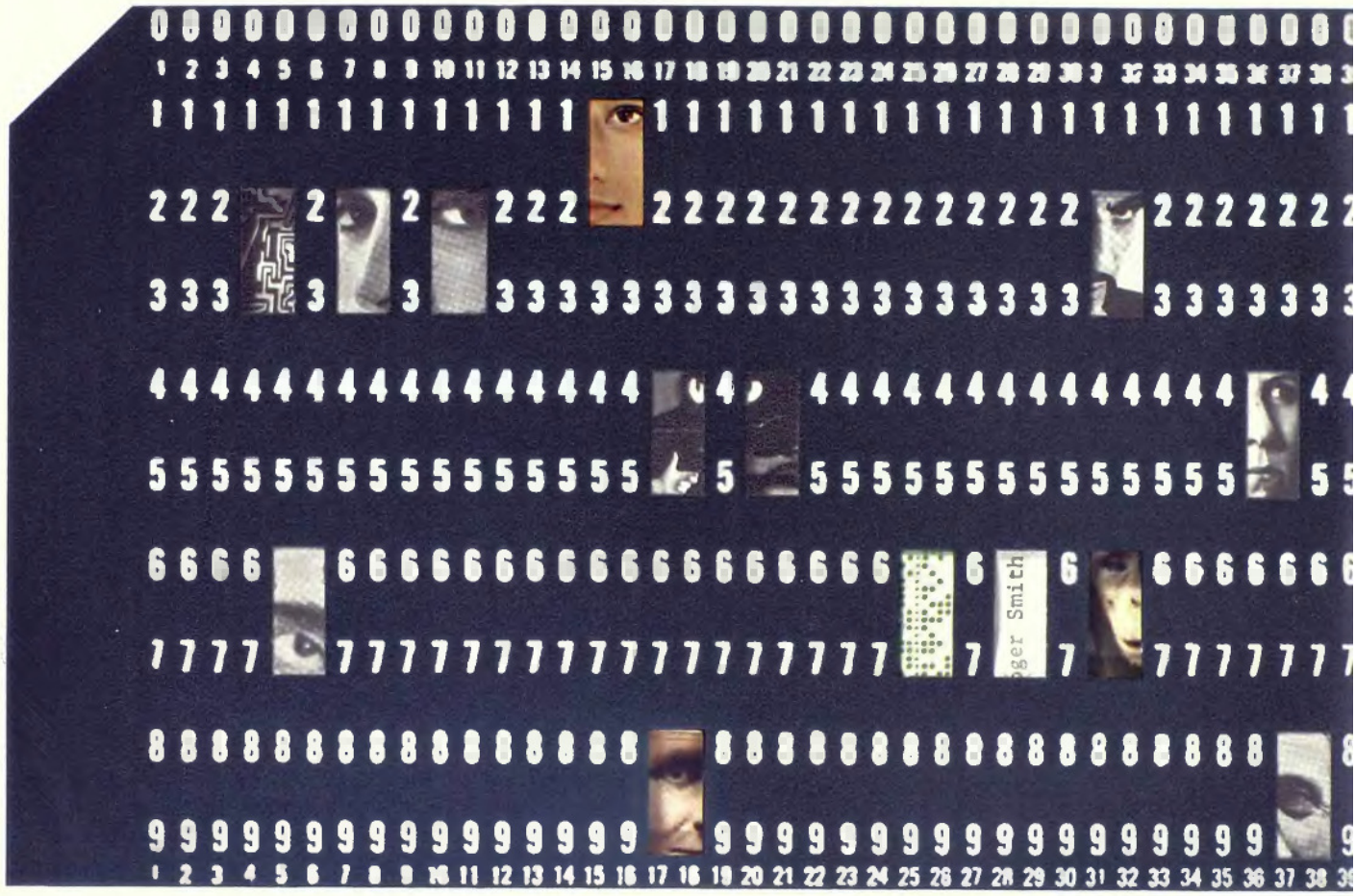


THE YEAR IS 1975. The place is a suburb in the United States. The setting is a record-control society that could make George Orwell's Oceania almost look like a haven of privacy.

