Rankin, Clyde E.
Conference on the Boundaries of
Privacy in the United States
Woodrow Wilson School of Public
and International Affairs
December 1, 1971

The Regulation of Stored Data
(Commission IV)

Modern society challenges past definitions of the right of privacy by generating increased pressure for personal and organizational information. For instance, our day-to-day decisions in business, government and social science require more and more data to forecast trends, predict outcomes, and generalize behavior. [1] Public service programs, economic programs and educational programs are neither funded nor enacted until sufficient data has been collected to ensure a reasonable amount of success. Public demand for increased crime prevention has resulted in more detailed police files, and the government's concern for domestic and international security has led to an increase in data-gathering on potentially dangerous individuals and groups.

This increase in data collection is as prevalent in the non-federal government and private sectors of our country as in the federal sector. The emergence of state data centers, credit bureaus, and the large scale communications industry has resulted in an increase of stored data. Much of this data is relevant and beneficial to the functioning of modern society. For example, predicted assurances of success in federal programs do help to secure appropriations from Congress, detailed police files do help law enforcement officials in their duties, and credit bureau reports do prevent the potential passing of bad checks and the resulting harm of this practice to society. But, this report will not discuss these beneficial results arising from the collection of data. Instead, this report will discuss some of the potential dangers of this increased data collection, the potentially harmful effects on society, and the present and potential invasion of privacy. The discussion will be limited to two basic questions; 1) what can be done with the data already already stored, and 2) what can we do with the data that is currently being collected?

The development and technological advancement of the computer poses a great potential threat to an individual's right to privacy. It is the computer that has made possible an efficient means of data transferal, storage and retrieval. This capacity, coupled with the increased tendency towards a centralization of data storage, necessitates immediate attention on stored data. Possible solutions to the present problem can be examined through

---

[1] Alan F. Westin, Privacy and Freedom, p. 321.

the study of present proposals and the thinking that they suggest.

First, the Bureau of the Budget, in 1961, decided to commission a study for the centralization and computerization of personal records in individual agencies of the Federal Government. The reasons for this study were simple: new advances in computer technology could make government record keeping and analysis more efficient and economical. The recommendations of the study were just as simple: a National Data Center is feasible and should be instituted promptly. [1]

This proposed National Data Center prompted the House Committee on Government Operations to convene the Special Subcommittee on Invasion of Privacy to study the ramifications of a National Data Center on the citizen's right to privacy. Their findings provoked heated debate and discussion, and brought the problem of stored data to the public's attention.

The subcommittee concluded that a possible threat to individual freedom was posed by the National Data Bank Concept. The data center could be misused intentionally or unintentionally through the long process of gathering and finally utilizing computerized information. In addition, it was evident, through the hearings conducted, that limitations on the type of data collected in the National Center would have to be defined. The security for this Data Center was another problem causing concern and disagreement. A report by Dr. Carl Kaysen, Director of the Institute for Advanced Studies at Princeton University, maintained that statutory provisions, provided there was no accumulation of individual dossiers, would be sufficient safeguards for personal privacy in a National Center. However, other testimony suggested that individual dossiers would inevitably be accumulated at a National Data Bank and that security of confidential information within a National Center would be more difficult than protection in existing federal agencies. Moreover, the danger of unauthorized access to information by outsiders or insiders is great, and this access could be inadvertent or intentional. Furthermore, the Federal Statistics User's Conference suggested improvements in the present federal statistical system that could make the creation of a National Data Center unnecessary. These conclusions were found to be relevant not only to the National Data Bank Concept but also to other data banks inside and outside the Federal Government. [2]

The subcommittee finally recommended:1) the priority of privacy in the design and implementation of any such data centers, and 2) that no work be done on a national data bank until these privacy matters are fully explored and guarantees provided.

Then, in 1970, Congress enacted the Fair Credit Reporting Act and included its provisions under the Consumer Credit Protection Act of 1968. The basic purpose of the act was to insure consumers that reporting agencies would exercise grave responsibility with regards to fairness, impartiality and respect for a consumer's right to privacy. The Fair Credit Reporting Act (FCRA) has authorization over credit bureaus, investigative reporting companies and other organizations whose business consists of gathering and

---

[1] U.S. 90th Congress, 2d Session, Thirty-Fifth Report by the Committee on Government Operations, "Privacy and The National Data Bank Concept, 1968, p.3

[2] Ibid., pp. 3-5.

and reporting information about consumers for use by others in making decisions concerning the granting of credit, the underwriting of insurance, or employment. The act states that users of consumer reports must inform consumers of adverse action taken on the basis of these reports. In addition, the consumer reporting agency must be identified. [1]

