618

Burns, James Kevin
Conference on the Boundaries
of Privacy in American Society
Woodrow Wilson School of Public
and International Affairs
November 18, 1971

NON-FEDERAL DATA STORAGE AND RETRIEVAL AND THE RIGHT OF PRIVACY

I. STATEMENT OF THE PROBLEM

The problem of this study is to investigate whether current controls over stored information are compatible with protection of a right of privacy in American society, and, if not, what measures should be taken to improve the situation.

II. SUMMARY OF PRINCIPAL FINDINGS

1. Data that has been and is being collected concerning individuals by non-federal interests is varied and extensive in nature. Current trends indicate that the amount stored will continue to increase.

2. New technology is enabling data to be stored and retrieved more easily and more efficiently than in the past, and consequently, more personal data is being stored. This ease has led to increased centralization of data storage and greater potential access to personal data.

3. Access to stored personal data has become increasingly easy, for reasons of both increased perceived legitimacy of the release of data on individuals and carelessness in self-regulation of release by data holders.

4. The current legal framework has been characterized by an evolutionary series of court decisions, and a failure of legislatures to establish coherent, comprehensive guidelines and laws to deal with present and future challenges to personal privacy. The result has been a general failure of the legal system to establish standards of data release, inaccuracy correction, storage safeguard and monitoring checks by the individual on whom data is held and released.

5. Given the current counter-privacy trends described in findings 1, 2 and 3, and given the continued failure of the legal system to provide comprehensive safeguards for the right of privacy, an immense decrease in the amount of personal privacy existing in American society is likely to become a continuing trend.

III. POLICY RECOMMENDATIONS

1. Comprehensive federal legislation should be enacted designed to define and protect individual privacy rights by providing regulation of the access to non-federal data files on individuals and checks to protect against inaccurate information being contained in those files (pp. 9-16).

2. A federal regulatory agency should be created to carry out the federal legislation and to make specific policy decisions relating the intent of the federal legislation to new developments in the art and use of data storage and retrieval.

> A new federal agency to safeguard the right of privacy could be created in such a way as to avoid its takeover by the interests it is created to regulate. Such an agency is necessary to make the highly complex policy decisions needed to carry out Congressional privacy legislation and provide the flexibility needed to meet a changing technological and social situation (pp. 10, 12, 16-18).

IV. TABLE OF CONTENTS

V. DISCUSSION

Whatever decisions are made to affect the collection of data on individuals, whether to limit, increase or leave unchanged information-gathering activities now in existence, there will still be serious issues involved with the data that has already been collected and data which will be collected in the future. Once the information has been gathered, by whatever means, decisions must be made to determine whether to release it at all and, if so, how, to what extent, to whom, when and for what reasons.

It is to this area that this paper turns, limiting itself to the non-federal sphere of personal data holders.[1] The major questions to be investigated by this study follow.

1. What is the situation now?
2. What does the future hold, and is the prospect desirable?
3. If the future seems less than idyllic, what options are available to remedy the situation, and which best suits both the long term and short term interests of the American people?

---

[1]The federal sphere of information-holders will be covered by Mark Stevens in his paper on federal personal data storage.

A major area which will not be covered by this study is a determination of what the right of privacy means in the United States. This will be handled by other papers in the Conference, specifically the study by Marilyn Green on the "moral and legal rights of the individual to privacy versus the government's need for surveillance,"[2] the study by Theodore Michael on the "Communications Industry and the Invasion of Privacy"[3] and the study by Betsy Freeman on "The Credit Bureau Industry and the Invasion of Privacy."[4] While crucial to a final resolution of the problem set before the Conference, the definition of privacy in America will not be the central focus of this paper. Thus, findings will leave room for a specific definition of the right of privacy while being more specific in relating this right to the non-federal data storage issue.

---

[2]Tentative outline list, Fall 1971 Policy Conference: "The Boundaries of Privacy in American Society," p. 5.

[3]Ibid., p. 5.

[4]Ibid., p. 9.