At seven A.M., our typical citizen, an engineer named Roger M. Smith, wakes up, dresses, has breakfast and gets ready to commute by car to his office in Central City. Already, heat, light and water records fed directly from his home to the Central City Utility Corporation (for purposes of billing and use analysis) provide data that can establish when Smith got up and just how he moved through his house.

Smith takes his car out of the garage and drives onto the turnpike, heading downtown. As he reaches the tollgate, his license plate is automatically scanned by a television camera and his number is sent instantaneously to an on-line computer containing lists of wanted persons, stolen cars and traffic-ticket violators. If Smith's plate registers a positive response, police stationed 100 yards along the turnpike will have the signal before Smith's car reaches their position.

As he stops at the tollgate, Smith gives the initial performance of what will be a ritual repeated many times during the day. He places his right thumb in front of a scanning camera. At the same time, he recites into the unit's microphone, "Smith, Roger M., 2734-2124-4806." Roger has just used his thumbprint, voiceprint and personal identification number to carry out his first financial transaction of the day.

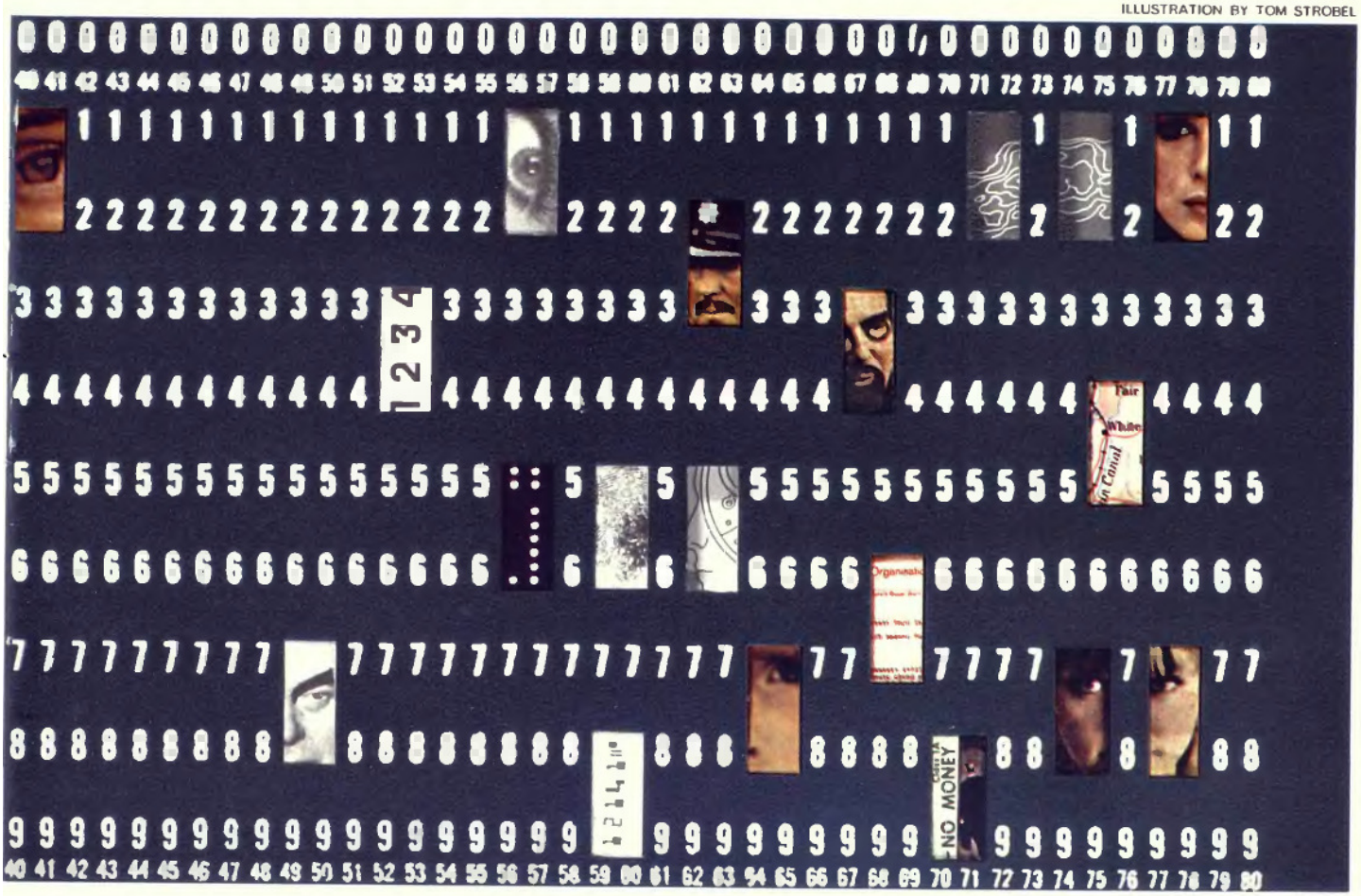
Roger's inputs are carried swiftly by data line to the Downtown National Bank, the central depository of Roger's financial account. Though he may have accounts in other banks throughout the country, these are all registered and monitored by the bank in Smith's place of residence or work. When the thumbprint and voiceprint recorded at the tollgate are compared with the bank's master prints, establishing that it is really "Smith, Roger M., 2734-2124-4806," the bank's computer posts a 75-cent charge to his account and flashes a 75-cent credit to the bank holding the Turnpike Authority account.

