of actions pending within the staff, as well as a record of decisions and an index to the documents related to them. I suggested a similar system to the White House Staff Secretary in 1972 but he was not interested.

While none of these new computer applications could be instituted overnight, some of them could be done within a few months, and actions could be taken right away to "capture" data in electronic form for later entry into an automated file system. There will be some cost involved for new applications development. Careful planning and attention to priorities is essential for success in this area.

I would be happy to be of assistance in these matters.



THE WHITE HOUSE
WASHINGTON

Eva:

Please send
copy to Doug &
put this in my
"privacy" file here.

my sent



THE WHITE HOUSE
WASHINGTON

Aug. 17

Mr. Buchen —

The public
comments on
your privacy
approach —

See attached.

Malt



Privacy

Telegram sent by the National Council of Jewish Women from the National office
on August 13, 1974:

The President
The White House
Washington, D.C.

WE WISH TO COMMEND YOU FOR YOUR STATEMENT IN YOUR ADDRESS TO THE JOINT
SESSION OF CONGRESS THAT YOU DESIRE TO LISTEN TO THE PEOPLE. WE AGREE
WITH YOU THAT IN A FREE SOCIETY THE CONSENT OF THE GOVERNED IS ESSENTIAL
TO THE DEVELOPMENT OF NATIONAL POLICY. THE NATIONAL COUNCIL OF JEWISH
WOMEN HAS AS ITS FIRST PROGRAM PRIORITY THE PROTECTION OF CONSTITUTIONAL
RIGHTS. YOUR STATEMENT ON INDIVIDUAL PRIVACY OFFERS GREAT HOPE AND
REASSURANCE TO US THAT OUR INDIVIDUAL RIGHTS WILL BE PROTECTED UNDER
YOUR LEADERSHIP. WE OFFER OUR UNEQUIVOCAL SUPPORT FOR YOUR EFFORTS "TO
PREVENT ILLEGAL INVASIONS OF PRIVACY IN BOTH GOVERNMENT AND PRIVATE
ACTIVITIES."

Mrs. Eleanor Marvin
National President
National Council of Jewish Women
One West 47th Street
New York, N.Y. 10036



Privacy

Monday 8/19/74

1:10 I checked with Tom about the memo from Bob Marik attaching the Memorandum for Federal Regional Council Chaimen. He sees no objection.



Talk with Larry Silberman 8/20

FOIA amendments

Privacy issues - Doug's authority

~~LSI~~

Functions of

Pres. Counsel:

- improper or illegal
- directions from WH

- mechanical



Doug Metz 8/20/74

THE WHITE HOUSE
WASHINGTON

Warrantless
wiretapping.

- letter by AG
instead from V-P

Criminal Justice
Priorities

- 1) ~~IRS~~ 1) FOA
- 2) IRS
- 3) Exec. Priv
(Erleborn)
- 4) Directions
- 5) re Committee
Target



Weather

Cloudy

Details on Page 6A

The Detroit News

AMERICA'S LARGEST EVENING CIRCULATION

THURSDAY, AUGUST 22, 1974

Finance

Pages 16D to 20D

Races

Pages 4, 5D

101st YEAR NO. 363

15 CENTS

FORD LIBRARY X-RT/PB

VA computer plan attacked as posing danger to privacy



Rep. John E. Moss

Copyright, 1974, The Detroit News
By SETH KANTOR
News Washington Bureau

WASHINGTON — President Ford has been asked to launch an investigation into charges that the Veterans Administration (VA) is preparing a \$50 million computer project that could threaten the private rights of millions of U.S. veterans.
Known as "Target System," the project is being put together without congressional approval, according to Rep. John E. Moss, D-

Calif., who alerted Mr. Ford in a letter last week about what he termed the dangers of the planned nationwide network.

Already under way is a \$600,000 Target System pilot contract, set up in Philadelphia by the VA without competitive contract bidding, in violation of federal regulations, Moss told the President.

Ralph E. Smith, general manager of Target System for the VA, told The Detroit News today he had reservations about a controversial decision to select IBM Corp. as the \$600,000 pilot

project contractor, without any bidding for the job that could lead to millions of dollars worth of future Target System contracts.

"There should be no sole-source procurement in government, anywhere," said Smith. "It's not healthy."

Smith also said "there will be no guarantees" that Target System will have enough safeguards to protect veterans from any "wholly evil man" who wants to yank personal information on them from computer files that could link up to

the data files at the Departments of Defense and Health, Education and Welfare (HEW).

Moss warned the President that the VA is putting together "what has become a governmentwide phenomenon — widespread, unauthorized data acquisition by agencies." Moss said, "this is the last policy we dare allow agencies to institutionalize, no matter how well motivated they may be . . . after what the nation has just passed through."

Earlier this year, Moss and his former House colleague, Mr. Ford, were instrumental in

killing FEDNET, a \$100 million interagency computer project planned by the General Services Administration (GSA).

As vice-president, Mr. Ford became chairman of a new Cabinet-level group known as the Right of Privacy Committee, which he still heads.

The Ford committee, along with a coalition of House and Senate committees, acted swiftly to kill FEDNET after Moss unearthed it four months ago.

(Continued on Page 11A)

PRIVACY



UP-126

(VETERAN INFORMATION)

WASHINGTON (UPI) -- REP. JOHN MOSS, D-CALIF., TODAY DISCLOSED HE HAS ASKED PRESIDENT FORD TO INVESTIGATE A COMPUTERIZED INFORMATION-SWAPPING SYSTEM PLANNED BY THE VETERANS ADMINISTRATION, SAYING IT CONSTITUTES A THREAT TO PERSONAL PRIVACY.

MOSS TOLD FORD IN A LETTER THE VA'S PROPOSED "TARGET SYSTEM," A \$50 MILLION COMPUTERIZED NETWORK THAT WOULD LINK THE 20 MILLION VETERANS RECORDS IN 59 FIELD OFFICES, WOULD BE SIMILAR TO A SYSTEM KNOWN AS FEDNET WHICH FORD AND OTHERS HAVE VIGOROUSLY OPPOSED.

"MY HOPE IS THAT YOU WILL INSTITUTE AN IMMEDIATE PROBE OF TARGET SYSTEM FOLLOWED BY INTENSIVE SCRUTINY OF WHAT OTHER AGENCIES PLAN IN THIS SENSITIVE AREA," MOSS SAID IN THE LETTER, A COPY OF WHICH HE MADE AVAILABLE TO UPI.

MOSS SAID THE VA WAS GOING AHEAD WITH ITS PROCUREMENT OF COMPUTER EQUIPMENT FOR TARGET SYSTEM WITHOUT AUTHORITY FROM CONGRESS OR OTHER SUPERVISORY FEDERAL AGENCIES TO DO SO. HE SAID ITS ONLY APPROVAL HAD COME FROM THE GENERAL SERVICES ADMINISTRATION, WHICH ALSO INITIATED AND PLANNED THE CONTROVERSIAL FEDNET SYSTEM.

THE VA HAS RECEIVED APPROVAL FROM CONGRESS AND THE OFFICE OF MANAGEMENT AND BUDGET ONLY TO CONDUCT A PILOT TEST OF CERTAIN PARTS OF THE TARGET SYSTEM.

VA OFFICIALS, HOWEVER, HAVE REPORTEDLY TOLD COMPUTER SUPPLIERS IN APRIL THAT ORDERS FOR THE FULL SYSTEM EQUIPMENT WAS ONLY "ABOUT NINE MONTHS AWAY".

UPI 05-22 04:11 PED

UP-127

THE WHITE HOUSE

WASHINGTON

August 27, 1974

To: Jerry terHorst

From: Phil Buchen

P.W.B.

Here is the memorandum for the President's consideration when you meet with him this morning and an extra copy for you. The proposal is in accord with my brief discussion with the President on August 24. It has been cleared with Geoff Shepard of the Domestic Council and a copy has gone to General Haig, as well as Dick Burress for communication to Mr. Rockefeller's staff.



THE WHITE HOUSE
WASHINGTON

August 27, 1974

To: Dick Burress

From: Phil Buchen *P.W.B.*

The President is expected to approve this proposal when he meets with Jerry terHorst at 10 a. m., and it will probably be announced at today's press briefing.

If you think you should advise Mr. Rockefeller's representative of the nature of this proposal as it would affect the new Vice President, please do so.

Attachment



August 30, 1974

MEMORANDUM FOR: Bill Timmons

FROM: Phil Buchen

SUBJECT: Proposed response by President
to Chairman Rodino's letter of
August 14.

As a suggested followup to your letter to Chairman Rodino dated August 20, 1974, I attach proposed draft of a letter for the President to sign.

Attachment

PWBuchen:ed

ALD R. FO

YRABUJ
DR

Dear Mr. Chairman:

Thank you for your thoughtful letter of August 14. I am heartened by your pledge to work seriously at cooperation and conciliation in striking a constructive balance between protection of personal privacy and the responsibility of the Congress and the Executive branch to protect the national security.

Consistent with my remarks to the Congress on August 12, I am taking every opportunity to urge that the officers of the Executive branch be open and positive in their relations and communications with the Congress in a manner that is consistent with our joint interest in national security and the public's interest in knowing about the decision-making processes of their government. Accordingly, I am sending copies of our correspondence to the Attorney General asking him to consider carefully your assessment of past relationships between the Justice Department and the Committee on the Judiciary.

You know of my respect for the work of the Committee as it endeavors to legislate in the complex but important field of individual rights and privacy. Be assured of my continuing commitment to progress in this area.

Best personal regards,

President



DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY

WASHINGTON, D.C. 20504

August 29, 1974

To: Phil Buchen
From: Doug Metz *Doug*
Subj: Response to Chairman Rodino

Attached is a draft reply to the
Chairman. Urge that the President reply
personally.

Attachment



August 29, 1974

Dear Mr. Chairman:

This will acknowledge and thank you for your August 14 letter to the President. I would like to assure you that it will be called to his attention without delay.

As you know, during his Vice Presidency, he addressed himself to the matter of the individual rights of Americans in the area of privacy. I am certain your offer of assistance will mean a great deal to him as he follows through on his commitment to pursue tough laws to prevent the illegal invasion of privacy in both Government and private activities.

With best regards,

Sincerely,

/s/ Bill

William E. Timmons
Assistant to the President

The Honorable Peter W. Rodino, Jr.
Chairman
Committee on the Judiciary
House of Representatives
Washington, D. C. 20515

bcc: w/incoming to Philip Buchen for further ACTION and
reply as appropriate.

WET:EF:VO:ckb



PETER W. RODINO, JR. (N.J.) CHAIRMAN

HAROLD D. DONOHUE, MASS.
 JACK BROOKS, TEX.
 ROBERT W. KASTENMEIER, WIS.
 DON EDWARDS, CALIF.
 WILLIAM L. HUNGATE, MO.
 JOHN CONYERS, JR., MICH.
 JOSHUA EILBERG, PA.
 JEROME R. WALDIE, CALIF.
 WALTER FLOWERS, ALA.
 JAMES R. MANN, S.C.
 PAUL S. SARBANES, MD.
 JOHN F. SEIBERLING, OHIO
 GEORGE E. DANIELSON, CALIF.
 ROBERT F. DRINAN, MASS.
 CHARLES B. RANGEL, N.Y.
 BARBARA JORDAN, TEX.
 RAY THORNTON, ARK.
 ELIZABETH HOLTZMAN, N.Y.
 WAYNE OWENS, UTAH
 EDWARD MEZVINSKY, IOWA

EDWARD HUTCHINSON, MICH.
 ROBERT MC CLORY, ILL.
 HENRY P. SMITH III, N.Y.
 CHARLES W. SANDMAN, JR., N.J.
 TOM RAILSBACK, ILL.
 CHARLES E. WIGGINS, CALIF.
 DAVID W. DENNIS, IND.
 HAMILTON FISH, JR., N.Y.
 WILEY MAYNE, IOWA
 LAWRENCE J. HOGAN, MD.
 M. CALDWELL BUTLER, VA.
 WILLIAM S. COHEN, MAINE
 TRENT LOTT, MISS.
 HAROLD V. FROELICH, WIS.
 CARLOS J. MOORHEAD, CALIF.
 JOSEPH J. MARAZITI, N.J.
 DELBERT L. LATTA, OHIO

Congress of the United States
 Committee on the Judiciary
 House of Representatives
 Washington, D.C. 20515

GENERAL COUNSEL:
 JEROME M. ZEIFMAN
 ASSOCIATE GENERAL COUNSEL:
 GARNER J. CLINE
 COUNSEL:
 HERBERT FUCHS
 HERBERT E. HOFFMAN
 WILLIAM P. SHATTUCK
 H. CHRISTOPHER NOLDE
 ALAN A. PARKER
 JAMES F. FALCO
 MAURICE A. BARBOZA
 FRANKLIN G. POLK
 THOMAS E. MOONEY
 MICHAEL W. BLOMMER
 ALEXANDER B. COOK
 CONSTANTINE J. GEKAS
 ALAN F. COFFEY

August 14, 1974

The Honorable Gerald R. Ford
 President of the United States
 The White House
 Washington, D.C.

Dear Mr. President:

BT
 I would like to express my personal congratulations on your very fine remarks before the Joint Session of Congress last Monday evening. I want to take special note of your remarks regarding the individual rights of Americans in the area of privacy.

We are all aware of the importance of moral leadership in the delicate and difficult efforts to strike a meaningful balance between the constitutionally protected privacy of individuals and the responsibility of the executive and legislative branches of government to protect personal and national security.

I am impressed and inspired by your pledge.

A great number of the subjects which fall under the general heading of individual rights and privacy are of course within the jurisdiction of the House Committee on the Judiciary. We have been at work for some months, in some cases years, endeavoring to legislate many facets of the subject of privacy. In our efforts, we have found a reluctance at times on the part of the Department of Justice to confer and compromise in some areas relating to criminal justice information systems and other areas of individual privacy. We have experienced past reluctance on the part of the F. B. I. to share information, even on a confidential basis, with our oversight subcommittee.

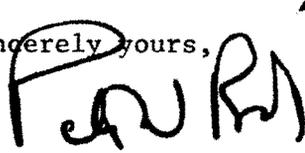
Let me respond to your remarks with my pledge to seriously work at cooperation and conciliation of the



differing points of view in this immensely complicated but important sphere. We ask no more in return.

With kindest personal regards, I remain

Sincerely yours,

A handwritten signature in black ink, appearing to read "P. Rodino, Jr.", with a small superscript "1" above the final letter.

PETER W. RODINO, JR.
CHAIRMAN

PWR:pm



U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

WASHINGTON, D.C. 20515

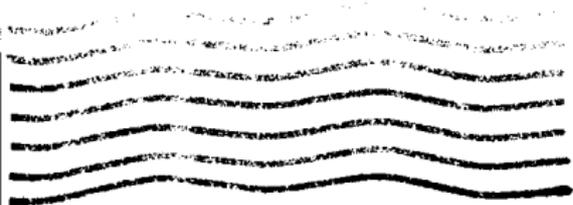
OFFICIAL BUSINESS

Pete W. Rodino

M. C.



The Honorable Gerald R. Ford
President of the United States
The White House
Washington, D. C.



9/6/74

To: Doug Metz

From: Phil Buchen

For further handling.
Thanks so much.



August 27, 1974

Dear Barry:

This will acknowledge and thank you for your August 22 letter to the President with which you forwarded the report of the Republican Task Force on Privacy of the House of Representatives.