The Situation Now: Incremental Legal Change in the Face of Increasing Ease of Storage and Retrieval and Increasing Usage of Data Stores

The Extent of the Data Already Collected

While large-scale federal data collection dates back to the advent of income taxation and the New Deal,[5] and continues to expand at a prodigious rate, a large portion of current personal data collection and storage activities remains in non-federal hands. The personal data that has been collected by state and local governments and private interests varies in nature from statistical information on specific items such as age and income to highly subjective evaluations written by private investigators.

With the advent of increasingly efficient means of information storage and retrieval, more and more uses of personal data have been found economically justifiable, and the amount of data being collected and stored has expanded immensely.

> As if responding to something akin to Parkinson's Law, technological improvements in information-handling capability have been followed by a tendency to engage in more extensive manipulation and analysis of recorded data. This in turn has motivated the collection of data pertaining to a larger number of

---

[5] Arthur R. Miller, The Assault on Privacy: Computers, Data Banks and Dossiers, p. 20.

> variables, which results in more personal information being extracted from individuals.[6]

It is undeniably true that our highly intradependent society has a need to know some aspects of the personal lives of its members.

> As William Zelermyer, Professor of Business Law at Syracuse University, observes in his penetrating legal study, Invasion of Privacy, "Considering the complexities and overpowering demands of current living, privacy assumes the appearance of an imaginary luxury." The point must be conceded: there are "reasonable" encroachments on our privacy...[7]

At the same time it must be kept in mind that some degree of privacy, too, must be maintained if there is to exist any right of privacy at all. Somewhere between total disclosure and total secrecy must lie an accommodation of the needs and rights of society or its members to collect, store and use personal data, and the needs and rights of the individual to successfully withhold such data.

The Effect of the Computer

Most central to the modern technological support of increased personal information storage is the computer

---

[6] Miller, op. cit., p. 21.

[7] Myron Brenton, The Privacy Invaders, p. 13.

and its immense capacity for efficient storage and selective retrieval of data. Computerization of data has encouraged increased centralization of information storage, while hardware and software advances within the field have encouraged easy mechanical access to central data stores. In considering the National Data Bank proposal, the House Committee on Government Operations listed as one of its findings that "Testimony (sic) and studies suggest that individual dossiers (i.e. ways of storing all information on an individual in one place or of compiling it quickly) cannot be avoided under the envisioned National Data Bank."[8] The increasing storage capacity and ease of retrieval and the tendency towards centralization of data storage posed by computer technology all offer significant potential threats to effective restriction of the flow of stored personal data.

The Immediate Legal Background: An Overview

Judicial Evolution

Protection of the right of privacy by judicial decisions has proven inadequate to coping with the continuing erosion of privacy that has spread greatly with the advent of the computer and what Arthur Miller calls

---

[8] U.S. 90th Congress, 2nd Session, Thirty-fifth Report by the Committee on Governmental Operations: "Privacy and the National Data Bank Concept," 1968, p. 4.

"the dossier society."[9] The courts have naturally approached privacy issues on a case by case basis and, while the resulting judicial framework within each state is by definition coherent, it is neither comprehensive in coverage nor characterized by concerted planning to accommodate a right of privacy to a rapidly-changing technological storage and retrieval potential. In addition, the judicial approach to protection of the right of privacy has the distinct disadvantage of reacting slowly to stimuli for change. These criticisms are of built-in characteristics of American judicial decision-making and, to the extent that the judicial framework is inadequate to protecting the right of privacy in the complex, technologically-dynamic field of information storage and retrieval, it is not the fault of the judicial system, but of the approach of relying too heavily upon protecting the right of privacy through that system.

The judicial definition of the right of privacy is derived primarily from natural law,[10] being only touched upon in the written Constitution. Until a stated right of privacy may be formally amended onto the Constitution, the courts cannot be expected to balance other Constitutional rights against a right of (continued on next page)

---

[9]Miller, op. cit., p. 20.

[10]Brenton, op. cit., p. 19.

privacy and find a median that will effectively protect personal privacy from significant further losses.