Throughout his typical day, when he parks at the Triangle Garage, is registered in and out of the company office for payroll verification, has lunch at Jimmy's East, makes purchases at Macy's, goes to Central City Stadium for a ball game, places a bet on the daily double, buys plane tickets, settles his hotel bill or buys 500 shares of Electronic Computers Unlimited, Roger Smith will use no cash. Money has been eliminated, except for pocket-change transactions.

Of course, all of Roger's regular, continuing obligations are paid automatically from his account—his mortgage installments, insurance premiums, magazine subscriptions, organizational membership dues, etc. Those continuing

The Snooping Machine

ILLUSTRATION BY TOM STROBEL



accounts that fluctuate monthly are also verified and paid automatically—medical bills, psychiatrist's fees, gasoline charges, telephone bills, pay-TV account, book-club purchases, etc. All financial credits to Roger's account, each carefully identified as to the source and classified as to the basis for payment, go directly to the bank, not to Roger. Roger's various Federal, state and local tax obligations are determined by computer analysis and are automatically paid when due.

This is a superb system—efficient, practical and far cheaper than the money economy with which mankind fumbled along for so long. But one by-product of the cashless society is that every significant movement and transaction of Roger Smith's life has produced a permanent record in the computer memory system. As he spends, uses and travels, he leaves an intransmutable and centralized documentary trail behind him. To those with access to his financial account, Roger Smith's life is an open tape.

But the daily denuding of Roger Smith has only begun. For every person in the United States in 1975, there are four master files. His complete educational record, from preschool nursery to postgraduate evening course in motorboat economics, is in an educational dossier, including the results of all intelligence, aptitude and personality tests he's taken, ratings by instructors and peers and computer analyses of his projected educational capacities.

Roger's complete employment record contains entries for every job he has held, with rate of pay, supervisors' evaluations, psychometric test results, recommendations, outside interests, family milieu and a computer-analyzed, up-to-date job-security profile. All of this is available for instant print-out when an employer wants to consider Roger for a job or a promotion.

Roger's financial file is probably the largest. It contains a selected history of his financial transactions, from his earliest entry into the computerized economy to his latest expenditure for a new Carramba-35 sports car. His patterns of earnings, fixed expenditures, discretionary spending, computer-projected earning capacity and similar items are all kept ready, so that decisions involving loans, mortgages, insurance and other credit-line transactions for Roger Smith are made with full knowledge of his fiscal history.

Finally, there is Roger's national citizenship file. This is a unified Federal-state-local dossier that contains all of Roger's life history that is "of relevance" to Government. In 1975, that is quite a broad category. It includes his birth facts and permanent identification number, his educational file in full (after all, it was either public education or

article By ALAN WESTIN *if the government has its say, the budget department's giant computer will take the first step toward stripping away your last vestiges of privacy*

publicly assisted), his military service, all the information from his license applications, income-tax records and Social Security data and, if he now works or worked in the past as a Government employee, consultant or contractor, his public employment record and assorted security clearances. If Roger was ever arrested for a crime other than a minor traffic violation, a special public-offender intelligence file is opened on Roger Smith that includes a large base of information relating to his educational, employment, military, family and civic activity. Citizenship files also include a personal-health category, developed to aid public-health measures and to assist individuals caught in health crises away from their home physicians. This contains a complete medical dossier from birth condition and psychosexual development to reports of last week's immunization shot, cardiogram flutter or extended-depression check-up. Most important of all, these four master files on education, employment, finances and citizenship can be put together into one unified print-out whenever a Government agency with subpoena power chooses to do so.