As you know, this is a subject which the President has asked be carefully studied and recommendations submitted to him. I know that he will be most appreciative of your report and I will make certain that he receives it without delay.

With warm regards,

Sincerely,

William E. Timmons
Assistant to the President

The Honorable Barry M. Goldwater, Jr.
House of Representatives
Washington, D. C. 20515

~~See. w/~~incoming to Philip Buchen for further handling.
Consideration of Presidential reply or reply on behalf
of the President.

WET:EF:VO:vo



14
BARRY M. GOLDWATER, JR.
9TH DISTRICT OF CALIFORNIA

COMMITTEE ON INTERSTATE
AND FOREIGN COMMERCE
COMMITTEE ON SCIENCE AND
ASTRONAUTICS

Congress of the United States
House of Representatives

Washington, D.C. 20515
August 22, 1974

8-26
WASHINGTON OFFICE:
LONGWORTH HOUSE OFFICE BUILDING
(202) 225-4461

SAN FERNANDO VALLEY OFFICE:
23241 VENTURA BOULEVARD
WOODLAND HILLS, CALIFORNIA
(213) 883-1233

VENTURA COUNTY OFFICE:
OXNARD
(805) 485-7777

SANTA CLARITA VALLEY OFFICE:
(805) 255-6595

end
BT
The Honorable Gerald R. Ford
The President
The White House
Washington, D. C. 20500

Dear Mr. President:

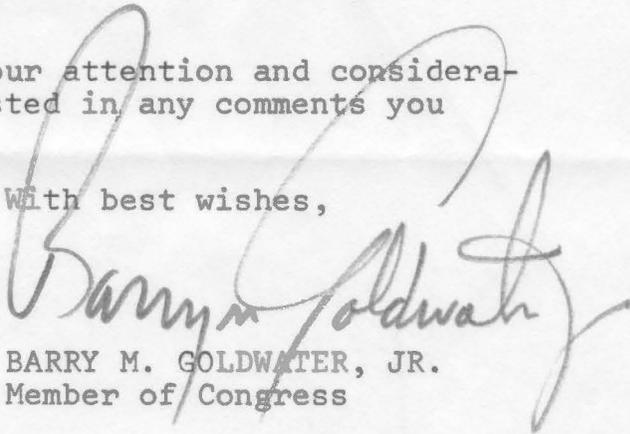
It is a distinct pleasure for me as Chairman of
the Republican Task Force on Privacy of the House
of Representatives to forward you a copy of the
initial task force report.

As I am sure you are aware, major legislation is
being considered by both Houses of Congress and
Republican initiative has been a strong factor in
this effort, as have the activities of your Committee
on Privacy.

This task force report is a first for either major
national party, and is fully in keeping with the
traditional high standards set by the Republican
party.

I commend the report to your attention and considera-
tion, and would be interested in any comments you
might wish to make on it.

With best wishes,


BARRY M. GOLDWATER, JR.
Member of Congress

BMG:jp
Enclosure



DOMESTIC COUNCIL COMMITTEE
ON THE RIGHT OF PRIVACY

WASHINGTON, D.C. 20504

DISTRIBUTION TO:

P. W. Buchen	<hr/>
A. H. McCarty	<hr/> ✓ <hr/>
D. W. Metz	<hr/> — <hr/>
D. Milanowski	<hr/> ✓ <hr/>
J. K. Miller	<hr/> ✓ <hr/>
C. W. Parsons	<hr/> ✓ <hr/>
G. B. Trubow	<hr/> ✓ <hr/>



Republican Research Committee

Republican Conference

U.S. House of Representatives

Washington, D.C. 20515

August 21, 1974

Dear Republican Colleague:

Attached are the recommendations of the Task Force on Privacy, chaired by Barry M. Goldwater, Jr., and Vice-chaired by Alan Steelman and Tennyson Guyer. Other Members of the Task Force are John Conlan, Charles Thone, Jack Kemp, Peggy Heckler, Andrew Hinshaw, Frank Horton, Charles Mosher, Bob Lagomarsino, John Rousselot, and Keith Sebelius.

These recommendations are a landmark in the area of individual rights. Nowhere has the total question of privacy been so well or thoughtfully covered. Nowhere has the human equation in our technological society been so strongly expressed.

The Research Committee is proud to have approved this report. These recommendations and the follow-up legislative efforts will ensure that the 1984 envisioned by George Orwell will remain only fictional.

The Task Force and its staff, especially Joe Overton, are to be commended for the time, effort and excellence of the product.

Most sincerely,



Lou Frey, Jr.

LFJr/hph

Attachments



HOUSE REPUBLICAN RESEARCH COMMITTEE

Recommendations of Privacy Task Force

August 21, 1974

The House Republican Research Committee has approved the following recommendations of the Task Force on Privacy which deal with the following areas:

Government Surveillance.....	Page 2
Federal Information Collection.....	Page 3
Social Security Numbers/ Standard Universal Identifiers.....	Page 4
Census Information.....	Page 4
Financial Information.....	Page 5
Consumer Reporting.....	Page 5
School Records.....	Page 6
Juvenile Records.....	Page 7
Arrest Records.....	Page 8
Medical Records.....	Page 9
Computer Data Banks.....	Page 9
Code of Ethics.....	Page 10



HOUSE REPUBLICAN RESEARCH COMMITTEE

Recommendations of the House Republican Task Force on Privacy

The House Republican Task Force on Privacy believes that the right to privacy is an issue of paramount concern to the nation, the public and the Congress. Recently publicized incidents of abuses have begun to focus attention on this long neglected area. Public awareness must be heightened and the legislative process geared up to address the full range of problems posed by the issue.

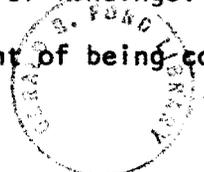
Modern technology has greatly increased the quantity and detail of personal information collection, maintenance, storage, utilization and dissemination. The individual has been physically by-passed in the modern information process. An atmosphere exists in which the individual, in exchange for the benefit or service he obtained, is assumed to waive any and all interest and control over the information collected about him. On the technical and managerial levels, the basic criteria in many decisions relating to personal information practices are considerations of technological feasibility, cost-benefit and convenience. The right to privacy has been made subservient to concerns for expediency, utility and pragmatism.

The trend in personal information practices shows no signs of abating. Twice as many computer systems and seven times as many terminals - particularly remote terminals - will be in use by 1984 as are in use today. And, with each federal service program that is initiated or expanded, there is a geometrically proportionate increase in the quantity and detail of personal information sought by the bureaucracy. The theory is that the broader the information base, the more efficient and successful the administration of the program.

Such a situation demands the attention of Congress and of the American public. The computer does not by definition mean injury to individuals. Its presence has greatly contributed to the American economy and the ability of government to serve the people. Under present procedures, however, the American citizen does not have a clearly defined right to find out what information is being collected, to see such information, to correct errors contained in it, or to seek legal redress for its misuse. Simply put, the citizen must continue to give out large quantities of information but cannot protect himself or herself from its misappropriation, misapplication or misuse. Both government and private enterprise need direction, because many of their practices and policies have developed on an isolated, ad hoc basis.

The House Republican Task Force on Privacy has investigated the following general areas involving the investigation and recording of personal activities and information: government surveillance, federal information collection, social security numbers and universal identifiers, census information, bank secrecy, consumer reporting, school records, juvenile records, arrest records, medical records, and computer data banks. These inquiries have resulted in the development of general suggestions for legislative remedies. Each statement is accompanied by a set of findings.

All findings and recommendations are presented with the intent of being consistent with these general principles:



1. there should be no personal information system whose existence is secret;
2. information should not be collected unless the need for it has been clearly established in advance;
3. information should be appropriate and relevant to the purpose for which it has been collected;
4. information should not be obtained by illegal, fraudulent, or unfair means;
5. information should not be used unless it is accurate and current;
6. procedures should be established so that an individual knows what information is stored, the purpose for which it has been recorded, particulars about its use and dissemination, and has the right to examine that information;
7. there should be a clearly prescribed procedure for an individual to correct, erase or amend inaccurate, obsolete, or irrelevant information;
8. any organization collecting, maintaining, using, or disseminating personal information should assure its reliability and take precautions to prevent its misuse.
9. there should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent;
10. the Federal Government should not collect personal information except as expressly authorized by law ; and
11. that these basic principles apply to both governmental and non-governmental activities.

Each recommendation of the Task Force seeks to contribute to a broader, more intelligent, viable understanding of the need for a renewed concern for personal privacy. An awareness of personal privacy must be merged with the traditional activities of the free marketplace, the role of government as a public servant, and the need for national security, national defense, and foreign affairs.

Surveillance

The Task Force is deeply disturbed by the increasing incidence of unregulated, clandestine government surveillance based solely on administrative or executive authority. Examples of such abuses include wiretapping, bugging, photographing, opening mail, examining confidential records and otherwise intercepting private communications and monitoring private activities. Surveillance at the federal level receives the most publicity. However, state and local government, military intelligence and police activities also must be regulated.

The Fourth Amendment of the Constitution clearly specifies "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." The First Amendment guards against abridgement of the rights of free speech, free press, and assembly for political purposes. The Fourteenth Amendment states that none of a citizen's rights may be taken from him by governmental action without the due process of law.

The direct threat to individual civil liberties is obvious in those cases in which a person is actually being monitored, but even more alarming is the "chilling effect" such activities have on all citizens. A person who fears that he will be monitored may, either subconsciously or consciously, fail to fully exercise his constitutionally guaranteed liberties. The mere existence of such fear erodes basic freedoms and cannot be accepted in a democratic society.

The various abuses of discretionary authority in the conduct of surveillance provide ample evidence that current safeguard mechanisms do not work. Procedures allowing the executive branch to determine whether a surveillance activity is

proper or not pose certain conflict of interest questions.

A degree of controversy surrounds the question of the authority of the President to initiate electronic surveillance without the safeguards afforded by court review. Present law is clear on this point: the Omnibus Crime Control and Safe Streets Act of 1968 lists those specific crimes in connection with which electronic monitoring may be instituted and requires that court approval be obtained in these cases. However, dispute has arisen over Executive claims of Constitutional prerogatives to implement wiretaps for national security purposes. The Supreme Court has ruled that, if such prerogative exists, it does not apply to cases of domestic surveillance unrelated to national security. The Court has not yet ruled on the constitutionality of national security wiretaps unauthorized by a court. Cases are pending before the courts at this time which raise this issue. The Task Force agrees with the movement of the Judiciary to circumscribe unauthorized wiretaps and hopes it will proceed in this direction.

The Task Force feels that surveillance is so repugnant to the right to individual privacy and due process that its use should be confined to exceptional circumstances. The Task Force further feels that no agent of federal, state, or local government should be permitted to conduct any form of surveillance, including wiretapping of U.S. citizens in national security cases, without having demonstrated probable cause and without having obtained the approval of a court of competent jurisdiction. The Task Force recommends enactment of new legislation to prohibit the unauthorized surveillance by any means, and further recommends that existing laws be clarified to the extent this may be necessary to ensure that no agent of the government, for any reason, shall have the authority to conduct any surveillance on any American citizen for any reason without first obtaining a court order.

The Task Force believes that this proposal would not lessen the capability of the government to protect and defend the American people, but would go a long way toward assuring the individual citizen that his constitutional rights will not be abridged by government without due process of law.

Federal Information Collection

Recently, there has been a pronounced increase in federal data and information collection. Over 11.5 million cubic feet of records were stored in Federal Records Centers at the beginning of FY 1973. Accompanying this increase has been a rise in the potential for abuse of federal information collection systems.

The Federal Reports Act of 1942 was enacted to protect individuals from overly burdensome and repetitive reporting requirements. The agency entrusted with the responsibility for implementing the Act has ignored the legislative mandate and failed to hold a single hearing or conduct any investigations. With the exception of the Bureau of the Census and the Internal Revenue Service, there are few restrictions on the collection or dissemination of confidential information compiled by federal agencies.

The Task Force recommends that the Office of Management and Budget immediately begin a thorough review and examination of all approved government forms and eliminate all repetitive and unnecessary information requirements.

Legislation setting down clear guidelines and spelling out restrictions is needed to protect the individual from unrestricted and uncontrolled information collection. Individuals asked to provide information must be apprised of its intended uses. Individuals supplying information which will be made public must be notified of that fact at the time the information is collected or requested. Public disclosure (including dissemination on an intra- or inter-agency basis) of financial or other personal information must be prohibited to protect the privacy of respondents.

Returning the use of the Social Security Number (SSN) to its intended purpose (i.e. operation of old-age, survivors, and disability insurance programs) is a necessary corollary to safeguarding the right of privacy and curtailing illegal or excessive information collection.

The use of the Social Security Number has proliferated to many general items including state driver licenses, Congressional, school and employment identification cards, credit cards and credit investigation reports, taxpayer identification, military service numbers, welfare and social services program recipients, state voter registration, insurance policies and records and group health records.

There are serious problems associated with the use of the SSN as a standard universal number to identify individuals. A standard universal identifier (SUI) will relegate individuals to a number; thereby, increasing feelings of alienation. The SSN's growing use as an identifier and filing number is already having a negative, dehumanizing effect upon many citizens. In addition, the use of a SUI by all types of organizations enables the linking of records and the tracking of an individual from cradle to grave. This possibility would negate the right to make a "fresh start", the right of anonymity, and the right to be left alone, with no compensating benefit.

A well-developed SUI system would require a huge, complex bureaucratic apparatus to control it and demand a strict system of professional ethics for information technicians. The technology needed to protect against unauthorized use has not yet been adequately researched and developed. A loss, leak or theft would seriously compromise a system and official misappropriation could become a political threat. The following Congressional action is needed:

1. legislation should be enacted that sets guidelines for use of the SSN by limiting it to the operation of old-age, survivors, and disability insurance programs or as required by federal law;
2. any Executive Orders authorizing federal agencies to use SSN's should be repealed, or alternatively, reevaluated and modified;
3. legislation should be enacted restricting the use of the SSN to well-defined uses, and prohibiting the development and use of any type of SUI until the technical state of the computer can ensure the security of such a system. At that time, a SUI system should have limited applicability and should be developed only after a full congressional investigation and mandate; and
4. new government programs should be prohibited from incorporating the use of the SSN or other possible SUI. Existing programs using the SSN without specific authorization by law must be required to phase out their use of the SSN. State and local governmental agencies, as well as the private sector, should follow this same course of action.

A review should be conducted of the Internal Revenue Service in both its collection and dissemination policies. Leaks must be ended. The need for stricter penalties for unauthorized activities should be reviewed.

Census Bureau

The greatest personal data collection agency is the Bureau of Census. Created to count the people in order to determine congressional districts, this agency has mushroomed into a vast information center which generates about 500,000 pages of numbers and charts each year.

Under penalty of law, the citizen is forced to divulge intimate, personal facts surrounding his public and private life and that of the entire family. These answers provide a substantial personal dossier on each American citizen. The strictest care must be taken to protect the confidentiality of these records and ensure that the information is used for proper purposes.

The Census Bureau sells parts of its collected data to anyone who wishes to purchase such information. Included are all types of statistical data that are available on population and housing characteristics. As the questions become more detailed and extensive, broad-scale dissemination becomes more threatening and frightening. When used in combination with phone directories, drivers' licenses and street directories, census data may enable any one interested to identify an individual. Therefore, it is vitally important that rules and regulations governing the access to and dissemination of this collected data be reviewed, clarified and strengthened.