Unfortunately, the FCRA was seriously modified from its original form through a concerted lobbying effort by consumer reporting agencies. As a result, the enacted legislation limits the individual's access to his credit files, it does not place restrictions on other's access to files, and it ignores the question of sensitivity of information and the viable life-span of collected data. [2]

Nevertheless, there is additional legislation that has been passed, is pending or is in the form of proposals that deals with restrictions on data storage. For instance, Senate bill 823 sets various guidelines on the question of consumers and their credit files. This bill, along with House Resolutions 6071 and 16340, provides legislation for establishing the means by which a consumer learns of adverse credit reports and gains access to his file to correct disputed items. Furthermore, the bills provide regulations for flushing obsolete information and for informing individuals about investigative credit reports. [3] Moreover, there are several bills in the present session of Congress that deal with invasions of privacy by credit bureaus. These include Senate Bill 968 amending the Consumer Credit Protection Act and providing greater protection for consumers against unwarranted invasion of privacy, Senate Bill 652 amending the Truth in Lending Act to protect consumers against careless and unfair billing practices, and House Resolution 945 to enable consumers to protect themselves against erroneous, arbitrary or malicious credit information. [4]

There are existing laws, such as United States Code, title 45, section 3508, that deal with the transfer of stored information between federal agencies. This particular law helps to regulate stored data by prescribing the forms it must take in transmission. However, there are few provisions relating specifically to the question of the invasion of privacy. There is no provision establishing a "need to know" on the part of receiving agencies nor are there safeguards restricting the director of the agency to transfer information. [5]

In summary, there are existing provisions regulating certain aspects of the storage of data, there is growing debate on the issue of the invasion of privacy, and there have been investigations and reports on possible ways to handle the data already collected and stored. But, none of these proposals is all-comprehensive and all leave open serious questions as to implementation, expected success and worthiness. Nevertheless, it is the opinion of

---

[1] Federal Trade Commission, Bureau of Consumer Protection, Division of Special Projects, Compliance With the Fair Credit Reporting Act, 1971, p.1.

[2] James Kevin Burns, Non-Federal Data Storage and Retrieval and the Right of Privacy, 1971, p.10.

[3] U.S. Congress, House Committee on Banking And Currency, Subcommittee on Consumer Affairs, Fair Credit Reporting, 1970, p.23.

[4] U.S. 92d Congress, 1st Session, H.R. 945, S. 968, S. 652.

[5] Mark W. Stevens, Federal Storage of Personal Information, p. 21-22.

Commission IV that this debate and these provisions have been good for the American public. They have raised the important questions of what society is to do with the data it has collected, and secondly, how society is to prevent this data from causing damage or harm to individual citizens. These questions can not be answered quickly or easily. Rather, they form part of an on-going process that challenges man to deal with the world he inhabits. In responding to these challenges, man must seek solutions that deal specifically with existing situations and problems. The fact that we have stored data, and that there is immediate potential for invasions of privacy demands that our attention focus on solutions for the issues at hand.

First, computer systems are headed toward increased centralization. Independently developed systems have merged for economic and efficiency reasons. Federal agencies, bureaus, and departments are already operating line-sharing systems. The Administrator of General Services is urged, by Title 40, section 759 of the United States Code to transfer computers from agency to agency and to utilize them jointly to save money. [1] In essence, there already exists a national data center along the lines conceived by the Bureau of the Budget in the early 1960's. What we must face is the fact that some of the data stored in the existing systems is potentially harmful to the privacy of citizens. To deal with this problem, Commission IV recommends the implementation of certain safeguard devices in any computer system which handles potentially harmful information. These safeguards include: a) partitioning of the memory banks, b) simple encryption codes, and c) real-time monitoring and random auditing of the security system. [2]

The partitioning of memory banks would serve two purposes: "1) it would stop an unauthorized user who got past earlier safeguards and thereby gained access to the memory of a computer, and 2) it would prevent authorized users from exploring off-limits sections of the files." [3] Partitions will provide a "bulkhead" effect with walls of security that can prevent accidental access to files. In addition, real-time monitoring and random auditing of the system will detect deception when two users claim the same identity or when identically labeled terminals become connected. A monitor program will also review computerized records and will be able to erase obsolete data.

Protection of the transmission lines of time-sharing systems can best be accomplished with the use of encryption codes. These codes can prevent transmitted data from being easily intercepted. [4]

There are other safeguards that can be installed in computers but these three are sufficient for providing protection of personal information files. It is recommended that federal legislation require the installation of these safeguards on existing computers and all new computers. The installation costs will prevent voluntary safeguarding by the information industry.

---

[1] Stevens, op. cit., pp. 32-33.

[2] Robert M. Capuano, Technology and the Control of Stored Data, 1971, p. iv.

