

Kevin Burns
Policy Conference on Privacy, Professor Forgie

STORAGE OF DATA BY NON-FEDERAL GOVERNMENTAL
AND PRIVATE INTERESTS IN THE UNITED STATES

I. INTRODUCTION

- A. Purpose: To investigate the need and legitimacy of public action concerning the access to and storage of existing state-, locally-, and privately-owned data which might infringe upon the individual's right to privacy in the United States.
- B. Definition of terms
 - 1. Need and legitimacy
 - 2. Public action
 - 3. Access
 - 4. Storage
 - 5. Existing data and present controls
 - 6. The individual's right to privacy

II. Exploration of purpose

- A. The situation today
 - 1. What is stored?
 - 2. Who is storing it?
 - 3. Access limitations
 - 4. What safeguards exist to protect against inaccuracies, out-of-date info, biased retrieval, etc
 - 5. Disposal criteria
- B. The potential infringements summarized
- C. Rights of others which conflict with the right of privacy
- D. How much privacy do individuals have a right to expect?
- E. Are there legitimate ways to insure these rights?
- F. Are they realistic and how effective can they be expected to be?

III. CONCLUSIONS

- A. Concluding summary of the individual's right to privacy in regard to existing data stored by non-Federal owners
- B. Proposals to help protect those rights
- C. Extrapolation into the future
- D. Broader implications of the proposals

Capuano, Robert M.
Conference on the Boundaries of
Privacy -- Commission IV
Woodrow Wilson School of Public
and International Affairs
October 6, 1971

TECHNOLOGY AND THE REGULATION & CONTROL OF STORED DATA

OUTLINE

I. COMPUTERS--GENERAL BACKGROUND AND USES

II. PRESENT STAGE OF COMPUTER TECHNOLOGY

- (A) "Hardware"--physical elements of the machine
- (B) "Software"--programming
- (C) Time-sharing
 - 1. Methods of storing data
 - 2. Methods of transferring data
 - 3. Methods of retrieving data
- (D) Costs

III. SNOOPING (i.e. ways of gaining improper access to data banks)

- (A) Technological methods
 - 1. Tapping transmission lines
 - 2. Breaking codes
- (B) Access through human failings

IV. CONTROLLING STORED DATA

- (A) Procedural methods
 - 1. Regulate operating personnel
 - 2. Keep record of system's operation
 - 3. Grant subject access to his file and its uses
 - 4. Grant subject ability to correct inaccuracies
 - 5. Control input, output, and storage
- (B) Technological Security
 - 1. Guarding against improper access
 - 2. Guarding against accidental leaks
 - 3. Flushing out obsolete data
- (C) Costs--Are they prohibitive?

V. A LOOK INTO THE FUTURE:

What can be done? versus What should be done?

Betsy Freeman

Conference on Boundaries of Privacy
Commission III, Topic I: The Credit
Bureau Industry and the Invasion of Privacy

This paper will be concerned with the invasion of privacy by an industry which has been called essential to the economy of the United States. It will attempt to examine thoroughly the workings of credit bureaus, how any invasions of privacy occur, and whether such invasions can or should be avoided.

I. INTRODUCTION: STATEMENT OF THE PROBLEM

- A. Importance of Credit Bureaus to U.S. Economy
- B. Credit Bureaus as Substantial Invaders of Privacy

II. THE OPERATION OF CREDIT BUREAUS

- A. Number and Type of Credit Bureaus in U.S.
 - 1. In-file operations
 - 2. Investigative Operations
 - 3. Associated Credit Bureaus of America: its functions
- B. Factors which Influence Actions of Credit Bureaus
 - 1. Clientele
 - 2. Type of information held at a premium
- C. Other Activities of Credit Bureaus
- D. The Computer and its Implications For the Credit Industry
 - 1. Ease of access, storage, transfer of information
 - 2. Influence on types of errors
 - 3. Influence on credibility of data
- E. Accessibility of Data

III. CREDIT BUREAUS AND THE LAW

- A. The Fair Credit Act
 - 1. Accomplishments
 - 2. Failures
 - 3. Enforcement
- B. Credit Bureaus and Privacy: Legal Precedent and Thought
 - 1. The individual "Right of Privacy"
 - 2. Liability of credit bureau for inaccuracy, unauthorized dissemination.