Legislation is needed to guarantee the confidentiality of individual information by expanding the scope of confidentiality under existing law and by increasing the severity of punishment for divulging confidential information. These provisions should be specifically directed at the officers and employees of the Bureau of Census, all officers and employees of the Federal government and private citizens who wrongfully acquire such information. In addition, the Bureau of the Census must use all available technological sophistication to assure that individuals cannot be inductively identified.

Financial Information

On October 26, 1970, sweeping legislation known as the Bank Secrecy Act became law. The Act's intention was to reduce white collar crime by making records more accessible to law enforcement officials. However, in accomplishing its purpose, it allowed federal agencies to seize and secure certain financial papers and effects of bank customers without serving a warrant or showing probable cause. The Act's compulsory recordkeeping requirements, by allowing the recording of almost all significant transactions, convert private financial dealings into the personal property of the banks. The banks become the collectors and custodians of financial records which, when improperly used, enable an individual's entire life style to be tracked down.

The general language of the Act allowed bureaucrats to ignore the intent of the law and neglect to institute adequate privacy safeguards. The Supreme Court affirmed this approach by upholding the constitutionality of both the law and the bureaucratic misinterpretation of it.

Congress must now take action to prevent the unwarranted invasion of privacy by prescribing specific procedures and standards governing the disclosure of financial information by financial institutions to Federal officials or agencies. Congress must enact legislation to assure that the disclosure of a customer's records will occur only if the customer specifically authorizes a disclosure or if the financial institution is served with a court order directing it to comply. Legislation must specify that legal safeguards be provided requiring that the customer be properly notified and be provided legal means of challenging the subpoena or summons.

Passage of such legislation would be an important step forward in reaffirming the individual's right to privacy.

Consumer Reporting

The consumer reporting industry, through its network of credit bureaus, investigative agencies, and other reporting entities is in growing conflict with individual privacy. Most Americans eventually will be the subject of a consumer



report as a result of applying for credit, insurance, or employment. The problem is one of balancing the legitimate needs of business with the basic rights of the individual.

Consumer reports fall into two categories. First, there are the familiar which contain "factual" information on an individual's credit record such as where accounts are held and how promptly bills are paid. 100 million consumer reports are produced each year by some 2600 credit bureaus.

The second ones go beyond factual information to include subjective opinions of the individual's character, general reputation, personal characteristics, and mode of living. These are often obtained through interviews with neighbors, friends, ex-spouses and former employers or employees. An estimated 30 to 40 million such reports are produced annually.

The first Federal attempt at regulating the collection and reporting of information on consumers by third-party agencies came in 1970 with the enactment of the Fair Credit Reporting Act (FCRA). In theory, the Act had three main objectives: to enable consumers to correct inaccurate and misleading reports; to preserve the confidentiality of the information; and to protect the individual's right to privacy.

The specific safeguards provided by the FCRA are: A consumer adversely affected because of information contained in a consumer report must be so notified and given the identity of the reporting agency. The consumer is entitled to an oral disclosure of the information contained in his file and the identity of its recipients. Items disputed by the consumer must be deleted if the information cannot be reconfirmed. The consumer may have his version of any disputed item entered in his file and included in subsequent reports.

The FCRA needs to be strengthened in two major areas: disclosure requirements and investigative reports. The individual should be entitled to actually see and inspect his file, rather than rely on an oral presentation. Further, he should be allowed to obtain a copy of it by mail (the consumer is often geographically distant from the source of the file). Users of consumer reports should be required to specifically identify the information which triggered any adverse action.

The FCRA protects the sources used in investigative reports. The Task Force believes that this is contrary to the basic tenets of our system of justice and that the information source must be revealed upon the subject's request. Furthermore, the Task Force recommends that advance written authorization be required from any individual who is the subject of an investigative report for any purpose.

School Records

The recent increase in popular awareness of the seriousness of the privacy issue has been accompanied by an increase in the general concern over loose, unstructured and unsupervised school recordkeeping systems and associated administrative practices. There has also been general discussion about what information should be kept on a child and considered part of his or her "record". Parents are frequently denied access to their own child's record, or are prohibited from challenging incorrect or misleading information contained in his file. At the same time, incidents of highly personal data being indiscriminately disseminated to inquirers unconnected with the school system are not uncommon.

Remedial measures are available to the Congress in the form of legislative actions. The sanctions under which such provisions would operate, however, are the key to their effectiveness. The Task Force proposes the Congress adopts as a general policy the rule that federal funds be withheld from any state or local educational agency or institution which has the policy of preventing parents from inspecting, reviewing, and challenging the content of his or her child's school record. Outside access to these school records must be limited so that protection of the student's right to privacy is ensured. It is recommended that the release of such identifiable personal data outside the school system be contingent upon the written consent of the parents or court order.

All persons, agencies, or organizations desiring access to the records of a student must complete a written form indicating the specific educational need for the information. This information shall be kept permanently with the file of the student for inspection by parents of students only and transferred to a third party only with written consent of the parents. Personal data should be made available for basic or applied research only when adequate safeguards have been established to protect the students' and families' rights of privacy.

Whenever a student has attained eighteen years of age, the permission or consent required of and the rights accorded to the parents should be conferred and passed to the student.

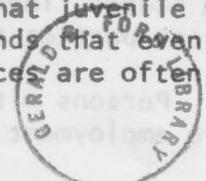
Finally, the Secretary of HEW should establish or designate an office and review board within HEW for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions set forth by the Congress.

Juvenile Records

The Task Force supports the basic philosophy underlying the existence of a separate court system for juvenile offenders, which is to avoid the stigmatizing effect of a criminal procedure. The lack of confidentiality of such proceedings and accompanying records subverts this intent and violates the individual's basic right of privacy.

Most states have enacted laws to provide confidentiality. Yet the Task Force finds that due to a lack of specific legislation, and contrary to the intent of the juvenile justice system, the individual's right of privacy is often routinely violated. Juvenile records are routinely released to the military, civil service, and often to private employers as well. This occurs in cases in which the hearing involves non-criminal charges, in cases of arrest but no court action, in cases in which the individual is no longer under the jurisdiction of the juvenile court, and in cases where his file has been administratively closed.

Legislation governing the confidentiality of juvenile court and police records varies widely from state to state. Only 24 states control and limit access to police records, therefore enabling a potential employer who is refused access to court records to obtain the information from the police. Only 16 states have expungement laws providing for the destruction of such records after a specified period of good behavior. Only 6 states make it a crime to improperly disclose juvenile record information. And, one state, Iowa, in fact provides that juvenile records must be open to the public for inspection. The Task Force finds that even in those states whose laws provide adequate protection, actual practices are often inconsistent with legislation.



Many new questions about confidentiality, privacy and juvenile rights are being raised, and the Task Force finds that the establishment of safeguards has lagged significantly behind technological developments. For example, presently no state has enacted legislation regulating the use of computers in juvenile court; as a rule, each system establishes its own guidelines for data collection, retention, and distribution.

The Task Force finds that with the use of computers, the juvenile's right to privacy is additionally threatened by the increased accessibility to his record and therefore increased possibility of misuse. Staff carelessness, less than strict adherence to rules of limited access, and electronic sabotage must now be added to the existing threats to the juvenile's right to privacy.

The Task Force recommends the establishment of minimum federal standards for state laws to include the following provisions:

1. all records of the juvenile court and all police records concerning a juvenile shall be considered confidential and shall not be made public. Access to these records shall be limited to those officials directly connected with the child's treatment, welfare, and rehabilitation;
2. dissemination of juvenile records, or divulgence of that information for employment, licensing, or any other purpose in violation of statutory provisions shall be subject to a criminal penalty;
3. to protect the reformed delinquent from stigma continuing into his adult life, provisions should specify a procedure for either the total destruction or the sealing of all juvenile court and police investigative and offender records at the time the youth reaches his majority, or when two years have elapsed since he has been discharged from the custody or supervision of the court. Subsequent to this expungement, all proceedings and records should be treated as though they had never occurred and the youth should reply as such to any inquiry concerning his juvenile record; and
4. all police records on juveniles arrested but where no court action was taken should be systematically destroyed when the incident is no longer under active investigation.

The Task Force recommends the enactment of legislation specifically prohibiting federal agencies from requesting information relating to juvenile record expungement from employment applicants or from requesting such information from the courts or the police.

The Task Force further recommends the cessation of all federal funding for computerized systems which contain juvenile records unless it can be demonstrated that these systems provide adequate safeguards for the protection of the juvenile's right of privacy. These standards must fulfill all the requirements of the minimum standards for state legislation previously enumerated, including special provisions to strictly limit data accessibility.

Arrest Records

A large percentage of arrests never result in conviction. Yet, in over half the states, individual's arrest records are open to public inspection, subjecting innocent parties to undue stigma, harrassment, and discrimination.

Persons with arrest records often find it difficult, if not impossible to secure employment or licenses. A study of employment agencies in the New York City

area found that seventy-five percent would not make a referral for any applicant with an arrest record. This was true even in cases in which the arrest was not followed by a trial and conviction. This is just one example of the widespread practice of "presumption of guilt" based on the existence of an arrest record.

The Task Force holds that release of information about arrests not followed by conviction is a direct violation of the individual's right of privacy. It therefore recommends that legislative efforts be directed toward:

1. establishing minimum standards for state laws calling for the automatic sealing of all individual arrest records which were not followed by conviction and which are no longer under active investigation;
2. requiring the FBI to seal arrest records not followed by conviction; and
3. prohibiting inclusion of arrest records not followed by conviction on computerized systems involving more than one state or using federal funds.

Medical Records

Medical records, which contain sensitive and personal information, are especially in need of privacy safeguards to maintain basic trust in the doctor-patient relationship. Yet, development of automated data processing systems has enhanced the ability of government and private organizations to store, analyze and transfer medical records. Increasingly, this occurs without the individual's knowledge or consent. Abuse of such information systems can have a deleterious effect on doctor-patient relations.

To guarantee the privacy of medical records, the Task Force recommends that:

1. the federal government provide dollar grants and incentives to States for the voluntary adoption and execution of State plans to insure the right to privacy for computerized medical information systems. Such a plan would place principal responsibility on the States, giving the federal government the right to set minimum standards;
2. Congress review the recently enacted Professional Standards Reviews Organizations (PSRO) legislation. There are increasing numbers of reports and complaints regarding Review Board uses of medical files and the threat this poses to privileged, confidential doctor-patient relationships; and
3. provisions be included in national health insurance legislation which specifically ensure the individual's privacy. The institution of a national health insurance plan will create a vast medical information network which will require stringent safeguards to prevent abuses of the patients' right to privacy.

Computer Data Banks

The use of the computer has brought great commercial and social benefits to modern America. Greater reliance on the computer, however, increases its integration into all aspects of daily life. The result is increased vulnerability to abuse or misuse of computerized information.

The Task Force finds that the individual possesses inadequate remedies for the correction of such abuses. In fact, the Task Force considers it probable that many abuses have gone unreported simply because the individual involved did not know of the data being collected about him.

Even if the individual is aware that data is being collected about him, he faces several obstacles if he wishes to expunge purely private information or to correct erroneous information. Among his obstacles are the following: the lack of statutory support for legal action (except in the credit reporting area), the cost of litigation, and even fear of retaliation by the company or agency being challenged.

Despite their potential for abuse, data banks remain an inescapable fact of life in a society growing more complex and more technological. The Task Force does not oppose data banks as such, but favors strong safeguards against their misuse, and recommends that:

1. rights under the Fair Credit Reporting Act of 1970 be extended to all data collection. The individual must have and be informed of his right to review information contained in any collection of data about himself (excluding national security and criminal justice files);
2. Congress establish categories (i.e. in-depth biographical, financial, medical, etc.) of information which may not be included in reports on an individual unless the individual knowingly gives his uncoerced consent;
3. limited exceptions be granted for national security and criminal justice investigations;
4. criminal and civil penalties be established for any use of statistical data (collected for collective analysis) to wrongfully acquire information on individuals;
5. transfer of personal information between governmental agencies be strictly limited;
6. the creation of a centralized Federal data bank (except for national security and criminal justice purposes) be prohibited; and
7. a federal "privacy protection agency" be established to enforce the proposed legislation.

Code of Ethics and Standard of Conduct

The Republican Task Force on Privacy believes there to be a definite need for the development of a universal code of ethics and standard of conduct for the technical, managerial and academic personnel involved in the development and use of personal information systems. The Task Force regards this to be essential for the automated and computerized information systems. Personal information systems are becoming an integral aspect of the daily life of every individual in our society. This sensitive relationship demands and merits the development of an attitude of professionalism. It is recognized that some efforts have been made to develop and foster such attitudes. But, the information industry as a whole has not supported such efforts as a matter of policy. The Task Force declares its commitment to the development of a professional standard of conduct and code of ethics for the persons involved in the development, maintenance, management and use of personal information systems.

Conclusion

The Task Force is aware that this is a relatively new area of concern. Some recommendations may go too far and some not far enough. Some areas may have been overlooked. But there is no question that now is the time to address ourselves to this important and far reaching issue. If we fail--George Orwell's 1984 may become a reality by 1976.

Bibliography

- Breckenridge, Adam Carlyle. The right to privacy. Lincoln, University of Nebraska Press, 1970.
- Canada. Department of Communication and the Department of Justice. Privacy and computers. A report of a task force established jointly by the Canadian Department of Communication and the Department of Justice. Ottawa, Canada, Information Canada, 1972.
- Campaigne, Howard and Lance J. Hoffman. Computer privacy and security. Computers and automation, v. 22, July 1973.
- Cashman, Charles E. Confidentiality of juvenile court proceedings: A review. Juvenile Justice, v. 24, August 1973.
- Cohen, Richard E. Justice report/hearings focus on privacy, limitations on use of FBI data. National Journal reports, Feb. 16, 1974.
- Computer applications in the juvenile justice system, National Council of Juvenile Court Judges, 1974.
- Countryman, Vern. The diminishing right of privacy: The personal dossier and the computer. Texas Law Review, May 1971.
- Curran, William J., et. al. Protection of privacy and confidentiality. Science, v. 182, Nov. 23, 1973.
- De Weese, J. Taylor. Giving the computer a conscience. Harper's, Nov. 1973.
- Gotlieb, Calvin. Regulations for information systems. Computers and automation, v. 19, Sept. 1970.
- Gough, Aidan R. The expungement of adjudication records. Washington University Law Quarterly, 1966.
- Hunt, M.K. and Rein Turn. Privacy and security in data bank systems: an annotated bibliography. 1969-1973. R-1044-NSF. Santa Monica, Calif., Rand Corp., 1974.
- Hoffman, Lance J. Security and privacy in computer systems. Los Angeles, Calif., 1973.
- Hoglund and Kahan. Invasion of privacy and the freedom of information act: Geman v. NLRB, 40 Geo Washington Law Review, 1972.
- Koehn, E. Hank. Privacy, our problem for tomorrow. Journal of systems management, v. 24, July 1973.
- Kraning, Alan. Wanted: new ethics for new techniques. Technology review, v. 70, Mar. 1970.