> The established tort doctrine relating to our problem follows: If accurate information is disclosed out of the subject's file, there is no liability unless disclosure is made to a great number of people, however sensitive the information may be ... Meager as it is ... the law of torts is at present the principal legal protection against unjustified access to data in nongovernmental files...[11] underlining inserted

The courts do provide for redress in the case of inaccurate information distribution, although it has become very difficult to claim damages (in the case of the media publishing an untrue newsworthy story, the person seeking retraction or damages must prove that the media knew beforehand that the knowledge was false or that the media acted with reckless disregard of whether the item was false or not).[12] The American Law Institute's Restatement of Torts, Second Tentative Draft 13 §652 (1967) reads in part, "The right of privacy is invaded when there is ... (d) Publicity which unreasonably places the other in a false light before the Public."[13] [underlining inserted]. However, whether or not inaccurate information has been publicized if given to selected people is one crucial question here, and beyond

---

[11] Kenneth L. Karst, "'The Files': Legal Controls Over the Accuracy and Accessibility of Stored Personal Data," Law and Contemporary Problems, p. 347.

[12] M. C. Slough, Privacy, Freedom and Responsibility, p. 71.

[13] Berton R. Clarke, "The Dossier in Colleges and Universities," On Record, p. 71.

the consideration of damages is the undesirability of correcting inaccuracies in records after they have been publicized. The major problems presented here are the prior inaccessibility to the individual's dossier of the individual himself (to discover what is inaccurate) and the vagueness or selectiveness of recorded data and commentary (for which there is little hope of judicial correction).

Legislation

Current legislation does provide a certain degree of standardization and privacy protection in access and accuracy controls, often evidenced through similar self-regulation by state and local public agencies, and governmental standards placed on private information holders. State and local regulation, however, has not established any comprehensive non-federal data holder guidelines yet.

The Fair Credit Reporting Act of 1970 was a significant step in the direction of comprehensive privacy protection. The credit information network has control over much data on the personal lives of individuals and this bill attempted to provide a certain degree of consumer protection against inaccuracy and biased data collections in credit reporting agencies. However, the bill ran into serious modification problems in committee and, in the form finally

passed, gave the individual the right of access to his file, ensured his notification if a report affected him adversely in a credit decision and somewhat restricted non-credit investigations into credit files. However the questions of who, exactly, shall have access to a person's file and how information shall be determined outdated or too sensitive for further distribution were not considered in the final bill.[14]

While legislative enactment of a comprehensive federal privacy act regulating information flows is desirable for reasons of uniformity of law and centralized enforcement, it must also be recognized that hasty action might result in legislation inadequate to meeting the challenges of rapid hardware and software evolution. This consideration has probably been a major factor in inhibiting the development of comprehensive legislation.[15]

---

[14] Miller, op. cit., p. 88.

[15] Ibid., p. 224.

The Major Alternatives Available For Safeguarding the Right of Privacy

The data storers can not be relied upon to self-police the accuracy of their information and provide sufficiently effective access regulations. The free market of information offers some help in discrediting sources of egregiously poor information, but this process is much too time-consuming and uncertain in the face of rapid technological innovation and proliferation, and in the face of the large numbers of individuals who are meanwhile having decisions made against them for reasons of inaccurate or incomplete data. The data storers also cannot be relied upon to regulate access to their stores, for the result has been lax access restrictions at many data denters.

The judicial framework of the society, too, is incapable of leading the way in determining standards of privacy protection (for reasons discussed under Judicial Evolution, pages 6-9). The assurance of privacy is not a matter to be left mainly to precedent and natural law, for the challenge to privacy has become too extensive and too adaptable for courts to be fully successful in meeting it.

In many areas the courts have specifically left action up to the legislatures. While a Constitutional Amendment is a possibility, it would be time-consuming and very possibly impossible to pass and ratify, relatively inflexibly set upon its course once initial decisions come out based upon it, and still contain the inherent lack of quick reaction and a planning function.

Legislation, although by no means a magic formula, offers the most realistic hope of controlling further enoroachments into the right of privacy. The national level is most fitting to attack the problem on since the most serious threats in the way of data networks extend accross state lines. Also, a uniform law would provide a protective base upon which states could build further safeguard regulations. There is much to be said for enacting comprehensive legislation which would include a statement of the individual's right to privacy, regulations to protect it and sufficient flexibility and broadness of scope to be adaptable to technological and societal changes while not being so loose as to prove ineffectual or so tight as to seriously handicap the data storage industry.