IV. RECOMMENDATIONS AND CONCLUSIONS

- A. Legislative: what is needed
- B. Judicial: interpreting the right of privacy

19

WOODROW WILSON SCHOOL
CONFERENCE OUTLINE
"THE BOUNDARIES OF PRIVACY IN AMERICAN SOCIETY"
STEVEN L. GLAUBERMAN
COMMISSION I

I. Introduction: The Federal Government, the Cybernetic Revolution, and the Information-Based Society

II. The Information Seekers

A. Organizations in the Federal Government engaging in data collection and/or surveillance

1. Census Bureau
2. Department of Justice - the autonomy of the Federal Bureau of Investigation (FBI)
3. Department of Defense - United States Army
4. Department of Health, Education and Welfare
5. Internal Revenue Service

B. Methods of Surveillance

1. Dossiers and the Proliferation of Government forms and applications
2. Use of the Social Security Number
3. Decennial Census and Government Questionnaires
4. Mail Scanners
5. Computerization and Electronic Eavesdropping
6. Security Checks

C. Data Storage and Access to Data in the Federal Government

1. Census Bureau
2. National Data Bank Proposal
3. Transfers of Information among Federal Agencies
4. Cooperation among Federal-State-Local levels in the Transfer of Information

III. Legal Precedents for Government Surveillance Authority - The National Security Question

- A. Supreme Court Decisions
- B. Congressional Mandate

IV. Misuse of Information - Specter of Surveillance

- A. Federal Data Banks
- B. Existing Controls in the type and volume of information to be collected and the means of surveillance
- C. Confidentiality of Information

V. Policy Recommendations

- A. Changes in the Law for How to Gather Data
- B. Controls over Access
- C. Controls over Accuracy
- D. Strengthening Privacy Protecting Procedures of Information-Exchange Programs

Marilyn Green

THE BOUNDARIES OF PRIVACY IN AMERICAN SOCIETY

Commission I: Domestic Surveillance Activities of the Federal Government

Report: The moral and legal rights of the individual to privacy versus the government's need for surveillance

I. The introduction and statement of the problem

- A. The relevancy of the problem of privacy.
- B. A definition of terms.
- C. The scope of the examination.

II. The moral and legal rights that entitle an individual to privacy.

- A. The moral rights.
 - 1. Privacy as the necessary prerequisite to the formation of basic relationships of human beings.
 - 2. Privacy as necessary for the insulation of the individual from society's conforming pressures.
- B. The legal rights.
 - 1. Privacy as delineated in the Common Law.
 - 2. Privacy as protected in the Bill of Rights.
 - 3. Privacy as affected by Congressional legislation.
 - 4. Privacy as interpreted by the Federal courts.

III. The governmental functions which necessitate the surveillance of individuals.

- A. An examination of the fundamental nature of a democratic state's functions.
- B. Surveillance as necessary to ensure the functioning of governmental agencies.
- C. Surveillance as necessary to protect the national security from internal and external threats.

IV. The balance between the individual's need for privacy and the government's need for information.

- A. Current legislative perceptions of the balance as evidenced by pending bills.
- B. Personal perceptions of the desired balance with policy recommendations to achieve this balance.

Alex Hartnett

COMMISSION @: STATE LAWS ON WIRETAPPING

- I. History of legal right to privacy
 - A. Early standards, beliefs about privacy in Western civilizations
 - B. English common law, Blackstone's commentaries, John Stuart Mill, Hobbes
 - C. U.S. legal right to privacy
 - 1. Interpretation of Constitution, especially Bill of Rights in context of a right to privacy
 - 2. Early cases, Cooley's Torts, and other commentaries up to Warren-Brandeis article
 - 3. Capsule summary of development since Warren-Brandeis

- II. History of Federal and State relationships on laws relating to concept of privacy and eavesdropping
 - A. Initial relationship w/ sample cases
 - B. Study of several concepts important to area of state-federal relationships
 - 1. Incorporation of Bill of Rights into 14th Amendment
 - 2. Exclusionary rule (Wolf, Mapp)
 - C. Present relationship and implications of this relationship

- III. Overview of present state laws on eavesdropping
 - A. Presentation of general summary of present laws
 - B. Distinctions, if any, in concept and/or effect of those states that now have laws
 - C. Analysis of ABA model eavesdropping code

- IV. New Jersey eavesdropping laws
 - A. History, if possible, of passage of laws - what forces aided or resisted passage
 - B. Listing of present law
 - C. Scope of actual surveillance
 - D. Presentation of state and private group's proposed recommendations for revision
 - 1. N.J. legislature committees (e.g. Rules of Evidence Com., Causes and Prevention of Crime Study Com.)
 - 2. National Commission of Review of Federal and State laws R lated to wiretapping
 - 3. Private groups (ACLU, law enforcement ass.)
 - E. Analysis of New Jersey present laws and proposed revision

- V. Possible investigation into municipal laws if enough research material can be found

- VI. Recommendations

Alex Hartnett
Privacy Com.