- Kuhn, David. Your life: how private? Reprint from Minneapolis Tribune, Oct. 7-12, 1973 by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation, Washington, D.C.
- Lapidus, Edith J. Eavesdropping on trial. Rochelle Park, New Jersey, Hayden Book Co., 1974.
- Levin, Eugene. The future shock of information networks. Astronautics and aeronautics, Nov. 1973.
- Lusky, Louis. Invasion of privacy: a clarification of concepts. Columbia Law Review, v. 72.
- Miller, Authur R. The assault on privacy: computers, databanks, and dossiers. Ann Arbor, University of Michigan Press, 1971.
- Miller, Herbert S. The closed door. U.S. Dept. of Labor, 1972.
- National Committee for Citizens in Education. Children, parents and school records. Columbia, Md., National Committee for Citizens in Education, 1974.
- Organisation for Economic Co-operation and Development. Toward central government computer policies. OECD Information Studies, 1973.
- Pennock, J. Roland and John W. Chapman. Privacy. New York, Atherton Press, 1971.
- Privacy in the First Amendment. The Yale Law Journal, June 1973.
- Project Search Staff. Committee on Security and Privacy. Security and privacy considerations in criminal history information systems. Technical Report No. 2. Sacramento, Calif., Project Search. California Crime Technological Research Foundation, July 1970.
- Ralston, Anthony G. Computers and democracy. Computers and automation, v. 22, april 1973.
- Reed, Irving S. The application of information theory to privacy in data banks. Santa Monica, Calif., Rand Corp., 1973.
- Rule, James B. Private lives and public surveillance. London, Allen Lane, 1973.
- Sargent, Francis W. Centralized data banks - where public technology can go wrong. Astronautics and aeronautics, v. 11, Nov. 1973.
- Schrag, Peter. Dossier dictatorship. Saturday Review, April, 17, 1971.
- Social Security Administration. Social Security Number Task Force: Report to the Commissioner. Department of Health, Education and Welfare, 1971.
- Springer, Eric W. Automated medical records and the law. Pittsburgh, Aspen Systems Corporation, 1971.
- Stone, Michael and Malcolm Warner. The data bank society: organizations, computers, and social freedom. London, George Allen and Unwin LTD, 1970.

- Thomas, Uwe. Computerized data banks in public administration. Paris, France, Organization for Economic Co-operation and Development, 1971.
- Turn, Rein. Privacy and security in personal information databank systems. Prepared for the National Science Foundation. R-1044-NSF. March 1974. Santa Monica, Calif., Rand Corp., 1974.
- U.S. Congress. House. Committee on Government Operations. Federal information systems and plans -- Federal use and development of advanced technology. Hearings before the Subcommittee on Foreign Operations and Government Information. 93rd Cong. 1st and 2d session, Washington, U.S. Govt. Printing Office, 1973, 1974.
- U.S. Congress. Senate. Committee on the Judiciary. Federal data banks, computers and the Bill of Rights. Hearings before the Subcommittee on Constitutional Rights. 92nd Cong. 1st session, Washington, U.S. Govt. Printing Office, 1971.
- U.S. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. Records, computers, and the rights of citizens. Washington, U.S. Govt. Printing Office, 1973.
- Westin, Alan F. and Michael A. Baker. Databanks in a free society: computers, record-keeping, and privacy. Report of the Project on Computer Databanks of the Computer Science and Engineering Board. National Academy of Science. New York, Quadrangle Books, 1972.
- Wheeler, Stanton. On record: files and dossiers in american life. New York, Russell Sage Foundation, 1969.



NEWS...

From Congressman **BARRY GOLDWATER, JR.**

27th District - California

FOR IMMEDIATE RELEASE

10 a.m.

8/21/74

PRIVACY TASK FORCE ISSUES

REPORT AND RECOMMENDATIONS

1423 Longworth House Office Building, Washington, D.C. 20515

Washington (8/21/74)-----The Task Force on Privacy, chaired by Congressman Barry M. Goldwater, Jr. (R-Ca) today issued its comprehensive recommendations during a press conference in the Nation's Capitol.

"For many years," stated Goldwater, "we have witnessed the increased pervasive use of the Social Security number for unlimited purposes, as well as the intense use of the computer in data collection. This has resulted in unprecedented abuse of the 4th Amendment in far too many cases. We have the tools and the opportunity to restore personal privacy and individual rights, and I am very hopeful the report issued today, with its specific recommendations, will provide the final impetus for the entire Congress to pass the legislation many of my colleagues and I have introduced to correct the serious problems that exist."

Goldwater listed important recommendations made in the report:

*No agent of government should be permitted to conduct any form of surveillance without demonstrating probable cause and without obtaining prior approval of a federal court.

*When an individual supplies information which will be made public, he must be notified of that fact at the time the information is collected or requested.

*The use of the Social Security number should be restricted to well-defined areas

* The development and use of any type of standard universal identifier should be prohibited

*The application of the Bank Secrecy Act should be limited

*Parents must have full access to their children's school records, but outside access to these records must be severely limited

Goldwater concluded by stressing the need for a strict code of ethics and standard of conduct for all technical, academic and managerial personnel involved in the development and use of personal information.

Vice Chairmen of the Task Force were Reps. Alan Steelman and Tennyson Guyer. Other members were Reps. John Conlan, Jack Kemp, Robert Lagomarsino, Margaret Heckler, Andrew Hinshaw, Frank Horton, Charles Mosher, John Rousselot, and Keith Sebelius.

Contact: Signy Ellerton (Washington) 202-225-4461

Jack Cox (California) 213-883-1233

9/74

Bushin file
Box 56
Privacy-General

The Privacy Report

Issued by Project on Privacy and Data Collection / American Civil Liberties Union Foundation
410 First Street, S.E. ■ Washington, D.C. 20003 ■ (202) 544-2026

Volume II, No. 2, September 1974

FREE SPEECH AND THE ZONE OF PRIVACY

By Robert E. Smith

As Oren Taylor watched TV in his home in Boise, Idaho, lying naked (as was his custom), there was a knock on the door. Police ordered him out on his porch, refused his pleas to let him get dressed, and arrested him on a firearms charge. Out of a ditch in front of the home came a local TV news man, with lights on and camera rolling. KTVB showed the naked Mr. Taylor on its news show the following day to 17,000 households in Idaho and eastern Oregon. Taylor's lawsuit against the station will go to trial this fall (Taylor v. KTVB, Inc., Civil No. 11345, Idaho Dist. Ct., Ada Co.).

The case symbolizes the frequent confrontation between the individual's right to privacy and others' First Amendment rights of free speech and free press. The conflict is not a new one; in fact the Warren-Brandeis law review article in 1890 that first articulated a legal right to privacy stemmed from press coverage of one of Mrs. Warren's parties that she considered an invasion of her privacy.

The privacy-First Amendment confrontation is manifest in new ways in the computer age, as government seeks to regulate private data collection that the data collectors sometimes regard as an expression of their free speech rights; as communities respond to privacy concerns by limiting commercial solicitation; as newsmen seek access to government files on individuals; and as news media themselves employ computer techniques in news gathering.

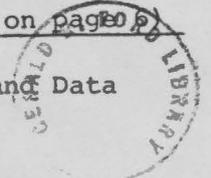
The Retail Credit Co., which maintains subjective data on some 50 million American citizens, has argued in a court challenge to its activities that its databanks are no more than an exercise of free speech and that state regulation of its databanks violates the First Amendment. The Supreme Court has often held that "purely commercial" speech, like libelous statements, obscenity and "fighting words," is not entitled to the full First Amendment protections of other speech. Calling computerized data collection "speech" may itself require a long stretch of the imagination. Still, the argument is made, and civil libertarians seeking to limit the types of information that consumer reporting firms or insurance companies may collect on individuals find themselves in the uncomfortable position of being censors.

In recent weeks, those drafting privacy legislation have partially exempted private data collection from the coverage of their bills, partly out of fear of censoring private fact-gathering. The latest draft of the Koch-

(Continued on page 6)

Robert E. Smith is associate director of the Project on Privacy and Data Collection of the American Civil Liberties Union.

Photocopy from Gerald R. Ford Library



IN THE COURTS

A mail cover placed on a New Jersey high school girl who wrote to the Socialist Workers Party as part of a class assignment was not an invasion of privacy, according to U.S. District Judge James A. Coolahan. The judge denied Lori Paton's motion for an injunction barring such FBI mail surveillance, as he earlier denied her motion for relief in behalf of a class of citizens similarly affected. The judge, however, ordered that an FBI file on Miss Paton be destroyed and, in a footnote, implied there was less cause for the police to maintain investigative files than arrest records (Paton v. LaPrade, No. 1091-73, D.N.J. Aug. 29, 1974). * * * In an amicus curiae brief, the ACLU Foundation has urged the Tenth Circuit Court of Appeals to allow Paul W. Polin's challenge to Dun & Bradstreet's credit reporting procedures to be heard on its merits, because credit reporting about an individual is often misleading, inaccurate, and indiscriminately disseminated (Polin v. Dun & Bradstreet, Inc., No. 74-1375). * * * A Fairfax County Circuit judge has dismissed an ACLU of Virginia suit against Virginia's law that citizens must provide a Social Security number for voter registration. The ACLU will now try federal court. * * * The U.S. Court of Appeals in the District of Columbia has ruled that a Washington man could be discharged by the Peace Corps when he refused to allow his employer access to his psychiatric records and to meet, without his attorney, with a government psychiatrist. Government investigators were concerned about admissions made during an interrogation concerning the employee's sex life (Anonymous v. Kissinger, No. 73-1141, July 5, 1974).

Generally, confessions that result from economic coercion are inadmissible against a defendant. But the Second Circuit Court of Appeals refused to allow this principle to protect an apprentice truck driver required to take a polygraph test administered by his employer at the request of and in the presence of the police. During the test, the man admitted a killing. His employer's threat not to hire him was hardly "substantial economic sanction" against a truck driver, said the court (Sanney v. Montanye, 43 U.S.L.W. 2028, June 20, 1974). * * * A divided Massachusetts Supreme Judicial Court, saying that lie detector evidence remains generally inadmissible, allowed polygraph evidence admitted in a case in which the defendant had agreed in advance to its use (Commonwealth v. A Juvenile (No. 1), 43 U.S.L.W. 2018, June 12, 1974).

Human Experimentation -- The U.S. Department of Health, Education, and Welfare has published proposed regulations to protect fetuses, abortuses and pregnant women, prisoners and the mentally disabled who are subjects of research involving risk (39 Fed. Reg. 30649, Aug. 23, 1974). Comments are due Nov. 21. The rules, supplementing previous regulations intended to protect all subjects generally (45 CFR 46.1), would require consent by the subject or responsible representative. Research programs would have to establish consent committees to qualify for federal assistance. Regulations affecting children as research subjects are now being drafted.

QUOTABLE

"Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery."

Samuel D. Warren, Louis D. Brandeis,
The Right to Privacy, 4 Harv. L. Rev.
5 (1890).

September 23, 1974

Dear Barry:

The President has requested me to comment on the Initial Report of the House Republican Task Force on Privacy, of which you have kindly sent the President a copy.

He also asked me to pass on his congratulations to you as Chairman and to the other members for an outstanding report. This concerted initiative -- a first for either party -- and the nonpartisan tenor of the report constitute a significant contribution to the bipartisan effort to further the right of privacy to all Americans.

As you know, the Domestic Council Committee on the Rights of Privacy, in which I have participated, is continuing its effort to foster new privacy initiatives. I know you will be interested in the enclosed comparison by Doug Metz of the Committee's initiatives with the recommendations of the Republican Task Force on Privacy. It is gratifying to see the extent of common concern and mutualty of objectives.

Best personal regards.

Most sincerely yours,

Phillip W. Bucher
Counsel to the President

Honorable Barry M. Goldwater, Jr.
House of Representatives
Washington, D. C. 20515



The Privacy Project

Project on Privacy and Data Collection / American Civil Liberties Union Foundation

410 First Street, S.E.

Washington, D.C. 20003

(202) 544-2026

September 26, 1974

DOUGLASS LEA
Director

ROBERT E. SMITH
Associate Director

SHARON E. BIEDERMAN
Administrative Assistant

TO READERS OF THE PRIVACY REPORT:

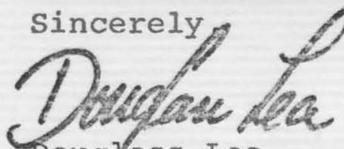
The Privacy Project will be terminated in October and The Privacy Report will cease publication -- unless we are able to raise sufficient funds to continue. Because of your interest in privacy, we are asking you to help us.

We estimate that we need \$15,000 immediately. The ACLU Foundation has been victimized by the financial crunch that has hit many institutions. This is particularly unfortunate at this time, because the need for a group like ours to monitor the government's increased data collection and to expose abuses of personal privacy, as we have done, is great. The current focus on this issue may fade if we are not able to make certain that citizens in every part of the nation continue to stand up for their individual rights of privacy.

Please notify groups or individuals able to make sizable grants to our project and then let us know about them.

Large or small donations from you, which are tax deductible, will make the difference between life and death for this project. Checks should be made payable to ACLU Privacy Project. We need to hear from you as soon as possible so that we will know whether the project can continue.

Sincerely



Douglass Lea
Director

Name _____

Address _____

Amount _____

Check here if you wish us to regard this as a subscription payment for the coming year: _____



The Privacy Report

Issued by Project on Privacy and Data Collection / American Civil Liberties Union Foundation
410 First Street, S.E. ■ Washington, D.C. 20003 ■ (202) 544-2026

Volume II, No. 2, September 1974

FREE SPEECH AND THE ZONE OF PRIVACY

By Robert E. Smith

As Oren Taylor watched TV in his home in Boise, Idaho, lying naked (as was his custom), there was a knock on the door. Police ordered him out on his porch, refused his pleas to let him get dressed, and arrested him on a firearms charge. Out of a ditch in front of the home came a local TV news man, with lights on and camera rolling. KTVB showed the naked Mr. Taylor on its news show the following day to 17,000 households in Idaho and eastern Oregon. Taylor's lawsuit against the station will go to trial this fall (Taylor v. KTVB, Inc., Civil No. 11345, Idaho Dist. Ct., Ada Co.).

The case symbolizes the frequent confrontation between the individual's right to privacy and others' First Amendment rights of free speech and free press. The conflict is not a new one; in fact the Warren-Brandeis law review article in 1890 that first articulated a legal right to privacy stemmed from press coverage of one of Mrs. Warren's parties that she considered an invasion of her privacy.

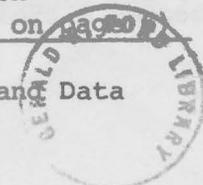
The privacy-First Amendment confrontation is manifest in new ways in the computer age, as government seeks to regulate private data collection that the data collectors sometimes regard as an expression of their free speech rights; as communities respond to privacy concerns by limiting commercial solicitation; as newsmen seek access to government files on individuals; and as news media themselves employ computer techniques in news gathering.

The Retail Credit Co., which maintains subjective data on some 50 million American citizens, has argued in a court challenge to its activities that its databanks are no more than an exercise of free speech and that state regulation of its databanks violates the First Amendment. The Supreme Court has often held that "purely commercial" speech, like libelous statements, obscenity and "fighting words," is not entitled to the full First Amendment protections of other speech. Calling computerized data collection "speech" may itself require a long stretch of the imagination. Still, the argument is made, and civil libertarians seeking to limit the types of information that consumer reporting firms or insurance companies may collect on individuals find themselves in the uncomfortable position of being censors.