For purposes of economic forecasting, demographic studies and behavioral prediction, the data base such a dossier society has created provides unequaled opportunities for research and policy analysis. For enforcement of public programs—educational reforms, integration rules, crime control, mental health—the national file system brings unparalleled advantages. But crucial elements of privacy in a free society, such as the partial anonymity of life, limited circulation of personal information and preservation of confidence in certain intimate relationships, are the bleeding casualties of a dossier society. For the Roger Smiths of 1975, life is by, on and for the record.

How does the record net work? For Roger Smith, who started work as an engineer at Consolidated Technics in the "old personnel system" days of 1965, the flash of understanding came when he was considered for the key promotion of his career, a possible move from engineering supervisor at Consolidated Technics to deputy vice-president for engineering at General Space, Incorporated. As Roger sat in the office of the information-system analyst (formerly personnel director) of General Space, he found himself staring at a print-out that had just been handed to him. It was titled "Inconsistent Items for Personal Explanation at Assessment Interview." As he scanned the list, he found these items:

1. *High School Personality Test Profile.* High score on the Fosdick Artistic and Literary Interest Inventory; technical career rated "doubtful."

2. *Criminal Record.* Disturbing-the-peace conviction, Daytona Beach, Florida, age 18. Speeding tickets, New Jersey Turnpike, 1973, 1974.

3. *Civic Activity.* Signed antidraft petition circulated by Colgate University chapter, Make Love Not War Society. Door registers showed attendance at campus lecture by George Lincoln Rockwell, age 20.

4. *Income Management Rating.* B—. Average annual personal loan held during past five years—$3000 to $5000. Balance in savings account on April 1, $217.41.

"If you have studied this long enough," the information-system analyst broke in, "let me briefly explain our procedure here to you. You are one of four men being considered for this position. We want you to take as much time as you need to write out an explanation of these items in your record. Your answers should be in terms of how these items might affect a possible career for you here at General Space, Incorporated. Keep in mind that we do seventy-five percent of our work for the Federal Space Voyage Program, and that involves classified information. The explanations you give us will become part of your general personnel files, of course, including the disposition we make of your employment review.

"Since this is the first time you seem to have applied for a job under the new computerized career-analysis system, let me reassure you that this is not an unusually large number of inconsistent items to be presented with. Your complete file runs close to two hundred and fifty pages, which is about the average length for a man of your age. However, I think it is only fair to tell you that two of the men being evaluated for the position have no inconsistencies to comment on as part of their personal interviews. After you have done this on several occasions, you will probably get used to it. . . ."

• • •

At this point, Rod Serling should appear on the television screen, grin his raffish grin and say, "Portrait of life in a fish bowl, somewhere in the Twilight Zone." We should all be able to smile appreciatively at his superb science-fiction imagination and then check the late movie on channel two. The trouble is that Roger Smith's dilemma is closer to reality than we think, both technologically and as a matter of social trends in America.

Consider first the question of technological feasibility. The average person knows that computers can collect and store vast amounts of data, search this with great swiftness, make comparisons and collations and engage in machine-to-machine exchanges of data, all at quite reasonable cost per bit of information. Despite this general awareness, there is still a common tendency to believe that "technological limitations" make it impossible to collect information for a dossier system of the detail described for Roger Smith.

Such a belief is simply nonsense. To illustrate this fact, we need only look at one data memory process recently developed by the Precision Instrument Company of Palo Alto, California. This system uses a one-watt, continuous-wave argon laser to burn minute "pits" in the opaque coating of plastic computer tape. The laser is so precise and can be focused so intensely that each pit is only one micron, or .000039 inch in size. Where normal recording has been about 5600 bits of information on an inch of magnetic tape, the new laser process can put *645,000,000* bits in microscopic parallel rows on each inch. And the recording process achieves speeds of 12,000,000 bits per second.