Legislation aimed at a particular problem suffers the disadvantage of a certain degree of tunnel vision in

not seeing that problem as part of the larger issue of what the limits of privacy are in the United States. Also, the specific problem approach is more likely to tend only to the problems which are foremost in the public's consciousness and the Congress's consensus. This may leave many less obvious or more disputed portions of the issue unaffected.

While the enactment of national comprehensive legislation seems most useful in facing the challenge now presented to privacy in American society, this paper's recommendations must of needs be limited to that part of the problem posed by the two major components of data storage decision-making: retrieval decisions (including access restrictions and protection against unauthorized access) and accuracy checks.

Accuracy Checks

Turning to the latter components first, this study concludes that certain regulatory checks against inaccuracy of data in the system are highly desirable. A first check would be the registration of all interstate personal data banks[16] to provide knowledge of who is

---

[16]Miller, op. cit., p. 227.

storing data.

A second check would involve the individual's right to periodically (every time an addition is made) have access to his complete dossier at every center which has a file on him or mentions him in any other file such as a group file or another individual's file (in files which are not specifically concerning him, his access right would only be to those portions which give the substance of his involvement). Each data holder must inform individuals upon whom it has a file or who are mentioned in a file of the file's existence within a reasonable period of time following the file's creation (length of time to be fixed by statute: the shorter, the better).

This study recommends, however, that the data holders included in this check exclude those who use the information solely for internal purposes (e.g. employee files not subject to external access, police and F.B.I. files on criminals, suspects and potential suspects that are not subject to external access, mental hospital files, etc.). This recommendation is in recognition of the right to privacy of the data holders themselves.

Internal files can be abused, as in the case of the confidentiality of performance reports in an employee's

file. This abuse has most recently been given wide media coverage in the case of Foreign Service promotion and selecting out (firing) practices. While this is part of a serious problem with many employee files, the constitutionality and the efficiency of any sort of enforced access regulation in the internal files of an employer is doubtful. Self-regulation will have to remain the principal privacy protection in this case.

Once having access, the individual would have the right to correct inaccuracies and challenge information he disagrees with by informal discussion with the data holder or, that failing to reach an agreement, by mandantory arbitration with an agent of the Federal Privacy Agency (see page 16). If internal files are needed to justify externally-accessible ones during arbitration, then the arbitrator must be shown the relevant portions of those files and he will consider their contents confidential. Failing success in the arbitration stage of his contention, as would be the case with much subjective data, the individual would have the right to enter countering information into the file to be distributed whenever the contested information is given out.

Relying upon the individual to correct inaccuracies,

coupled with penalties for dissemination of inaccurate materials (removing the "qualified privilege" protection from data holders), seems to be a relatively easy way of at least providing the citizen the option of correcting inaccurate files. As a final part of the second check, data centers would be obligated to inform the individual of additions to his file as they are made[17] (and before they are disseminated).

As a third check, all data must be identified by source and date of submission in any report on an individual made by a data holder. The data holder need not reveal the source to the individual, however, since the individual's right is to challenge the data, not the source. In arbitration, however, the arbitrator must have access to the source of the information being challenged and, again, he will consider the source confidential. The date of submission is to be available to the individual, leaving upon him the burden of expunging obsolete data.

First Amendment guarantees will exempt the press from regulation, and may challenge the enforced arbitration recommendation as leading to an abridgement of free speech. If the latter occurs, then either the individual or the data

---

[17]Miller, op. cit., p. 227.

holder may have to resort to the courts to resolve a challenge to the accuracy of information in the file. Such might prove to be a strain on the court system's already strained docket. Hopefully the large majority of disputes will be settled directly between the data holder and the individual.

Access Regulations

The problems of who should be permitted to look through files concerning individuals and whether data should be available for purposes other than those implied at the time of collection are both important and complex, and any decisions on the access problem enacted into legislation may easily bear the scars of innumerable interest group clashes. Some general recommendations can be made, hoever.