In recent weeks, those drafting privacy legislation have partially exempted private data collection from the coverage of their bills, partly out of fear of censoring private fact-gathering. The latest draft of the Koch-

(Continued on page 3)

Robert E. Smith is associate director of the Project on Privacy and Data Collection of the American Civil Liberties Union.



A mail cover placed on a New Jersey high school girl who wrote to the Socialist Workers Party as part of a class assignment was not an invasion of privacy, according to U.S. District Judge James A. Coolahan. The judge denied Lori Paton's motion for an injunction barring such FBI mail surveillance, as he earlier denied her motion for relief in behalf of a class of citizens similarly affected. The judge, however, ordered that an FBI file on Miss Paton be destroyed and, in a footnote, implied there was less cause for the police to maintain investigative files than arrest records (Paton v. LaPrade, No. 1091-73, D.N.J. Aug. 29, 1974). * * * In an amicus curiae brief, the ACLU Foundation has urged the Tenth Circuit Court of Appeals to allow Paul W. Polin's challenge to Dun & Bradstreet's credit reporting procedures to be heard on its merits, because credit reporting about an individual is often misleading, inaccurate, and indiscriminately disseminated (Polin v. Dun & Bradstreet, Inc., No. 74-1375). * * * A Fairfax County Circuit judge has dismissed an ACLU of Virginia suit against Virginia's law that citizens must provide a Social Security number for voter registration. The ACLU will now try federal court. * * * The U.S. Court of Appeals in the District of Columbia has ruled that a Washington man could be discharged by the Peace Corps when he refused to allow his employer access to his psychiatric records and to meet, without his attorney, with a government psychiatrist. Government investigators were concerned about admissions made during an interrogation concerning the employee's sex life (Anonymous v. Kissinger, No. 73-1141, July 5, 1974).

Generally, confessions that result from economic coercion are inadmissible against a defendant. But the Second Circuit Court of Appeals refused to allow this principle to protect an apprentice truck driver required to take a polygraph test administered by his employer at the request of and in the presence of the police. During the test, the man admitted a killing. His employer's threat not to hire him was hardly "substantial economic sanction" against a truck driver, said the court (Sanney v. Montanye, 43 U.S.L.W. 2028, June 20, 1974). * * * A divided Massachusetts Supreme Judicial Court, saying that lie detector evidence remains generally inadmissible, allowed polygraph evidence admitted in a case in which the defendant had agreed in advance to its use (Commonwealth v. A Juvenile (No. 1), 43 U.S.L.W. 2018, June 12, 1974).

Human Experimentation -- The U.S. Department of Health, Education, and Welfare has published proposed regulations to protect fetuses, abortuses and pregnant women, prisoners and the mentally disabled who are subjects of research involving risk (39 Fed. Reg. 30649, Aug. 23, 1974). Comments are due Nov. 21. The rules, supplementing previous regulations intended to protect all subjects generally (45 CFR 46.1), would require consent by the subject or responsible representative. Research programs would have to establish consent committees to qualify for federal assistance. Regulations affecting children as research subjects are now being drafted.

QUOTABLE

"Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery."

Samuel D. Warren, Louis D. Brandeis,
The Right to Privacy, 4 Harv. L. Rev.
5 (1890).

The Ford Administration, like its predecessor, is resisting legislation that would limit White House access to personal income tax returns. The Internal Revenue Service similarly is trying to get its own house in order, to head off legislative restrictions of its operations.

Article II of the impeachment resolution voted by the House Judiciary Committee says of Richard Nixon: *He has, acting personally and through his subordinates and agents, endeavored to obtain from the Internal Revenue Service, in violation of the constitutional rights of citizens, confidential information contained in income tax returns for purposes not authorized by law, and to cause . . . income tax audits or other income tax investigations to be initiated or conducted in a discriminatory manner.*

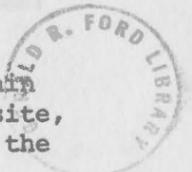
Sen. Lowell P. Weicker, R.-Conn., and Rep. Jerry L. Litton, D.-Mo., have introduced S. 3982 and H.R. 16602 to permit only the President personally to send for a tax return, naming the taxpayer, and then only with written justification to Congress. The Treasury Department is insisting that a Presidential executive order is adequate to curb the abuse cited in Article II. Meanwhile, IRS has circulated internal guidelines that require such White House requests to be in writing and channelled through the commissioner. The IRS guidelines also say it will respond to tax checks on prospective Presidential appointees with only notification as to whether a criminal tax investigation is pending.

Weicker and Litton are still trying to convince the House to go along with a Senate-passed amendment to the White House staff authorization bill that would accomplish the same purpose as S. 3982 and H.R. 16602.

The Weicker-Litton bill would also limit access to IRS returns to federal agencies with tax enforcement responsibilities. The Ford Administration this month proposed a weaker version that would allow four agencies, including Census and the Social Security Administration, to see personal tax returns, even for non-tax purposes. Among those resisting the tighter access provisions is Henry E. Petersen, who heads the criminal division at the Department of Justice. The Administration bill, unlike the Weicker-Litton measure, would not limit Congressional access to Form 1040.

IRS no longer informs the White House of so-called sensitive cases handled by district offices and henceforth will evaluate tips from informers about others' alleged tax violations at its national computer center, not at each district office, according to Commissioner Donald C. Alexander. And the service will design its new computer system to assure limited access to tax data, the commissioner promises. Alexander still thinks that taxpayer audits ought to be selected on the basis of machine screening and subjective decisions of IRS staff, and not subject to high-level centralized approval nor totally based on machine.

"The present tax code says that tax returns are public, with certain exceptions," noted Alexander, "when, in fact, it ought to say the opposite, that tax returns are confidential, with certain exceptions." On that, the Administration and Congressional critics agree.



Computer Dragnet -- When David E. Drew was stopped on a traffic violation in Quincy, Ill., last February, the police routinely ran his name through the FBI's computerized criminal history file of 420,000 individuals arrested for "serious" federal or state offenses. The FBI computer reported that Drew was wanted by the Marines as a deserter. He was jailed without bond, and the Marines requested, by letter, that he be detained. Drew, however, was released a few days later on a writ of habeas corpus. Drew explained to his attorney that in 1970 the Marine Reserves temporarily lost touch with him when as a reservist he changed addresses. Subsequently, he was rejected by the Selective Service System on the basis of a physical exam. Drew's reserve unit in El Paso said it had no record of Drew as being wanted; the Marine Corps Regional Office in St. Louis said all it knew about Drew was the FBI computer entry. Police in Quincy were aware of the bureaucratic mix-up and assured Drew he would no longer be arrested. But Drew did not feel safe about traveling outside of his hometown. On July 1, a military policeman arrested Drew, took him away from his family to detention at Camp Pendleton in Southern California. There he sat, until his records could be located. By this month, the Marines had agreed to discharge Drew. He has returned to Illinois and the FBI computer entry on him has been erased, after a seven-month ordeal.

No More "Fiche" -- The French government will no longer require hotels to turn over to the police daily forms with the name, address, profession, sex, identity number and signature of each new guest. As everyone suspected, the police have no time to read the more than one million "fiches" that pile up each month. The reforms do not yet apply to foreign travelers.

Drug, Alcohol Abuse -- Two federal agencies have proposed identical regulations on confidentiality of patient records in federally assisted drug and alcohol treatment programs. Hearings on the proposals will be held in October in 11 cities (39 Fed. Reg. 30426, Aug. 22, 1974). The regs allow disclosure of patient information with consent for various purposes and without consent for research, audits and evaluation. Patients would not have to disclose treatment information to prospective employers unless their addiction within the past three years caused unsatisfactory work performance. Deadline for comments is Nov. 4. * * * Earlier, the Drug Enforcement Administration of the Department of Justice proposed amendments to its recordkeeping requirements for narcotic treatment programs (39 Fed. Reg. 26424, July 19, 1974).

Privacy Push -- The Church of Scientology has adopted privacy as one of its major social campaigns. A worldwide sect, the church has exposed the international aspects of data collection (notably a report on Nazi influences in Interpol, the private affiliation of police officers). As a victim of Internal Revenue scrutiny, the church has also focused on IRS invasions of privacy and IRS refusals to make public its policies and procedures. The privacy effort is led by its National Commission on Law Enforcement and Social Justice, 5930 Franklin Ave., Los Angeles, Calif. 90028. * * * The National Council of Jewish Women plans to devote many of its local activities this fall to the privacy issue.

Subscribers are asked to send \$15 (\$5 for students) to defray the costs of publishing The Privacy Report. Contributions to the Privacy Project are tax-deductible and help the project to increase its monitoring of government and private data collection about individuals and to inform citizens of their rights to privacy.

A young woman wrote the following letter August 17 to Reuben Askew, Governor of Florida. The lawyer for the bank at which she sought employment wrote that her "apprehension over the polygraph examination of applicants is certainly misplaced" because it is "only one item in a battery of tests, interviews, and examinations which the banks apply in a uniform and indiscriminate manner to all applicants."

Dear Sir:

Upon applying for a job at Sun Bank of Pine Hills in Orlando, Florida, I was told that I would have to submit to a lie detector test. Refusal to submit will mean that you are not permitted employment at said organization! As a newcomer to the Orlando area, I was in need of a job. Therefore, much against all my beliefs in the American system, I took the lie detector test feeling very much like a criminal. One must realize growing up in America, the first time one sees a lie detector test is normally on a detective show on television, where the gangster, who is normally lying, is screaming -- "I'll take a lie detector test." Therefore, you compare yourself in your own mind to that gangster on the Late, Late Show!

At 11:00 on a Thursday morning, you go in to the Hallmark Corp. for a lie detector. The man there then says he's going to try to put you at ease as he then commences to ask you a lot of questions such as do you have any hidden motives for applying for this job, have you ever drunk to excess, have you ever smoked marijuana, or taken any other drugs not given to you by a doctor? Have you ever stolen any merchandise or money over \$5? Have you ever been arrested? Have you ever used any other name? Have you ever been dismissed from a company where you previously worked? Did you have to leave Washington because of delinquent bills or any other such reason? The questions go on through two pages -- these questions are asked orally, however!

Then, now that you are supposed to be relaxed, he tells you to turn the chair around, this is so you are not facing the machine, he puts something around your arm as if a doctor was taking your blood pressure, a chain around your waist, and two small bands around two fingers of your right arm. Your arm is then placed on two sponges and you are told to close your eyes and keep them closed! This alone is scary!

Then he continues to ask you about ten questions pausing 15 seconds after every question. Of course, unless you are stupid or completely in some kind of euphoria the question that you await is Have you ever stolen anything? Whether you have or have not this makes you feel as if you have. Therefore, although, you are broke, you go home feeling like a thief!!

Massachusetts law prohibits an employer from requiring lie detector tests of his applicants or employees, and so a Boston book store owner decided he would use psychological stress evaluators. Unlike the polygraph the PSE measures only one indicator of stress -- voice modulation. A supervisor figured that the PSE sounded like a lie detector to him and refused to administer the tests. He was promptly fired. Now he is trying to get the Massachusetts Attorney General to take action against the book store.

(Continued from page 1)

Goldwater/Ervin broad-based bill would authorize a new Federal Privacy Commission to study private databanks not regulated by the bill (presumably using the commission's subpoena powers) and to recommend legislation.

The First Amendment issue is sure to arise if the commission seeks to study databanks now maintained by many news organizations. The most notable example is the "morgue" of The New York Times, now the on-line New York Times Information Bank, which indexes and abstracts data from every New York Times and from about 60 other publications. The personal information stored in the IBM 370/145 and available by display terminals to distant reporters -- or commercial subscribers -- has all been published previously, but under some circumstances it still may be regarded by an individual as private, especially after the passage of time. Such a computer system now means, in fact, that an individual who felt his privacy was invaded by a news item is no longer protected by the passage of time.

The New York Times plans eventually to computerize 100,000 Times articles. It markets the service vigorously to outsiders for \$675 - \$1350 a month plus installation charges. A remote terminal has already been installed at the University of Pittsburgh library and nearly two dozen other government agencies, businesses and news organizations. What an employer or investigator may no longer be able to get from the Federal Bureau of Investigation or the Internal Revenue Service he may be able to get easily through the New York Times, or some other private service. A person may then have a better chance for a job or insurance if he has never had his name in the papers.

The computerized morgue is only one way that news media now use modern data processing. "At large and small newspapers all over the country, political reporters are doing sophisticated samplings of voter opinions," according to a Times article September 1. "Crime reporters are sifting criminal justice records with computers. Others have rummaged through census data and analyzed traffic accident patterns, the background of rioters, political campaign contribution lists and countless other kinds of data."

Aware of this, representatives of newspaper publisher and editor associations have opposed legislation that restricts access to computerized criminal records maintained by local and federal agencies. They say this limits their First Amendment rights to know and report the news and to monitor the conduct of the police. In fact, the current proposals would prohibit outside access when the system is queried by name of an individual. When the system is queried as to an arrest as an event, access would be available, much as police "blotter" information is now open to press and public. News representatives recognize the abuses of arrest records, but argue that the remedy is to prohibit the use of an arrest record to deny employment, housing or other benefit not to close off government arrest records to outside scrutiny.

Further, they argue, the remedy for abuses of personal privacy is not to prohibit publication of presumably private facts. A case in point is Roe v. Doe, which the U.S. Supreme Court has agreed to hear this year (No. 73-1446). In that case, a psychoanalyst team wrote a book that included the edited notes of their sessions with a woman and her late husband, together with a so-called diary of their child. The authors claim to have concealed the identity of the patients; the patients claimed an implied contract of doctor-patient confidentiality had been breached. The Appellate Division in New York, despite the strong precedents against prior restraint of the press, issued an injunction barring distribution of the book pending the outcome

(Continued on page 7)

(Continued from page 6)

of a suit, "in light of the expanding recognition of invasion of privacy actions, and in view of the confidentiality accorded the physician-patient relationship" (42 A.D. 2d 559, 352 N.Y.S. 2d 626).

The Supreme Court will decide this fall whether to hear a challenge to the Georgia criminal statute that prohibits news media from disclosing the name of a rape victim when covering a trial. The Georgia Supreme Court found this privacy statute no violation of the First Amendment. Cox Broadcasting Corp. v. Cohn, No. 73-0938.

The last great privacy-First Amendment clash before the Supreme Court was in 1966. Then a 53-year-old Manhattan attorney named Richard M. Nixon argued that a Philadelphia family was entitled to collect damages, for an invasion of their privacy, when Life magazine published photographs of their former home along with the implication that the play "The Desperate Hours" mirrored the family's experience when held hostage by escaped convicts for 19 hours. The Court held that, in the absence of a reckless disregard of truth, the press was protected from such privacy actions. Time v. Hill, 385 U.S. 374 (1966).

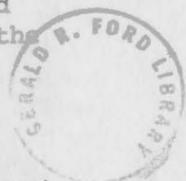
The conflict continues to arise in other contexts: the Pennsylvania State Supreme Court ruled last year that The Philadelphia Inquirer was not entitled to the names, addresses and grant amounts of city welfare recipients. Thus, the newspaper's First Amendment right to gather news was limited by the welfare recipients' privacy rights. The U.S. Supreme Court let the decision stand.

Attempts to regulate telephone, door-to-door or "junk mail" solicitation have been opposed on the grounds that such solicitation, even though commercial, is a valid exercise of the First Amendment. The ACLU defends unwanted mail on this basis, even though many persons regard such mail as an invasion of their privacy.

