DePaul Law Review

Volume 20
Issue 4 *1971*

Article 10

The Assault on Privacy by Arthur R. Miller

Charles R. Ashman

BOOK REVIEW

The Assault on Privacy. BY ARTHUR R. MILLER. Ann Arbor, Michigan: University of Michigan Press, 1970. Pp. 320. $7.95.

In 1890 Louis D. Brandeis warned that mechanical devices threatened to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops.[1] Now in 1971 Arthur Miller warns that a "Dossier Society" nurtured by computers threatens to destroy the essence of that personal privacy that is fundamental to democracy.[2]

The eighty-one years between these two warnings have been filled with sophisticated business inventions and techniques making it increasingly impossible to secure to each individual what Judge Cooley called the right "to be let alone."[3]

The emotionalized concept of privacy has faced continuing difficulty in its quest to become a "right" within our legal system. Exasperatingly vague and evanescent as a doctrine, it is all things to all men.[4] Rhetoric over the conflict between constitutional guarantees of the individual and the people's right to know often neglects to include the former beneficiary within the latter. Our national pride is offended when we dilute our open society's concentration, and yet we cringe at sacrificing personal autonomy to the intrusion of government and our fellow man.

Recently lawyers and a growing segment of social scientists have determined that a basic element of the right of privacy is the individual's ability to control the distribution of information relating to him.[5]

Miller in his book has issued a call to arms for a reticent society too busy or too naive to recognize the symptoms of computer suffocation. As a repository of knowledge and problem solving device, the computer has no peer. As in the case of most other significant industrial breakthroughs, there is tremendous feed-back—in this case, the sacrifice of privacy. Professor Miller believes our legal system has not responded to the implications of this new technology. In a well organized and impressively documented treatise, he has gauged the dehumanization process that irresponsible computerizing controls.

---

1. Warren & Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 5 (1898). For a comprehensive treatment, *see* Forkosch, *Freedom of Information in the United States,* 20 DE PAUL L. REV. 1 (1971).

2. MILLER, ASSAULT ON PRIVACY, 259 (1970).

3. COOLEY, TORTS, 29 (2d ed. 1888).

4. Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?,* 31 LAW AND CONTEMP. PROBLEMS 326 (1966); WESTIN, PRIVACY AND FREEDOM (1967).

5. Fried, *Privacy,* 77 YALE L.J. 475 (1968); Beaney, *The Right To Privacy and American Law,* 31 LAW AND CONTEMP. PROBLEMS 253 (1966).

As "Orwell's 1984" becomes only a little more than a decade away, "Big Brother" becomes less science fiction and more a relevant facet of life in the most advanced technological society history has known. One wonders if a world that watches its ambassador-astronauts putter on the moon can be less watchful of its populace at ground level.

Apprehension over the computer's threat to personal privacy seems particularly warranted when one begins to consider the possibility of using the new technology to further various private and governmental surveillance activities. One obvious use of the computer's storage and retrieval capacity along these lines is the development of a "record prison" by the continuous accumulation of dossier-type material on people over a long period of time. The possibility of constructing a sophisticated data center capable of generating a comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a national network is one of the most disturbing threats of the cybernetic revolution.[6]

Police on every level and military intelligence agencies have gained access to various communications outlets and are compiling a mass of computerized files on millions of law abiding yet "suspect" Americans.[7] The present administration's justification that an era of assassinations, violent dissent and civil disorder requires the government to accumulate dossiers on "people of interest" is not holding up to the man in the Senate or the man in the street. This issue as well as related spying tactics may well be the final straw in harnessing, if not breaking the back of J. Edgar Hoover's perennial personal reign of the F.B.I.

The threat of police-state tactics has raised critical constitutional questions and the computer-critics have achieved formal congressional inquiry into the indiscriminate collection and use of information on noncriminals for whatever purpose.

Computers are now fed such miscellaneous data as details from elementary and secondary schools as well as college records; aptitude, intelligence and personality tests results; tax returns, census findings and social security information; insurance applications, hospital records and military files; credit bureau records; employment reports; voter registration and court dockets; airline, hotel and automobile rental listings and credit card applications and files. Although not all sources have reached the sophisticated intrusion level of census information which is elicited under threat of criminal penalty,[8] our courts have upheld the Bureau's growing discretion in the proliferation of census questionnaires for the dubious needs of federal agency planning.[9]

---

6. *Symposium—Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968).

7. N.Y. Times, June 28, 1970, at 1, col. 2.

8. 13 U.S.C. §§ 221-24 (1964).

9. United States v. Rickenbacker, 309 F.2d 462 (2d Cir. 1962), *cert. denied*, 371 U.S. 962 (1963). We continue to speculate as to whether Mr. Rickenbacker was prosecuted for failure to honor the census or for publishing his criticisms. *See* Rickenbacker, *The Fourth House*, NATIONAL REVIEW, May 21, 1966, at 325.

The author is rightfully uneasy about private access to governmental agency personal data and the menace to privacy inherent in the accumulation of voluminous information.

The heretofore inaccessability of federal records by employees, creditors and others was significantly reduced by the 1967 statute, idealistically entitled *The Freedom of Information Act*,[10] which requires broad disclosure by government agencies. Among the diverse judicial applications of the Act to date have been: A businessman's request for General Services Administration's financial records to help justify tax listings;[11] a draftee's inquiry about members of his draft board;[12] and a historian's efforts to prove-up forced repatriation of nearly a million anti-communist Russians after World War II.[13] The stated purpose of the Act was insuring adequate public access to government agencies and administrators. It should be noted incidental to this means of possible official abuse is the sacrifice of the individual's right to restrict circulation of that which he divulges to his government.[14]

In a recent series of speeches on the floor of the Senate, Senator Sam J. Ervin, a former judge and author of the forward in this book, has claimed that computer technology is forcing our country into an unprecedented mass surveillance system. The information or "data base" for a Secret Service computer name check flows into the protective intelligence division from many sources—abusive or threatening letters or telephone calls received at the White House, F. B. I. reports, military intelligence, the Central Intelligence Agency, local police departments, the Internal Revenue Service, Federal building guards, individual informants.