[3] Ibid., p. 28

[4] Ibid., pp. 25, 27.

Consequently, the federal government must intervene and establish the installation costs as a necessary price to pay society for the privilege of building a potentially dangerous system.[1]

The enforcement of these federal regulations and guidelines can best be accomplished through the licensing of computer systems, their owners and operators. An operating license would be granted to a computer or data system upon demonstration of the following: 1) the nature and purpose of the system, the use of the data, and the class of customers it will serve, 2) precise identification and description of the data sources upon which it will draw and the checks to be established to validate this information, 3) description of procedural safeguards to edit information errors, to resolve ambiguity in identification of an individual, to treat information of doubtful validity, and to establish confidence levels on information derived from fragmentary data, 4) description of all physical safeguards, 5) a description of the audit processes in the system, 6) a mechanism that permits an individual to review his dossier, the sources from which the information was gathered, and an opportunity to challenge or correct the content, and 7) the tests performed on the system to assure that it operates properly.[2]

This information would be received by a government regulatory agency that would have final authority on the issuance of licenses. These licenses would apply to private operators and government agencies. Suspension of operator's licenses or the system's license would be the penalty for misuse of information or violation of existing regulations.

This government regulatory agency, an arm of the executive branch of the government, would be both investigative and administrative. The degree of investigations and inspections would be determined by the nature of the data bank and the information it contained. Government intervention would be minimal on systems that contained statistical information that could not seriously harm an individual, while systems containing detailed individual dossiers would be watched closely. These investigative and administrative duties will involve a certain amount of technical competence and expertise. This expertise must be made available. Consequently, a certain degree of autonomy must exist with this agency to develop a degree of technical competence, a uniformity of purpose, and a degree of adequacy in applying its policy.

The guidelines for agency policy will be provided by Congressional legislation that outlines licensing procedures, requires safeguards and establishes installation deadlines.[3] In addition, a commission will be set up (within the agency) to conduct research on centralization trends, technological safeguards, and the potential effect of future computer systems on informative storage.[4]

The regulatory agency would acquire an ombudsman type approach in dealing with problems. It would be staffed largely

---

[1] Capuano, op. cit., p. 29.

[2] W. H. Ware, Computer Data Banks and Security Controls, March 1970, pp. 7-8.

[3] Burns, op. cit., p. iv.

[4] Stevens, op. cit. p. iv.

by career civil servants with time limitations on many administrative positions as an insulation against control by interest groups. The agency will have access to public input through its continuous investigations. In addition, any agency ruling involving the suspension of operating licenses may be appealed to a District Court. It is the belief of Commission IV that with statutory licensing of computer system owners and operators, and with the threat of suspension of these licenses, the bulk of security measures will shift to the computer systems. As a result, computer systems may become self-policing.

Nevertheless, there are some additional measures that can be taken to deal effectively with the present storage and collection of data. First, an effective and efficient Federal Statistics Office should be established to handle the need of interagency transferal of statistics. The records in this Office will be purely statistical with no individual identification. The same material will be available to all agencies in the same form. This action will acknowledge the existence of de facto data banks among government agencies. The uniform centralization of this statistical information will improve the efficiency of existing operations and allow the application of appropriate safeguards.

Second, the individual's right of access to personal information files, especially in the credit bureau business, must be strengthened. Amendments should be added to the Fair Credit Reporting Act and Consumer Credit Protection Act to establish greater protection for consumers against invasions of privacy. These amendments should require: 1) mandatory notification to individuals at the commencement of any investigatory credit reports, 2) periodic access granted to the individual to check for inaccuracies in files.

These recommendations involve the federal government for several reasons. First, the magnitude of the existing stored data and the potential for misuse of this information requires the full attention of federal authorities. An efficient means for implementing new procedures on federal, state and private levels is through the use of federal powers. In addition, the most efficient means of enforcing new procedures is through the various branches of the federal government. Second, the federal government, as the largest collector of data, must assume the responsibility of striking a balance between information that is necessary for the functioning of a modern society and information that strictly infringes upon the individual's rights of privacy. The federal government must be aided and advised in striking this balance with the cooperation of the computer industry and the general public.

Commission IV believes that a step toward reaching a common balance can be made through the implementation of federal regulations requiring safeguards, an agency enforcing these regulations, continued research on technological advances, and the strengthening of existing laws to protect individual privacy.

"There is no way to stop computerization. As Professor Robert M. Fano of MIT has Remarked, 'You can never stop these

things. It is like trying to prevent a river from flowing to sea. What you have to do is to build dams, to build water-works, to control the flow.' " [1]

C. E. Rankin

[1] Westin, op. cit., p.326.