The First Amendment provides a specific Constitutional guarantee and, to many persons, the supreme Constitutional right; and so it will usually prevail over the more general privacy right. This is especially true where the invasion of privacy is relatively slight and the threat to free press and free speech is great. That was the situation in Time v. Hill, in the eyes of six members of the Supreme Court. Further, the remedy for invasions of privacy may be damage suits after the fact, but not prior restraint of the press. However, when the issue is government disclosure of personal information so that a news organization may report the news, courts and public opinion seem to opt for preserving confidentiality and letting the newspaper, like any good reporter, get the story elsewhere.

IN CONGRESS

Bills providing broad-based privacy protections for subjects of government files have moved closer to a floor vote in each House. The Senate Government Operations Committee this month reported out S. 3418. At the suggestion of Sen. Henry M. Jackson, D.-Wash., the committee deleted a provision that would limit demands for Social Security numbers. Sen. Charles H. Percy, R.-Ill., may try to restore the provision. Committee members also amended the bill to allow government sale of mail lists if authorized by another statute. The companion bill, H.R. 16373, has been approved by a subcommittee of the House Government Operations Committee and is now before the full committee. Details are available from the Privacy Project.



IN THE STATES

A rape victim may be questioned in open court about her prior sex conduct only under limited conditions, according to a California statute passed this month (SB 1678). To protect the privacy of the victim, such questioning is now permitted only on the issue of the witness' credibility and only after the defense submits a written petition asking for a hearing on the issue and the judge approves, outside of the presence of the jury. Such testimony is now inadmissible on the issue of whether the victim consented. The lone dissenter to the bill in the California Senate said the law would deprive a defendant of a fair trial by limiting the scope of testimony. * * * The California legislature also passed SB 1845 which, like federal law, would allow parents the right to challenge the accuracy of pupil records. The measure also requires that the anecdotal part of a cumulative record be removed when a student graduates. * * * A bill to supplement federal fair credit reporting requirements, AB 4494, was passed by the Assembly, but died in Senate committee. * * * Strong opposition from the information industry effectively buried AB 2656 in a California Assembly committee, after it passed the Senate 71-0 in January. Its sponsor eliminated a section in the Senate-passed version regulating private data banks, but even that concession could not prevent its defeat. The bill codified the "fair information practices" of the U.S. Department of HEW report on databanks. Virtually every state agency affected by the bill said it would cost too much for them to comply with it. * * * The legislature sent to Gov. Ronald Reagan a bill requiring banks to give customers prior notice before granting outsiders access to bank records (AB 1609).

THE PRIVACY REPORT is published monthly by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation. For a subscription (\$15 a year, \$5 for students) write: Privacy Project, 410 First Street S.E., Washington, D.C. 20003 or phone (202) 544-2026. The Privacy Project is a non-profit, tax-exempt effort to monitor increased data collection by state, local and federal governments, as well as by private institutions, and its impact on the individual's right to privacy. Tax deductible contributions aid the work of the project. Checks should be made payable to Privacy Project. *DOUGLASS LEA, Director; ROBERT E. SMITH, Associate Director; SHARON E. BIEDERMAN, Administrative Assistant*

MGMWSHT HSB
2-037349E296 10/23/74
ICS IPMBNGZ CSP
3037613770 MGM TDBN INGLEWOOD CO 100 10-23 0647P EDT
ZIP 20500

 **Mailgram**
western union



Handwritten signature

PHILIP BUCHEN, COUNSEL
WHITE HOUSE OFFICE
WASHINGTON DC 20500

THIS IS TO FOLLOW UP ON OUR LETTER OF OCTOBER 1 REGARDING OUR DESIRE TO PUBLISH PRESIDENT FORD'S POSITION ON CABLE COMMUNICATIONS AND PRIVACY. IN ORDER THAT WE MIGHT FINISH OUR PLANS FOR THE COMING ISSUE, WE WOULD LIKE TO KNOW IF WE CAN EXPECT TO RECEIVE MATERIAL WHICH WE REQUESTED. IF WE DO NOT HEAR FROM YOU WE WILL CONTACT YOU OR MR NESSEN BY TELEPHONE MONDAY, OCTOBER 28.

PATRICK GUSHMAN MANAGING EDITOR TV COMMUNICATIONS 1900 WEST YALE
ENGLEWOOD CO 80110

L 761-3770

18:47 EDT

MGMWSHT HSB

303

*I called 10/28 to Gushman
told him to talk w/ Doug Metz.*



10/9/74

~~no~~
Mr Metz

has prepared
& signed
a letter

to Cong Mess
on

VA Target



8/27/74

To: Doug Metz
From: Eva

Mr. Buchen would like you
to prepare a reply for his
signature to the letter from
Congressman Moss.

I don't find a copy of the
Ehrlenborn letter -- but will
find it. (Excuse the typo,
I'm so used to typing Ehrlichman)
(Expletive deleted!)



THE WHITE HOUSE
WASHINGTON

8/21
11:00

Marik wants the opportunity to reflect the experience in that report.

Cong. Moss ----
has also been sent to OMB and VA

We have carefully coordinated replies. Frank Silverman in Moss' office has gotten all the press on FEDMET

When the letter comes back, it will be released to the newspapers.

Whoever drafts the reply for the President, they would like to see to be sure their views are reflected.

Who got

Letter from ~~_____~~.

Congressman Moss to
Pres. Re V.A. Electronic
Data Processing System

Many calls -

Answer necessary
President



THE WHITE HOUSE
WASHINGTON

8/20/74

Send To Doug
Motz

sent
8/21

make
cg



Tuesday 8/20/74

9:20 Mr. Metz was asking whether we had received a copy of the letter to Cong. Moss regarding another so-called Fednet ---- TARGET.

(here)

If not, probably anyone over there working on it should coordinate with the Privacy Cmte.

Seth Kantor had called late yesterday afternoon and wanted to talk with you. Mr. Kantor had just left the office when Mr. Metz called him.

Said he wouldn't want anyone at the White House going off on a parallel and different track --- so we would urge this be checked out and whoever is designated.



August 19, 1974

Dear Mr. Moss:

On behalf of the President, I would like to thank you for your August 14 letter to the President concerning invasion of privacy, with particular reference to the government use of computers.

As you may know, the President has asked that the study on privacy he commenced as Vice President be continued at an accelerated pace. I have been asked to make certain that the members of his staff who are working in this area receive your letter as soon as possible.

With kind regards,

Sincerely,

Max L. Friedersdorf
Deputy Assistant
to the President

The Honorable John E. Moss
House of Representatives
Washington, D.C. 20515

bcc: w/incoming to Philip Buchen for further action
and DIRECT REPLY if appropriate
bcc: w/incoming to Bill Timmons - FYI

MLF:VO:ld



14
JOHN E. MOSS
3RD DISTRICT
SACRAMENTO, CALIFORNIA

ADMINISTRATIVE ASSISTANT
JACK MATTHEWSON



WASHINGTON OFFICE:
LEGISLATIVE ASSISTANT
EUGENE A. BROWN
ROOM 2354
RAYBURN HOUSE OFFICE BUILDING
PHONE (202) 225-7163

DISTRICT OFFICE:
DISTRICT REPRESENTATIVE
JERRY WYMORE
8058 FEDERAL BUILDING
650 CAPITOL MALL
SACRAMENTO, CALIFORNIA 95814
PHONE (916) 449-3543

Refer Philip Busher
792 BT

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515

GOVERNMENT OPERATIONS COMMITTEE:
RANKING MAJORITY MEMBER SUBCOMMITTEES ON
FOREIGN OPERATIONS & GOVERNMENT INFORMATION
CONSERVATION & NATURAL RESOURCES

INTERSTATE AND FOREIGN COMMERCE COMMITTEE:
CHAIRMAN,
COMMERCE & FINANCE SUBCOMMITTEE

DEMOCRATIC STEERING AND POLICY COMMITTEE

August 14, 1974

BT

The Honorable
Gerald R. Ford
President of the United States
The White House
Washington, D.C.

Dear Mr. President:

On the night of August 12th I welcomed your reaffirmation of the right of every American to remain secure against illegal, unauthorized invasions of privacy. I noted your sincere promise to prevent such violations of privacy by any agent or agency of government during your tenure of office. I congratulate you, sir, upon your firm statement. Specifically:

"There will be no illegal tappings, eavesdropping, buggings or break-ins by my administration. There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities."

Our shared concern prompts my letter. As you know, government's computer acquisitions are growing by quantum jumps. I do not quarrel with the need for such procurements. However, use of computers and their advanced methods of transmitting data can and does lead to abuses. Just recently, an attempt to create what would have amounted to a forbidden national data center via a GSA/Agriculture data network procurement termed FEDNET was prevented. This modular system would have allowed massive data exchange between agencies. Your role in preventing procurement of this system was both timely and vital. Revelation by Congress, anti-procurement language in GSA's House and Senate appropriations bills and assistance from OMB



coincided with your efforts.

My further probes, however, have unearthed not one, but a number of proposed Federal agency computer procurements. None has been authorized by law, nor have lawfully secured appropriations been made by Congress. Most possess little if any allocation authority from OMB. In each case, the agency has taken its "wish list" of computers to GSA, asking for and receiving a delegation of procurement authority. Though Congress and OMB may know absolutely nothing of such an undertaking, the agency owns a "hunting license" and feels free to hold vendor's conferences, prepare requests for procurement and generally go about acquiring its system.

Worse, most of these procurements are total computer systems, modular in nature, with ultra-modern telecommunications capacities. In virtually each case the agency's goal is total computerization of all its data and linkage of all its branches and components into the system. Add a telecommunications capability and whatever goes into the computer can be transmitted to other machines. The potential for privacy invasion is both obvious and ominous.

One projected system fitting all these criteria is V.A.'s "TARGET SYSTEM." A \$50 million effort, "TARGET SYSTEM" has no Congressional or OMB authorization, appropriation or allocation. V. A. does possess a delegation of procurement authority from GSA's Department of Automatic Data Procurement. V.A. has begun a pilot project with an IBM computer, obtained through what appears to be sole source procurement. Competitive bidding, required by Federal regulations, seems to have been adjourned here.

"TARGET SYSTEM" would include all 20 million V.A. records, all 59 field offices and 16 million annual veteran's contacts made by that agency. My investigation reveals that



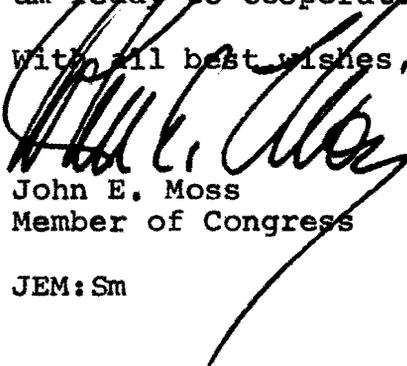
August 14, 1974

V.A. has been exchanging personal data on veterans with other agencies for some time, although how extensive this exchange is is as yet unknown. Yet there is no known way of protecting such exchanges from abuse.

Here in microcosm is what has become a government-wide phenomenon; widespread unauthorized data network acquisition by agencies, complete with sole source procurement and information exchange of personal facts.

After what the nation has just passed through, I submit that this is the last policy we dare allow agencies to institutionalize, no matter how well motivated they may be. My hope is that you will institute an immediate probe of "TARGET SYSTEM", followed by intensive scrutiny of what other agencies plan in this sensitive area. I am ready to cooperate with you in any way possible.

With all best wishes,



John E. Moss
Member of Congress

JEM:Sm



DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY

WASHINGTON, D.C. 20504

January 28, 1975

Handwritten scribble

MEMORANDUM FOR: PHIL BUCHEN

FROM: DOUG METZ *DM*

SUBJECT: ACLU National Privacy Program

As per attached, the ACLU plans to mount a nationwide campaign (of the kind used in New Mexico) to heighten public concern over personal privacy. This "total media" effort will be tied to the Bicentennial celebration beginning March 1976 and running for the balance of that year.

The implications are obvious, and I thought you should be aware of the plan. We shall watch developments closely.

Attachment



A BICENTENNIAL PROPOSITION

In an effort to confront the issues outlined in this brochure, the ACLU Foundation proposes the establishment of a National Privacy Program. We are determined to stimulate a nationwide discussion on the dangers of privacy invasion and what this leads to — control of behavior.

NATIONAL PRIVACY MEDIA CAMPAIGN

Believing that an informed public is crucial to democratic government, we propose, as part of the National Privacy Program, a National Privacy Media Campaign:

1. Saturation, mixed-media campaign, of thirty days duration; in conventional and creative media (refer to insert), in the Washington, D.C. Metropolitan area; on the issues of Invasion of Privacy/Technology of Control; scheduled for March, 1976
2. Distribution of the campaign nationally via television, radio, and print media on a psa (public service announcement) basis; 30-minute documentary film on campaign themes, produced for television and for 35mm theatre release; to begin in March 1976 and to run throughout the Bicentennial Year
3. National Bicentennial Exposition on the Invasion of Privacy/Technology of Control, to open in Washington, D.C. in March 1976, and to travel by special train to urban centers during the year; preceded and prepared for by a psa media effort (using the Washington campaign media materials) conducted by the ACLU Affiliates in local areas
4. Work with television and radio network to produce several documentary presentations on various issues connected to the campaign, and aired during the Bicentennial Year; work with the various print media to stimulate in-depth investigative journalism on the issues

NATIONAL PRIVACY CENTER

The Center, operating in Washington, D.C., will serve as the national clearinghouse, research and organizational headquarters for the issues covered in the campaign. The Center will open in January 1976 and offer among its many services:

1. To monitor the activities of private enterprise and public agencies insofar as they clash with fundamental notions of individual privacy and as they relate to control the behavior through data collection, medicine, social science, and technology
2. *The Privacy Report* — the information gathered through our national network will be organized and disseminated throughout the country on a monthly basis; in addition, the Center shall issue periodic, in-depth reports, bulletins and press releases
3. To stimulate investigative journalism on privacy-related issues in the print and broadcast media
4. To provide speakers and conduct conferences and seminars
5. To make available nationally a research guide and organizational plan that provides both citizens and organizations guidance toward programs of action
6. To design and produce programs of public education on the issues, for use by media, educational institutions, community groups, organizations and ACLU affiliates
7. To work with the President's Commission on Privacy to: avail them of the findings of the ACLU national effort on privacy; to cooperate wherever possible; and to provide critical review of the Commission's activities

LITIGATION PROGRAM

Litigation is often the only effective means of securing rights which have not yet received wide public recognition, as well as a means of enforcing recognized rights which are frequently violated. For several years the ACLU has defended citizen rights of privacy in the courts. A continuing and stepped-up ACLU litigation program will concentrate on the following areas, among others:

1. Injuries to citizens resulting from the growth of government databanks and increased dissemination of personal records, particularly in the criminal justice area; 2. Invasions of First Amendment rights by various forms of surveillance and data gathering about the political activities of citizens; 3. Violations of Fourth Amendment rights through wiretapping, eavesdropping and other forms of electronic and technical surveillance; 4. The manipulation or "tracking" of citizens through a variety of public and private data gathering and recordkeeping practices; 5. Credit and insurance reporting abuses; 6. Efforts to prevent government privacy-invasive activities from being conducted in secret, including suits against government agencies under the Freedom of Information Act; 7. Challenge to government secrecy and privacy-invasive practices conducted under spurious claims of "national security".