First, as mentioned in the section on inaccuracies, the individual should generally have access to his own file.

Second, guidelines will have to be established concerning the use of collected information for purposes other than those implied in the collection process. A required contractual note at the end of each questionnaire or other data collecting mode asking the informant whether he will permit the dissemination of his information for purposes other than those implied in the data collection would help solve this dilemma without arbitrarily denying entire classes of information seekers access to personal data files or allowing the data storer fairly unlimited distribution of information. Concomitant with such a policy might be

a sensitivity classification for volunteered data to restrict access to certain groups or persons having certain access qualifications, together with a policy of providing a note on how much of an individual's dossier has not been released in each report to information seekers. Non-volunteered data could be required to have a predetermined sensitivity classification. Such a sensitivity classification system would be used only for data of a personal nature. A suggested system follows.

Sensitivity 1 - only for the purpose implied in the collection (individuals described have access if purpose involves external access)

Sensitivity 2 - internal use only

Sensitivity 3 - listed uses only (individuals described have access)

Sensitivity 4 - open for various uses at the data collector's option (individuals described have access before external use is made)

Sensitivity 5 - available to the public

Data transfered to another data holder under Sensitivity 3 classification would not be transfered unless the second data holder agreed to abide by the classification's restrictions.

Third, a sense of strict security-mindedness should be instilled in data centers holding personal data. Here is where licensing could have a strong influence, if a prerequisite for provision or renewal of the license is adherence to a set of strict security measures, including hardware and software checks against electronic espionage and accidental dumping of data, and personnel checks to insure against leaks and carelessness. Professionalization of the information retrievers should be encouraged, perhaps by licensing key positions, and penalties for leaking information should be severe.

The complete considerations and practicalities of national privacy legislation are overwhelming for a study of this length. For some years now the Congress has been investigating the problem of massive data storage and its retrieval and accuracy. The problem is largely a political one now, for the information needed to synthesize national comprehensive legislation is already available in thousands of pages of Congressional hearings. Privacy simply is not a sufficiently burning issue at this time and resistance to key aspects of any comprehensive bill will be strong. Nevertheless, what is needed is a comprehensive proposal to work on.

To develop comprehensive national legislation, a task force should be appointed and given a date to have a proposal ready by. In addition to proposing Congressional authorization of privacy regulations, the task force should also be directed to draw up a proposal for a new federal agency to actually regulate the data storers.

A New Federal Agency

The Federal Privacy Agency's authorization should charge the agency with specific implementation of the privacy legislation and its guidelines, arbitration of data accuracy disputes (pages 13a, 13b, 13c), licensing of interstate personal data networks which allow external access to their files (page 15), and a planning function and the ability to adapt regulations to meet new situations.

Its composition would have to include data specialists, lawyers and professional arbitrators. The agency should have an executive board to determine policy with members to be appointed by the President and ratified by Congress. This board should be composed so as to provide representation to both the data holders and private citizens and each members should serve a two year term, half to be appointed each year. The size of this board should be determined by the task force keeping in mind the needs of adequate representation and

efficiency.

The agency is not envisioned as a large one; rather, much of its effect should be felt indirectly as most disputes hopefully will not come to its attention. For the licensing function, spot inspections will be made, but not extensively. Part of the inspections will include an attempt to obtain some of the stored data, thus testing the safeguards.

Any disputes between the agency and those it is attempting to regulate shall be settled through the courts, with court injunctions available to enforce temporary cease and desist action until the issue can be settled.

The annual cost for this agency should not exceed $10 million (based upon 400 employees, including staff, at an average expenditure of $25,000 per employee). The task force may find this figure inadequate to the need, but more likely will find the financial needs of the agency well within this figure. Of more significance will be the cost incurred by obeying federal regulations to the data storage industry as a whole. This cost will be appreciable, but has been minimized where possible (in the case of accuracy checks, relying upon the individual to actively correct his files saves much industry expense and the three software regulatory recommendations made by Steve Capuano in his paper on computer

technology and safeguards are both efficient and effective). Much of the cost of data protection and accuracy will be absorbed by the continuing increase in storage efficiency brought about by computer hardware and software evolution.