Once recorded, the information is permanently available for use. To read the data, a lower-powered laser beam examines the tape as it flies past at high velocity, translating the light that shines through the pits into an electrical pulse that is sent to a print-out machine or a computer for further use.

In terms of a dossier society, the laser memory system means that a single 4800-foot reel of one-inch tape could contain about 20 double-spaced typed pages of data on every person in the United States—man, woman and child. It would take only four minutes to retrieve a person's dossier under such a system. With 100 reels of tape, stored in a room no larger than 15 feet by 20 feet, 2000 pages of data could be maintained on every American. Allowing extra time to locate the particular reel on which a subject's file was stored, his entire 2000-page dossier could be retrieved in about ten minutes.

The cashless society lies equally within technological reach. Enough computers could easily be produced to handle the volume of transactions that would be generated by an automatic economy. Remote-point inquiries and inputs from small desktop units to a central computer are in common use today in airline- and hotel-reservation systems. New types of telephone instruments, such as the Bell Touch Tone card-dialing system, allow bills to be paid from the home and permit merchants to verify availability of funds before releasing products to purchasers. Vending machines have been developed that use optical scanners to accept credit cards. Though there are still some problems in achieving unique identification of each individual by single fingerprint or voiceprint, simultaneous use of these techniques could now prevent all but the most elaborately conceived frauds. Any losses of this kind would probably be far less than those currently sustained by check forgery and stolen credit cards. Technologically, then, we now have the capability of

(continued on page 152)

The Snooping Machine

(continued from page 132)

installing a computerized economic system.

Even though both the dossier network and the automated economy are technologically possible, this does not mean that American society has to use its capabilities in this way. Why shouldn't we dismiss this prospect as something that Government and private organizations would never think of adopting? The answer is that several basic social trends in American life have been moving us in precisely such a direction during the past two decades.

The first of these trends is the enormous expansion of information gathering and record keeping in our society. Partly, this stems from factors such as the increasing complexity of our industrial system, the expansion of regulatory, welfare and security functions by Government and the growth of large-scale bureaucracies in our corporations, universities, unions and churches. Partly, the growth in record collection stems from the breakdown of traditional, face-to-face techniques for personal evaluation of individuals by authorities. In an age of increased personal mobility, nationalization of culture and standardized mass education, when so many people within each socioeconomic group look, talk and think alike, "the file" becomes the Government's instrument for distinguishing among them.

Similarly, the turn of social science from rational or interest-seeking models of human motivation to heavily psychological and sociological explanations of human behavior means that masses of highly personal data must be collected to analyze events "scientifically" and make wise choices in public policy. Self-disclosure by individuals, then, becomes an obligation of good citizenship in the modern age, as well as an act of faith in "science."

Thus, when each American today reaches the gatekeepers of public and private authority, the official's basic response is to open a file on him, ask for extensive self-revelation, conduct independent investigations and share information with other certified file managers of our society. If anyone thinks this is an exaggerated portrait, just stop and think for one moment: How many Government forms and reports on yourself or your family did you fill out during the past year? How many questionnaires did you answer about yourself? How many progress reports on your activities did you file with financial, employment and organizational authorities? How many investigations of yourself do you think were conducted without your knowledge? How many investigators asked you about other people's lives? How many evaluations of others did you contribute to the permanent files? Did you ever refuse to answer questions about others or yourself? Do you know anyone who did?

This growth of investigations, dossiers and information sharing has been, of course, enormously accelerated by the advent of the computer. Now, private and public organizations can process 10, 50, 100 times as much personal information about their employees, clients or wards than was ever possible in the eras of print, paper and analysis by eyes and ears. The older barriers of too much cost, not enough time and too much error that once protected privacy of personal transactions have been overcome by the computer in just the same way the barriers of closed rooms or open spaces that once protected privacy of conversation have been swept away by new electronic eavesdropping devices.