Invasion of Privacy/Technology of Control



National Privacy Program

American Civil Liberties Union Foundation

GERALD R. FORD LIBRARY



"Privacy," said Justice Louis D. Brandeis, "is the most comprehensive of rights and the right most valued by civilized men." Invasions of the privacy of Boston citizens by British soldiers armed with writs of assistance sparked the American revolution.

Today privacy is invaded more subtly — but more pervasively. All our misdeeds, real and fancied, are recorded in public and private data banks. These dossiers limit our horizons. We find it difficult to make of ourselves and our lives something other than what the records say about us.

Today the American Civil Liberties Union attempts to protect the right of privacy as it has in the past, only now the job is more complex and widespread. We feel this situation necessitates our stepping up the ACLU's traditional role of research and litigation. Accordingly, we propose a major new effort to inform the public about their right to privacy.

To celebrate the bicentennial of the American Revolution and the Declaration of Independence, the American Civil Liberties Union Foundation plans the National Privacy Program. This major project includes litigation, research, and, most importantly, an effort to inform the public about intrusions upon individual privacy and the ways to resist those intrusions.

A conference in Chicago, February 23-25, 1975, will provide participants with a chance to shape and launch the Program. Some exciting proposals will be presented. Through such a process, we hope an effective campaign can begin which will confront the present challenge to this precious right. We hope you will be among those helping us in this effort.

Aryeh Neier
Executive Vice President
A.C.L.U. Foundation



THE ISSUES

Record Keeping/Data Surveillance

Everyone has records: of credit, medical or psychiatric treatment, academic performance, banking, military service, perhaps arrests and convictions. A person may have up to fifty records, some held by government agencies, others by private organizations, and many on computers. This web of records can become a prison. Much of the data will be stale or incorrect or, when taken out of context, misleading. Yet there is no opportunity to see one's own records, correct them, or control their dissemination to the decision-makers who can determine the course of one's life — from insurers and employers to welfare agencies, the police, and the courts. Just the keeping of so much information is an invitation to decision-making by labels: the "tracking" of school children is one example of how classification can become permanent; the denial of employment to anyone with an arrest record is another. And the knowledge that one is "followed" forever by one's past can stifle free and individual expression, activity, creativity, even personality.

Surveillance

The Army is keeping watch on civilians who "might cause trouble"; included in this definition were American civilians in Germany working for the Democratic candidate in the 1972 Presidential election. City, state, and federal intelligence agents are collecting and computerizing dossiers on "radicals," using such methods of surveillance as infiltration, wiretapping without warrants, bugging, burglary, and opening mail. The dossiers include some fact and much fiction about the political beliefs, activities, and affiliations of thousands of people who have never committed a crime, but who have exercised their constitutional right to express their disagreement with the policies of the government. There could hardly be a more powerful incentive to remain silent, out of sight — and unrecorded.

Wiretapping & Bugging

There are no restrictions on the government's freedom to wiretap for reasons of "national security," though no one knows what "national security" really means. But even wiretaps initiated under a warrant are virtually uncontrolled. They intercept all conversations of all persons using the tapped phone, including legally "privileged" conversations between attorney and client, and they may continue for unlimited periods of time. Any wiretap is a dragnet. Existing legislation, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, barely touches this gross invasion of privacy.

Control of Behavior

To invade one's privacy is also to control one's behavior. Modern technology has produced new techniques of behavior control, from drug therapy for "hyperactive" school children and psychosurgery to sophisticated reward-and-punishment behavior modification programs for "aggressive" prisoners. There are new screening programs for the genetic identification of "violence-prone" individuals, invariably focussed on minority groups and the poor, and "predelinquency" programs for elementary school children which label such children as "risky" and then, quite naturally, treat them accordingly. Like the record prison, labelling becomes a self-fulfilling prophecy; there may be no better way of creating a delinquent than by labelling a six-year-old as a pre-delinquent. Labelling invites prediction, and prediction invites behavior modification — the manipulation of an individual's thoughts, feelings, and actions in the guise of "treatment." The means of invading privacy, then, becomes the tool for controlling what people do, say, and even feel.



Big Brother's Big Eye

An elderly Albuquerque couple, lounging in the backyard one cool New Mexico evening, heard a roar from above. Then a light appeared, focusing with terrifying intensity on the man and woman. A UFO? Hallucination? Not at all. The source was the Albuquerque police department's "spy in the sky" plane on a routine patrol. "It scared the world out of us," the man said later. "It reminded us of George Orwell's *1984*." The low-flying craft operates by daylight too. A woman complained that she could no longer sunbathe on her roof because the plane kept circling overhead.

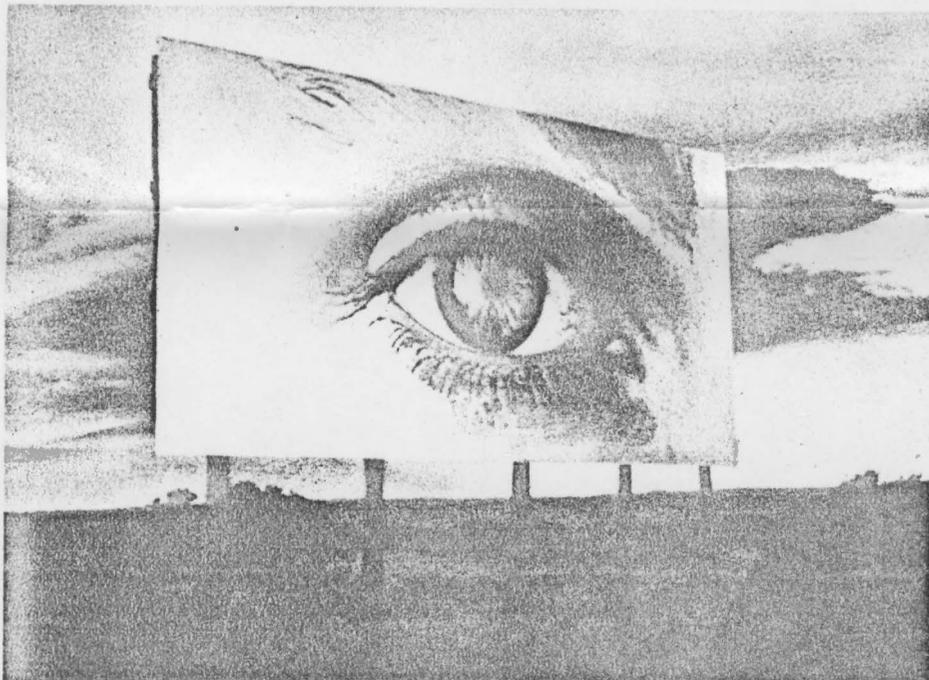
More than 100 complaints about assorted varieties of snooping have been filed by Albuquerque-area residents in response to an unusual month-long educational campaign by the New Mexico Civil Liberties Union. If any area resident was unaware of Big Brother when the \$50,000 publicity effort began, he was saturated with the image by last week. Along the freeways, billboards were filled with an eerily staring human eye. Similar eyes glared balefully from a dozen small ads in a single day's newspaper. Television spots showed a grade-school girl playing unconcernedly, then frozen into a prisoner-like pose with a Social Security number on a placard hung from her neck. A "Mission Control" sequence depicted the launching of a pyramid with a staring eye on top, like that on the reverse of a dollar bill.

The idea was first promoted by a group of self-styled "alternative culture" activists, then endorsed by no less a conservative than Congressman Barry Goldwater Jr. Designed as a pilot program, the campaign and its response have provided a representative sample

of what—and who—is bugging citizens all over the U.S. The most common complaints concerned the difficulty of penetrating the bureaucratic labyrinth, only to find a Minotaur at the end. Almost as numerous have been insoluble hassles with billing computers and instances in which a would-be buyer was turned down because a credit bureau provided a report based on unfavorable but unchecked information. (Some credit-bureau employees admitted that investigators are afraid of losing their jobs if they fail to turn in any unfavorable material about a subject; they occasionally fabricate negative information.) Many complaints involved the improper release of military records—in most cases, from cryptic, numbered coding on supposedly honorable discharges—and the illegal disclosure of bank data.

The project directors were determined to go beyond invasions of privacy, however serious, to the broad area of "control by technology, whether by a king or a computer or a bureaucracy." An especially chilling example of such control came from a woman who said she had worked all her life to be sure her daughter could go to college. Then she found that the high school girl had been suddenly transferred from a college preparatory curriculum to vocational courses. The school refused all information, and officials of the federally funded vocational program to which the daughter was assigned would give no reasonable explanation. Their response amounted to: "This was devised by experts who know what's in the best interests of your daughter." From such cases the Civil Liberties Union will choose which of Big Brother's practices will be the targets of court action.

CIVIL LIBERTIES "EYE" BILLBOARD ON NEW MEXICO HIGHWAY



United States Senate

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS
(PURSUANT TO SEC. 6, S. RES. 235, 93D CONGRESS)
WASHINGTON, D.C. 20510

November 22, 1974

Dear Mr. Neier:

Thank you for your recent letter informing me of the plans to make the protection of individual privacy a major theme in the Bicentennial.

Your organization has been in the forefront of efforts to preserve and extend the privacy rights of all Americans. Much of the progress made thus far would not have occurred had it not been for the work of the ACLU.

The choice of the right to privacy is particularly appropriate for the 200th Anniversary of the Nation's founding. I believe that what we now tend to call the right to privacy is merely a modern expression of those fundamental principles of human liberty which were recognized at our Nation's beginning and expressed in the Declaration Of Independence, the Mecklenburg Resolutions, and the Bill Of Rights.

I am familiar with the success of the New Mexico ACLU's program on privacy in 1974. Your more ambitious objective of presenting a similar program on a national scale will accomplish the important purpose of making all citizens aware of the necessity of safeguarding their rights to privacy. I wish you every success in your project and I appreciate your keeping me informed of your plans.

With kindest wishes,

Sam J. Ervin, Jr.

Sam J. Ervin, Jr., Chairman



A Bicentennial Proposition

A Call For

A National Privacy Conference

From February 23-25, 1975, the American Civil Liberties Union Foundation will host a national conference on the Invasion of Privacy and what this leads to — a Technology of Control. The conference will be held at the University of Chicago, Center For Continuing Education.

The American Civil Liberties Union Foundation intends to use this conference to launch a major Bicentennial initiative — The National Privacy Program. National leaders from business and labor, the political community, foundations, educational institutions, and civic and professional groups have been invited to participate in the launching of this effort.

"I have long felt that the key to effective privacy protection and confidentiality of records in this country depends upon a citizenry that is fully informed of its rights, and upon an educated data handling community that is sensitive to the ways in which improperly used information can affect the lives of people.

"Thus I cannot think of anything more effective than a public information program that will educate people and awaken them to the importance of safeguards in the recordkeeping field.

"The privacy media program of the ACLU in New Mexico was a powerful beginning and I heartily endorse its expansion into the National Privacy Program."

Arthur R. Miller
Harvard Law School
Author of *Assault on Privacy*

American Civil Liberties Union Foundation
22 E. 40th Street
New York, New York 10016



Privacy

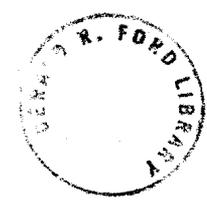
THE WHITE HOUSE
WASHINGTON

March 4, 1975

MEMORANDUM FOR: BILL NICHOLS
FROM: PHIL BUCHEN
SUBJECT: Request of Senate Permanent
Subcommittee on Investigations
for Access to Files of the
Internal Revenue Service

Attached to this memorandum is a request by the Chairman of the Senate Permanent Subcommittee on Investigations for the issuance of a new Executive Order providing access of the kind authorized in E. O. 11711 of April 13, 1973. I understand that both executive and legislative actions since E. O. 11711 was issued have tightened restrictions on access to income tax records for the purpose of protecting individual privacy. Your memorandum to Dudley Chapman of March 4, 1975, also notes that, at a minimum, some changes in the form of E. O. 11711 would be necessary to comply with the Privacy Act of 1974. In addition, you should consult with IRS to determine if additional restrictions consonant with E. O. 11805 would be appropriate.

Would you, therefore, please initiate, on an expedited basis, the preparation of a new Executive Order that will (a) satisfy the requirements of the Privacy Act of 1974, and (b) be consistent with the spirit of Executive Order 11805.



DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY

WASHINGTON, D.C. 20504

March 17, 1975

Honorable James T. Lynn
Director, Office of Management and Budget
Washington, D.C. 20503

Dear Mr. Lynn:

We have noted the views of the Department of Commerce contained in Mr. Parette's letter to you of March 12, 1975, concerning the "Consumer Privacy Code" to be proclaimed by the President.

The purpose of the Code is to implement the July 10, 1974 decision of the Domestic Council Committee on the Right of Privacy to establish voluntary standards of fair information practices to cover the many records generated by marketplace transactions not now regulated by the Fair Credit Reporting Act. The wording of the Code resulted from extended discussions with representatives of consumer interest groups and of the banking, insurance, retail, and credit industries.

These conferences confirmed the Committee's original judgment that legislative and regulatory action was premature because of the complexities of the record-keeping systems associated with marketplace transactions, the absence of solid empirical information on such systems, as well as the cost/services impact of finite regulation.

It was concluded that significant steps in behalf of consumer privacy protection should be taken pending needed further study, including possible review by the Privacy Protection Study Commission to be established shortly.

As a result of the efforts of the Office of Consumer Affairs, key segments of American industry are prepared now to subscribe publicly to a Presidential proclamation and to attend a signature ceremony.

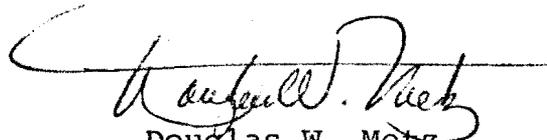


The terms of Code are purposely broad so that a single set of principles can be subscribed to by a cross section of consumer-oriented businesses. It can form the basis for development, as required, of more detailed, industry by industry, or company by company, expressions of fair information practices.

The choice of the word "code" is, I believe, unfortunate since it implies activities traditionally associated with "industry codes" and thereby, may account for the concerns expressed by the Commerce Department. The proposed proclamation should more appropriately be designated "A Declaration of Fair Information Principles for Consumers."

The proposed proclamation is not intended as a substitute for any subsequent regulations or legislation which may, as a result of future study be needed to protect consumer privacy rights. Its objective is to give public visibility to the need for adherence to fair information practices in the marketplace and provide a single set of basic principles to which significant consumer industries can subscribe through commitments of their chief executive officers.

Sincerely,



Douglas W. Metz
Acting Executive Director

cc: James N. Ravlin, Commerce
S. John Byington, Office of Consumer Affairs

DWM:sgd

bcc: Philip W. Buchen



Privacy

Tuesday 4/21/75

4/21/75

10:10 Pete Warner called from the Institute of Internal Auditors to ask if you might be available to speak at a symposium they're having in Orlando, Florida, on April 21st.

Had worked with you when you were the Executive Director of the Privacy Commission.

I suggested he call Doug Metz, and if Mr. Metz felt this would be an appropriate thing for you to attend, they could be in touch with us again; however, I felt that Mr. Metz would probably be the one they would want for this symposium.

They will call Mr. Metz.



March 26, 1975

To: Doug Metz

From: Eva

Roderick
Buchen's
resumes

Mr. Buchen asked me to
send these resumes
to you.

Thanks for your help.



Privacy

Friday 9/19/75

Meeting
9/19/75
2:30 p. m.