Among the worst kept secret data sources intruding into the remnants of privacy are:

(a) A Secret Service computer, one of the newest and most sophisticated in Government. In its memory the names and dossiers of activists, "malcontents," persistent seekers of redress, and those who "embarrass" the President or other Government leaders are filed with those of potential assassins and persons convicted of "threats against the President."

---

10. 5 U.S.C. 552 (Supp. III, 1965-1967); Paul, *Access to Rules and Records of Federal Agencies: The Freedom of Information Act*, 42 LOS ANGELES BAR BULLETIN 459 (1967); Note, *The Information Act: Judicial Enforcement of the Records Provision*, 54 VIRGINIA L. REV. 466 (1968).

11. General Services Administration v. Benson, 415 F.2d 878 (9th Cir. 1969).

12. Martin v. Neuschel, 396 F.2d 759 (3rd Cir. 1968).

13. Epstein v. Resor, 421 F.2d 930 (9th Cir. 1970).

14. The fundamental conflict between these two objectives is perhaps best illustrated by the following excerpt from the statement of President Johnson on signing Public Law 89-487 (the Freedom of Information Act) on July 4, 1966, reprinted in United States Department of Justice, *The Attorney General's Memorandum on the Public Information Section of the Administrative Procedure Act ii* (1967) [hereinafter Attorney General's Memo]: "A citizen must be able in confidence to complain to his Government and to provide information. . . . Fairness to individuals also requires that information accumulated in personnel files be protected from disclosure. . . . I have always believed that freedom of information is so vital that only the national security, not the desire of public officials or private citizens, should determine when it must be restricted."

(b) A data bank compiled by the Justice Department's civil disturbance group. It produces a weekly printout of national tension points on racial, class and political issues and the individuals and groups involved in them. Intelligence on peace rallies, welfare protests and the like provide the "data base" against which the computer measures the mood of the nation and the militancy of its citizens. Judgments are made; subjects are listed as "radical" or "moderate."

(c) A huge file of microfilmed intelligence reports, clippings and other materials on civilian activity maintained by the Army's Counterintelligence Analysis Division in Alexandria, Va. Its purpose is to help prepare deployment estimates for troop commands on alert to respond to civil disturbances in 25 American cities. Army intelligence was ordered earlier this year to "destroy a larger data bank and to stop assigning agents to 'penetrate' peace groups and civil rights organizations." But complaints persist that both are being continued. Civilian officials of the Army say they "assume" they are not.

(d) Computer files intended to catch criminal suspects—the oldest and most advanced type with the longest success record—maintained by the Federal Bureau of Investigation's National Crime Information Center and recently installed by the Customs Bureau. The crime information center's computer provides 40,000 instant, automatic teletype printouts each day on wanted persons and stolen property to 49 states and Canada and it also "talks" to 24 other computers operated by state and local police departments for themselves and a total of 2,500 police jurisdictions. The center says its information is all "from the public record," based on local and Federal warrants and complaints, but the sum product is available only to the police.

(e) A growing number of data banks on other kinds of human behavior, including, for example, a cumulative computer file on 300,000 children of migrant farm workers kept by the Department of Health, Education and Welfare. The object is to speed the distribution of their scholastic records, including such teacher judgments as "negative attitude," to school districts with large itinerant student enrollments. There is no statutory control over distribution of the data by its local recipients—to prospective employers, for example.[15]

What constitutes a computer-worthy "threat" thus becomes important. The government claims it applies easy-going and "sophisticated" standards in deciding who is to be encoded. Critics argue that the vast capacity of a computer for names and dossiers—unlike that of a paper filing system, which has a self-limiting ceiling based on the ability to retrieve—is an encouragement to both unlimited growth and error.

As Professor Miller suggests, the present state of the law on privacy is unsettled and strained as social philosophers and legislators are applying doctrines to changes far beyond their original contemplation. Further confusion is caused by the legal system's hemorrhage over wiretapping. The Federal Government's justified electronic eavesdropping plans have already been ruled unconstitutional by the prestigious United States Court of Appeals for the Second Circuit[16] and Attorney General Mitchell will appeal to the Supreme Court.

At one time "dossiers" were reserved for those few who had achieved spectacularity through public life. However, millions of Americans have now been invaded by an army of computers, programming devices and data banks. Today, it is the exceptional American who does *not* live in the shadow of his tape or electronic counterpart.

---

15. N.Y. Times, June 28, 1970, at 42, col. 1.

16. United States v. Sinclair, 321 F. Supp. 1074 (E.D. Mich. 1971); United States v. United States District Court, 444 F.2d 651 (6th Cir. 1971).

The Assault on Privacy is an extremely important book on a frighteningly imperative subject. Miller has shown grace and style in analyzing today's threat, and reason in prophesizing tomorrow's even greater dangers. The computer cannot make a moral judgment—human dignity must be preserved even as we technologically advance or mechanical force may preempt the more vital human force.

CHARLES R. ASHMAN*

---

* MR. ASHMAN *is former Dean of the Riverside University Law School, Director of the Belli Foundation, and author of the book,* THE SUPREME COURT IS DYING.