Richard W. Nenzo
The Boundaries of Privacy in American Society
Commission 1

The Psychological Impact of Privacy Invasions Upon the Individual

- I. The Forms of Privacy Invasions
 - A. Invasions of the Physical Life Space
 - 1. Crowding
 - B. Invasions of the Intellectual Life Space
 - 1. Wiretapping
 - 2. Stored Data
- II. Crowding
 - A. The Seriousness of the Problem
 - B. Serious Emotional and Intellectual Crises resulting from the phenomenon
 - C. Adaptability to the Condition
- III. Invasions of the Intellectual Life Space
 - A. Known manifestations of the suspicion or knowledge of observation
 - 1. For the potential Criminal (deterrence of crime)
 - 2. For the citizen innocent of criminal intentions
 - B. Effect of observation upon the Performance of:
 - 1. Simple Tasks
 - 2. Complex Processes
- IV. Recommendations
 - A. Are there means to mitigate the unhealthy effects of crowding or to facilitate adaptation?
 - B. Can the productivity of workers be improved by varying degrees of supervision?
 - C. Can the detection of crime be increased by augmenting observation without harm to the psychological welfare of innocent individuals?
 - D. Is a privacy right necessary, or are those who protest transgressions of personal freedom those who are culpable to society?

Preventing the Abuse of Stored Information
On the Federal Level

1) Limitations and Purpose of Paper

In general, the paper will not include the basis, justifications or reasons, legitimate or otherwise, for information collecting or storage. Nor will it study in depth what kind of information is presently stored, or should be stored. The other Commissions should establish the legislative and/or judicial standards for the protection of privacy. However, a distinction will have to be made between sensitive and less sensitive information (for example, national security) throughout the paper.

The purpose of the paper then becomes to devise means to prevent the abuse of stored information.

2) Access to federally held information

- a) present legislation and practice
- b) potential and actual infringements of privacy
- c) distinction btw. public officials and private cit.
 - 1) does public official have less right to privacy
- d) who should have access
 - 1) in general
 - 2) may info collected for one purpose be used for another
 - a) society right and individual right

3) Reliability of information

- a) present standards and practice
- b) means of insuring accuracy; correcting inaccuracy
 - 1) right of challenge, redress, use of multiple sources, hearsay, access of individ.

4) Leaks of information

- a) present means of dealing with leaks
- b) redress, responsibilities of gov. officials

5) Obsolete data

- a) what is meant by obsolete
 - 1) in terms of time; in terms of need for inf.
- b) means of destroying obsolete info and on what basis

6) Centralized "National" Data centers or Banks

- a) current and pat legislation, ideas
- b) potential dangers
- c) potential benefits
- d) relationship of data bank to:
 - 1) numerous federal agencies
 - a) the transfer of data problem
 - 2) legislative recs. of Commissions
 - 3) relat. with outline numbers 2,3,4,5

Theodore, J. Michael
October 6, 1971
Woodrow Wilson School of Public and
International Affairs
Conference on Boundaries of Privacy
in American Society
Commission on Private Data-Gathering
Activities

Communications Industry and the Invasion of Privacy

Statement of the problem: What are the usual invasions of privacy that the mass media commit? How do these invasions differ from other private and government invasions of privacy (e.g. motives and uses)? Are social ethics as important as legal precedents? What can the people, the government and the communications industries do to protect various rights and still maintain an open and responsible press?

I. Contemporary Examples of Invasion of Privacy

- A. Libel
- B. Invading private lives
- C. Crime and publicity
- D. "Secret" data-banks and dossiers
- E. Purposes and uses
- F. The right to invade privacy?

II. Legal Precedents Protecting the Press and the People

- A. Time, Inc. vs. Hill
- B. Times vs. Sullivan
- C. Warren and Brandeis on Privacy

III. Social and Ethical Values Protecting the Press and the People

- A. Situation ethics
- B. Technological advances in communications and evolving ethics

IV. Social Responsibility of Communications Industry

- A. The right to invade privacy, cont.
- B. Are a fair press and an open press incompatible?