11:30 Barry is scheduling a meeting this afternoon
(Friday 9/19) at 2:30 with Doug Bennett, Peter McPherson.
They will come here to discuss the Privacy Act and how
it will affect this office.

*Mr. Buchan can't have
the meeting
asked if Ken could
meet with them.*



THE WHITE HOUSE

WASHINGTON

September 15, 1975

MEMORANDUM FOR: DOUG BENNETT

FROM: ROD HILLS *RH*

SUBJECT: The Privacy Act and Information
Concerning Political Affiliation

Interior is correct in its opinion that the Privacy Act prohibits agencies from maintaining any records describing the exercise of an individual's First Amendment rights, unless expressly authorized by statute or pertinent to and within the scope of an authorized law enforcement activity. Information concerning an individual's party affiliation, even if taken from the public record, does fall in this proscribed category of materials. For the purpose of this statute, maintaining files includes collecting, using or disseminating such information, as well as retaining it in the files.

The White House is not an agency for the purpose of the Privacy Act, and, therefore, you may continue to maintain files which include information indicating the party affiliation of candidates for, or incumbents of, the various "political" positions in the non-career service. Similarly, your files are not subject to mandatory disclosure under either the Privacy Act of the Freedom of Information Act.

In dealing with agencies after September 27, the effective date of the Act, your staff should be aware that the consent of the individual is generally required before an agency can acquire such information, whether from the public record or the White House. Either actual consent to maintain such information, i. e., given directly to the White House or the agency, preferably in writing, or implied consent, e. g., listing an individual's political affiliation in his resume, inclusion in Who's Who, etc., is sufficient for this purpose.

In response to your request, we do not view as a legal problem resubmission by the agencies of the various "clearance" sheets necessary to bring your files up to date with respect to the pre-August 9, 1974 political appointees, provided this is accomplished prior to September 27.



However, I recommend that you also consider any political reaction that could result from this resubmission procedure and our collecting such information without the consent of the individual. I would be pleased to discuss this further at your convenience.



THE WHITE HOUSE
WASHINGTON

FOR: *Red Hills*

FROM: PETER McPHERSON *P.M.*

For your information.

*I have sent Davey Path
a copy of this.*

Attachments





UNITED STATES
DEPARTMENT OF THE INTERIOR
OFFICE OF THE SOLICITOR

Red

JUL 7 1975

Memorandum

To: Hugh M. Duncan, Office of the Secretary

From: Solicitor

Subject: Privacy Act Restrictions on Records Concerning
Political Affiliation

A question has been raised as to what effect if any the Privacy Act will have on records concerning incumbents of and candidates for positions which are essentially political in nature. We have considered three types of such non-career positions: Presidential appointees, non-career executive assignments (supergrades) and Schedule Cs. The comments below apply equally to these positions as well as to incumbents of and candidates for various boards and committees which advise Interior. Also, in our opinion the restrictions of the Statute apply equally to incumbents and candidates although the means of processing them may be different, due to the difference in relationship of the individual to the Department.

The Privacy Act, which takes effect on September 27, 1975, provides that agencies maintaining systems of records shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

We have reviewed this provision and are of the opinion that, if faced with the matter, the courts would hold that it precludes the Department from maintaining records concerning the political affiliation or political activity of persons holding the above-named positions, except with the concurrence of these individuals.

The crux of the matter is whether affiliation with a political party is a right guaranteed by the First Amendment. In determining what is and what is not guaranteed by the First

Amendment, OMB's draft guidelines on the Privacy Act state, "agencies will apply the broadest reasonable interpretation."

Our review of the cases indicates that affiliation with a political party is a protected right. In the recent case of Kusper v. Pontikes, the Supreme Court stated, "There can no longer be any doubt that freedom to associate with others for the common advancement of political beliefs and ideas is a form of 'orderly group activity' protected by the First Amendment . . . The right to associate with the political party of one's choice is an integral part of this basic constitutional freedom." 414 U.S. 51, 56-57 (1973). See also, Williams v. Rhodes, 393 U.S. 23, 30 (1968); Cousins v. Wigoda, 42 L.Ed.2d 595 (1975).

While it is true that employees in the Federal service have been held to have forfeited some of their rights to take active part in political affairs, e.g., U.S. Civil Service Commission v. National Association of Letter Carriers, 413 U.S. 548 (1973), no decision has held that Federal employees forfeit the right to be a member of a political party. We think it unlikely that such a decision would be reached.

That Congress intended section 552a(e)(7) to include party affiliation as a matter not suitable for recordkeeping is also made clear by the legislative history. The House version of the section prohibited the keeping of records concerning "the political or religious belief of any individual," H. Rept. 93-1416, p. 30 (1974), a formulation which we would take to clearly include party affiliation. When the final version of the legislation was prepared by representatives of the House and Senate (in a complicated procedure not involving use of a conference committee), their report stated that the final formulation of the section was designed to expand the House formulation. 120 Cong. Rec. S21816 (daily ed. Dec. 17, 1974).

We believe that there is no express statutory authority which would take records of political affiliation or activity by incumbents to or candidates for the so-called political positions out of the purview of the Privacy Act. 5 U.S.C. § 3301 is the basic authority for appointment into the Civil Service. Under E.O. 10577, Nov. 22, 1954, 19 F.R. 7521, as amended (see note to 5 U.S.C. § 3301), the President has set up basic Civil Service Rules and charged the Civil Service Commission with the responsibility for administering them. Rule VI governs

positions excepted from the competitive service. This includes Schedule C - Positions of a confidential or policy determining character. Rule 9.20 concerns non-career executives who must 1) be involved in advocacy of administrative programs, 2) participate significantly in determining major political policies, or 3) serve as personal assistant to a key political figure. While gathering information on political affiliation may be inferred from rules VI and IX, we do not believe it has the level of express statutory authority.

Recognizing the need to collect information on a person's political convictions in determining suitability for a political appointment, such a record can be maintained provided Interior has the person's consent. Obtaining an incumbent's consent can be accomplished merely by asking, and preferably by having the incumbent sign an appropriate form.

The candidates present a different and much more sensitive problem: there are larger numbers of persons involved and, occasionally, they may not know they are under consideration. Depending on whether or not they know, several alternatives are possible:

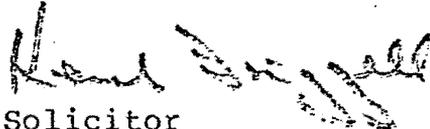
- 1) If an individual voluntarily includes such information on a resume', we can assume that such act constitutes a waiver of the prohibition.
- 2) Use a form method of obtaining a waiver. A statement such as failure to check a block or requiring one to check a block is sufficient to grant consent to maintain a record of a person's political background.
- 3) A letter to the person requesting consent and receipt of such consent.
- 4) Ask the individual only at the time a decision is imminent and he or she should know they are being considered. If the individual refuses to consent, he or she may

be dropped from consideration. If consent is given, at that time we may begin to maintain the desired record.

- 5) In some cases it may not be necessary to maintain a written record.

There are other methods which will accomplish the result which may require further discussion. Being realistic, however, the requirements of the Act clearly will complicate the legitimate process of recruitment and staffing for non-career positions, regardless of method.

In summary, then, it is necessary to obtain an individual's permission in order to maintain records on the individual which reflect political activity or affiliation, absent statutory authorization or the required nexus with law enforcement activity. Securing the necessary permission can be done by any number of methods which allow an individual the opportunity to indicate a willingness to have such records maintained or a desire not to have them.


Solicitor

10/17

Phil-

Because the FBI
message switch is
coming to a head and
memos are being
prepared "for high
places," I thought you
might like to have some
current documentation
handy -

George

DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY

WASHINGTON, D.C. 20504

October 15, 1975

MEMORANDUM FOR: KEN LAZARUS
LYNN MAY

FROM: GEORGE B. TRUBOW 
General Counsel

SUBJECT: FBI Message Switching Plan

Quincy Rodgers gave me a copy of Lynn's second draft memorandum on the above topic, dated October 13, 1975. We talked about the matter, and Quincy asked me to send a response since he had to leave town for a prior commitment.

The second draft goes further, in our opinion, toward providing a sound basis for a decision by the President on this important issue. We still had some concern, however, and I have attached a revised draft that reflects these notions:

1. The "Background" does not accurately portray the difference between NCIC and CCH (Computerized Criminal Histories). The latter is what the message switch problem is about, and comprises only a portion of the total NCIC system. There is little quarrel with the NCIC system itself, which lists outstanding warrants and stolen property, primarily. The CCH component was added about four years ago, and raises the major issues which the memorandum addresses. Nor does the background indicate the length of time this matter has been pending, and the seriousness of the controversy.



2. It is not accurate to say that privacy is not an issue. It is true that system security, just one aspect of privacy, is not a difficult problem since it can be accomodated by information system design. The larger privacy questions, however, in terms of "big brother", a national police force, and the access that Federal law enforcement has to monitor state and local law enforcement information, are very important matters.
3. The first option has been revised to emphasize that the resolution of the issue should be fashioned by state and local government, the chief users and beneficiaries of the CCH program.

The second option is eliminated since we consider it totally unacceptable. That option, though called "temporary", actually implements the plan, thereby incurring all the negative implications of the proposal, while leaving a continuing burden with the Federal government to finally resolve the problem. This seems to us to be the worst possible situation. Our revised statement of the first option obviates the headache in the first place, and leaves it to the states to develop a proposal in response to the need they perceive.



901

DRAFT

MEMORANDUM FOR THE PRESIDENT

FROM: JIM CANNON

SUBJECT: Proposed National Criminal Information
Center Message Switching Plan

The Deputy Attorney General proposes to announce shortly the plan of the FBI to install a "message switching" capability in the National Criminal Information Center (NCIC). The proposal, which has been pending for more than two years, has been held up in the department because it raises substantial policy issues with political dimensions. This memorandum places the underlying issues in some perspective and identifies the options available to you in passing on the proposal.

BACKGROUND

As presently constituted, the NCIC System entails the physical storage of State criminal information, e.g. stolen cars, wanted persons, arrest sheets, etc., with the FBI. Those State law enforcement agencies which make such information available to the FBI are eligible to access the FBI's system for information upon request. This has been the pattern of Federal/State information transfers for a substantial period of time, though computerized criminal histories (CCH), which gave rise to the message switch plan, have been in the NCIC system on an experimental basis for only about four years.

The telecommunication of the bulk of criminal information directly between the States, on the other hand, has been handled for a number of years by the National Law Enforcement Telecommunications System (NLETS) under a continuing grant from the Department of Justice. NLETS is managed by a consortium of officials from various States with no direct involvement by Federal law enforcement officials, and the performance capability of the system was substantially upgraded in 1973.



The proposal advanced by the Deputy Attorney General in behalf of the FBI would involve the return of records of single State offenders, comprising the bulk of CCH records, to the respective States, relieving the FBI of the responsibility for their maintenance. The FBI would maintain an index of State records and would establish a telecommunications system which would enable it to query the data base and, upon receiving a request for information from a State, to electronically check its own records, poll other States for Records and then transmit the information to the requesting State. The FBI would retain all multi-State offender records, Federal crime files, and single State offender records for states that do not computerize their files. Several Executive Department agencies (DCCRP, OMB and OTP) as well as members of Congress (Cong. Moss, Sen. Tunney),

have disapproved of the plan

DISCUSSION:

Opposition to the "message switching" proposal is generally based upon one or more of three arguments: (1) there is no demonstrated need for the involvement of the FBI in State-to-State communications -- NLETS is adequate to meet present and future needs; (2) the proposal runs afoul of the sound precepts of Federalism; and (3) the FBI's control of a nation-wide telecommunications system of computer records poses a severe threat to individual privacy.

The Deputy Attorney General defends the need for this program by pointing out the readiness of 19 states to join with the six States now participating in the limiting message switching experiment. He agrees that message switching arguably could be handled by a State-run organization, like the current National Telecommunications Law Enforcement System (NLETS), but maintains that the FBI is the only organization that can immediately implement message switching, the latter allegation being denied by NLETS. In regard to the privacy threat, Tyler maintains that the FBI will only have the electronic capacity to store information which it has had physically in its possession at the present, though this argument does not obviate the basic privacy problem.



The real issue in this matter is not that of privacy in terms of system security. Although the plan would present some additional potential for abuse, safeguards could be devised to minimize this potential. The key "privacy" issues are the need, and the dictates of Federalism. The other major issues are emotional fears of "big brother", a national police force, and the matter of Federal access to state law enforcement information.

NLETS would appear adequate to meet the short-term needs for State-to-State telecommunications. Moreover, a recent study commissioned by the Department of Justice indicated that long-term needs in this area could be met best by two State-operated switching systems (one on each coast).

On the Federalism issue, it should be noted that the vast majority of criminal information is State and local in nature, and your Administration's policy has been to limit the Federal role in matters where primary responsibility lies with State and local authorities.

OPTIONS:

1. Inform the Attorney General that he may not implement message switching within the Justice Department. If the states recognize a need for a national message switching network, they can develop and propose an alternative to Federal control.

Pro: Would eliminate a controversial program that has potential for political repercussions and administrative headaches. Would also leave responsibility for further action with state and local government, the principal users and beneficiaries of the proposal system.

Con: May possibly result in some delay in the computerization of criminal records.



2. Allow the Justice Department to implement the FBI message switching plan.

Pro: Would satisfy FBI desires in this matter and would promote rapid computerization of criminal records in the State system.

Con: Would open the Administration to criticism from liberals about endangering individual privacy and conservatives about the need or desirability of Federal control of state criminal justice information systems, as summarized previously. May endanger your Administration's credibility in areas where it has achieved notable success-in privacy and reduction of "big government".



THE WHITE HOUSE

WASHINGTON

October 22, 1975

MEMORANDUM FOR

The Honorable Antonin Scalia
Assistant Attorney General
Office of Legal Counsel

This is to inquire about the impact of the Privacy Act of 1974 on the Presidential Personnel Office.

The Presidential Personnel Office is not considered to be an 'agency' for the purposes of the Privacy Act because its sole purpose is to advise and assist the President. However, that office works closely with agencies that are subject to the provisions of the Privacy Act. Accordingly, it would be most helpful to have your advice on the following questions.

1. In the course of an FBI background investigation, 'records', as defined in the Privacy Act, are collected by the FBI as well as disclosed to the FBI by other Federal agencies (IRS, DOD, etc.). Does section 552a.(b) of 5 U.S.C. require the FBI (or these other agencies) to obtain the prior written consent of the individual applicant or nominee before disclosure of such records?

2. Prior to requesting a background investigation from the FBI, the White House Personnel Office obtains basic personal information on Form No. 86 from the individual. A copy of this form is delivered to the FBI by the White House Security Office to assist in the investigation. Does section 552a.(e)(3) of 5 U.S.C. require the FBI to comply with the provisions of that section?



3. Under certain cases, the White House Personnel Office collects information on the political affiliation of persons being considered for appointment or nomination. Such information may be obtained directly from the individual under consideration and/or from independent sources (national or state party headquarters). When the appointment or nomination is for a position at a Federal agency, the information on political affiliation is disseminated to and maintained by appropriate persons at that agency.

Does section 552a.(e)(7) require the individual to give his express authorization for the agency to maintain a record of his political affiliation

-- if the individual volunteered the information, such as in a resume?

-- if the information is obtained through independent sources and the individual has not volunteered such information?



Philip W. Buchen
Counsel to the President