The advantage of using a new agency would be to ensure primary responsibility and capability over privacy protection and to attempt to build in independence of the interest groups it will affect. The latter problem has distorted the protective effectiveness for the consumer of several federal agencies in the past, and a privacy agency inclined to favor the information storers would do serious harm to what remains of American privacy through dragging its feet while purporting to be taking adequate care of the individual's privacy rights. Senator Ervin of North Carolina was optimistic on the topic of a new agency in his speech at the Wharton School of Finance in 1969:

> I believe we have learned enough over the past 50 years about the design and operations and problems of regulatory agencies to enable us to create one which has built-in protections to assure that it serves the interests of the individual citizen and not solely those of the industry it is supposed to regulate.[19]

The new agency would have to have both the independence and the consumer responsiveness, the broadness of authorization and the funding to carry out the legislated regulations and react to continuing changes in

---

[19] Miller, op. cit., p. 233.

information storage hardware and software as well as shifts in American society's conception of a right of privacy.

Concluding Remarks

The threat to perceived norms of privacy in the United States is a serious and continuing one. The trend this society is moving in is unmistakably towards an ultra-dossiered society, where the files on each individual are both extensive and multipurpose. Self-regulation and the discrete approaches judicial decisions and legislative regulations have followed in the past leave too many loop-holes and grey areas in a right of privacy which has only partial definition. Hardware and software innovations continue to permit ever-increasingly efficient and effective storage and retrieval system capabilities to develop, while security, legitimate access regulations and inaccuracy checks range widely in effectiveness and protection for the individual described in the files. Without a compre-hensive approach to the problem, the right of privacy will continue to be eroded. It is hoped that with the establish-ment of a regulatory agency with definitive Congressional authorization and direction, individuals may receive a clear and protected definition of the right of privacy and its boundaries in American society.

VI. BIBLIOGRAPHY

Books

Breckinridge, Alan C. The Right to Privacy. Lincoln,, University of Nebraska Press, 1970.

Brenton, Myron. The Privacy Invaders. New York, Coward-McCann, 1964.

Clarke, Arthur. Profiles of the Future. New York, Harper, 1962.

Clarke, Berton R. "The Dossier in Colleges and Universities," On Record. Stanton Wheeler, editor. New York, Russell Sage Foundation, 1969.

Computers and the Law (American Bar Association Standing Committee on Law and Technology). Robert Bigelow, editor. 2nd ed. New York, Commerce Clearing House, 1969.

Kahn, H. and Weiner, A. The Year 2000. New York, McMillan, 1967.

Miller, Arthur. The Assault on Privacy: Computers, Data Banks and Dossiers. Ann Arbor, University of Michigan Press, 1971. (highly useful and well documented).

Slough, M. C. Privacy, Freedom and Responsibility. Springfield, Thomas, 1969.

Westin, Alan. Privacy and Freedom. New York, Atheneum, 1967.

Periodicals

Bennett. "Secrets Are For Sharing," Psychology Today. February 1969.

Comment. "Privacy, Defamation and the First Amendment: The Implications of Time, Inc. v Hill," 67 Columbia Law Review 926, 1967.

Dixon, "The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy." 64 Michigan Law Review 197. 1965.

Periodicals (cont'd)

Karst. "The Files: Legal Controls over the Accuracy of Stored Personal Data." 31 Law and Contemporary Problems 342. 1966.

Note. "Privacy and Efficient Government: Proposals for a National Data Center." 82 Harvard Law Review 400. 1968.

Sawyer and Schechter. "Computers, Privacy and the National Data Center: The Responsibilities of Social Scientists." 23 The American Psychologist 810. 1968.

Government Publications

U.S. 89th Congress, 2nd Session. Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives. The Computer and Invasion of Privacy. Washington, Government Printing Office, 1966.

U.S. 90th Congress, 2nd Session. Thirty-Fifth Report by the Committee on Government Operations, House of Representatives. Privacy and the National Data Bank Concept. Washington, Government Printing Office, 1968.

(Both these publications were excellent for touching across the board on their topics. The former especially was exceedingly interesting to read and very useful as a primary document where the arguments flowed freely and coherently).