V. Recommendations

- A. What the people can do
 - 1. the need for two-directional laws
- B. What the government can do
 - 1. FCC
 - 2. an FCC for newspapers
 - 3. a new first amendment
- C. What the communications industry can do
 - 1. existing codes
 - 2. revised codes

Commission I
The Scope of Surveillance Activity

- I. Who is under surveillance
 - A. Organization and Institutions
 - 1. Do they have any relation to each other?
 - 2. How long have they been under surveillance?
 - 3. Political affiliation
 - 4. Surveillance immunity
 - B. Private Citizens
 - 1. Do they have any relation to each other?
 - 2. How long have they been under surveillance?
 - 3. Political affiliation
 - 4. Surveillance immunity
- II. The present scope of surveillance activity
 - A. Numerical estimates of organizations, institutions under surveillance.
 - B. Numerical estimates of citizens under surveillance.
- III. Alleged surveillance selectivity
 - A. Organizations and Institutions
 - 1. Who they are
 - 2. Why chosen
 - 3. What the implications are
 - B. Private Citizens
- IV. Is data used to abuse others in any way?
 - A. Organizations and Institutions
 - 1. Peace, Civil Rights, Political right and left, etc.
 - B. Private Citizens
 - 1. Defamation of character, public ramifications
- V. What is being done with the data
 - A. The adequacy and precision of the data.
 - 1. Cases of surveillance by informants.

October 5, 1971
Eric H. Vinson '73

(continued)

II.

2. Tapes, taps, and other recordings taken out of context.

B. Kinds of assumptions made from data.

1. How many are positive and negative?

2. Forecasting after data is processed.

C. Data Storage

1. Public accessibility

VI. Counter-Action of surveillance by the observed

A. Legal counter-action

1. Court cases

B. Illegal counter surveillance techniques

C. Security procedures

Jeffrey C. Weil
Conference director:
Mr. Forgie
Commission 2

State Regulation of Private Sexual Activities of Consenting Adults

- I. Definition of Problem
 - A. Distinction between private and public behavior
 - B. Importance of consent
 - C. Concept of public morality
- II. Brief History of Problem
 - A. Edward Coke
 - B. William Blackstone
 - C. Others
 - D. Holfenden Report
- III. Current Laws of New Jersey and Illinois
 - A. Sodomy
 - B. Fornication
 - C. Incest
- IV. Administration of State Laws
 - A. Number and type of recent cases
 - 1. Methods of determination of sexual orientation
 - 2. Declared offense of suspect sexual activity to public morality
 - B. Discussion of acquittals
 - 1. Number of acquittals
 - 2. Reasoning behind decisions
 - C. Discussion of convictions
 - 1. Number of convictions
 - 2. Type of sentence
 - 3. Reasoning behind decisions
- V. Opinions of Community
 - A. Psychologist/psychiatrist/sociologist
 - B. Lawyers
 - C. Legislators
 - D. Clergy
 - E. Gay Liberation Front
 - F. Laymen
- VI. Recent Efforts at Legislative Reform
 - A. Historical description of efforts
 - B. Reasons for efforts
 - C. Likelihood of success
 - 1. Positive factors
 - 2. Negative factors
- VII. Evaluations and Recommendations of Report

Wolf, Robert A. '73
Conference on the Boundaries of Privacy in American Society
Committee III: Private Data-Gathering Activities

PHYSICAL AND PSYCHOLOGICAL SURVEILLANCE IN THE PRIVATE SECTOR

STATEMENT OF THE PROBLEM

Rapid gains in science and technology have made it easier than ever before, through the use of electronic devices and psychological tests, to discover what an individual is saying, thinking, and doing. The intent of this paper will be to examine how widespread is the use of such surveillance techniques in American society today, and to see whether their use poses a threat to the individual's right to privacy. This report will also deal with future improvements likely to be made in surveillance technology, and the implications of such changes for the rights of the average citizen.

- I. The Eavesdropper's Arsenal
 - A. Brief Description of Surveillance Devices
 - 1. The art of wiretapping.
 - 2. Hidden microphones, transmitters, and other snooping devices.
 - B. Surveillance Devices and the Mass Market
 - 1. Standard manufacture of these devices.
 - 2. Accessibility to the average citizen.
 - C. Likely Future Techniques of Electronic Eavesdropping
- II. Private Eyes, Spies, and Undercover Agents
 - A. The Growing Industry of Private Detection
 - 1. Who detectives work for.
 - 2. Use of electronic surveillance by the private eye.
 - B. Industrial Espionage
 - C. Industry and the Undercover Agent
 - 1. Detection of thieves.
 - 2. "Shoppers" who evaluate employees' performances.
- III. The Polygraph, or "Lie Detector"
 - A. History and Principle of the Lie Detection Machine
 - B. Industry's Uses of the Polygraph
 - 1. Evaluating potential and present employees.
 - 2. Uncovering thieves.
 - C. Reliability of Lie Detectors
 - D. Quality of Examiners
- IV. Psychological Testing
 - A. Personnel Selection
 - B. Testing in Schools
 - C. Typical Test Questions and the Threat to Privacy
 - D. Future Prospects for Psychological Surveillance
- V. Policy Recommendations