The impact of the computer is not just economic, however. Its real force is on the mental processes of our society, in the way we think we should make decisions once we have machines that are capable of accepting, storing and processing so much information. When machines can store so much data, and so many questions that we once thought beyond our capacities to resolve can be answered factually and logically, our society comes to expect that decisions of business, government and science ought to be based on analysis of all the data. Anyone who advocates withholding the necessary data from the information systems in the name of fragile values such as privacy or liberty may be seen as blocking man's most promising opportunity in history—to know himself and to make more rational, more predictable decisions about human affairs.

These technological capabilities and social pressures became a tangible issue for the American public with current proposals to create a national data center. For years, computer-industry leaders, Government data collectors and social scientists had been exchanging wistful memos on the need to bring together the statistical data gathered and held separately by various public agencies. Though this was felt to have great value for statistical research, it was generally believed that cost factors, technical problems and an "unready" public opinion made such a data center something for the future.

In 1965, a committee of the Social Science Research Council recommended that the Federal Bureau of the Budget create a national center for "socio-economic" data. The S. S. R. C. is one of the leading private sponsors of academic research, and the Budget Bureau is the President's chief coordinating instrument for Executive agencies. The report pointed out that bureaus within 21 major Federal agencies had accumulated more than 600 bodies of statistical data on 30,000 computer tapes and 100,000,000 punch cards, that there was a risk of destruction for some of this data and that what was kept was not being coordinated effectively for analytical use.

The Budget Bureau responded by hiring a management consultant named Edgar S. Dunn, Jr., to study the issue. Late in 1965, he reported that the data-center idea was excellent. Computer technology, he noted, now made possible statistical aids to public policy analysis that had never been possible before. At the same time, important new Federal responsibilities for urban renewal, health, antipoverty, education and civil rights programs made amalgamation of statistical data essential. Dunn observed that the nucleus of the center could be some 9000 tapes that had been identified as the most important of the Federal data pool. These would be drawn from housing and current population data held by the Census Bureau, consumer-expenditure surveys and industry-labor data from the Bureau of Labor Statistics, Social Security data and Internal Revenue Service records.

The Dunn report recommended that the Budget Bureau ask Congress for a small appropriation in 1967 to preserve the 9000 key tapes and to start design of the data center. The proposal seemed to be gaining momentum when the Budget Bureau named a task force in December 1965 to make over-all recommendations for more effective utilization of Federal data. This committee, chaired by Professor Carl Kaysen, an economist who had served with the Kennedy Administration and is now chairman of the Institute for Advanced Study at Princeton, was expected to give the data-center proposal warm endorsement. About the same time, the press reported that another Federal Executive commission had urged the creation of a computerized national employment service; this would contain personnel files on persons seeking employment and would be used to match prospective employees with new job openings. Yet another Federal study group reported in 1965 that a national citizens' medical data bank would be desirable and would probably be established "in the next decade."

To those familiar with the Washington political process, it looked as though the full Executive "softening-up process" was at work. Prestigious private groups had called on the Executive branch to move forward with a badly needed program. Executive task forces had affirmed the necessity and feasibility of the proposal. If no Congressional authorization had been needed to go ahead with this "technical program" and if existing funds could have been used for the early design

studies, the national data center might well have been launched.

But 1966 was a year too full of public alarms over Big Brother technology for this proposal to slide by unnoticed. In early 1966, two Congressional subcommittees that had specialized in probing invasions of privacy by Executive agencies—one under Congressman Cornelius Gallagher of New Jersey and the other chaired by Senator Edward V. Long of Missouri (see *Big Brother in America*, PLAYBOY, January 1967)—began studying the proposed data center, and with serious initial reservations. While they were doing so, the Washington press corps learned of the idea: a series of sharp attacks on the Dunn report appeared in leading national magazines and newspapers during May and June 1966. The liberal *Washington Post* headlined its story, "CENTER FOR DATA ON EVERYBODY RECOMMENDED." "Apparently no secrets would be kept from the data center," the *Post* concluded. The conservative *U. S. News & World Report* was even more alarmed. In "A GOVERNMENT WATCH ON 200,000,000 AMERICANS," *U. S. News* warned its readers: "Your life story may be on file with the Government before long, subject to official scrutiny at the push of a button." In addition, several articles were written about the millions of investigative files, or dossiers, that were being collected regularly on American citizens by Government agencies and private credit bureaus. The public began to realize just how much personal information was going into public and private information files.

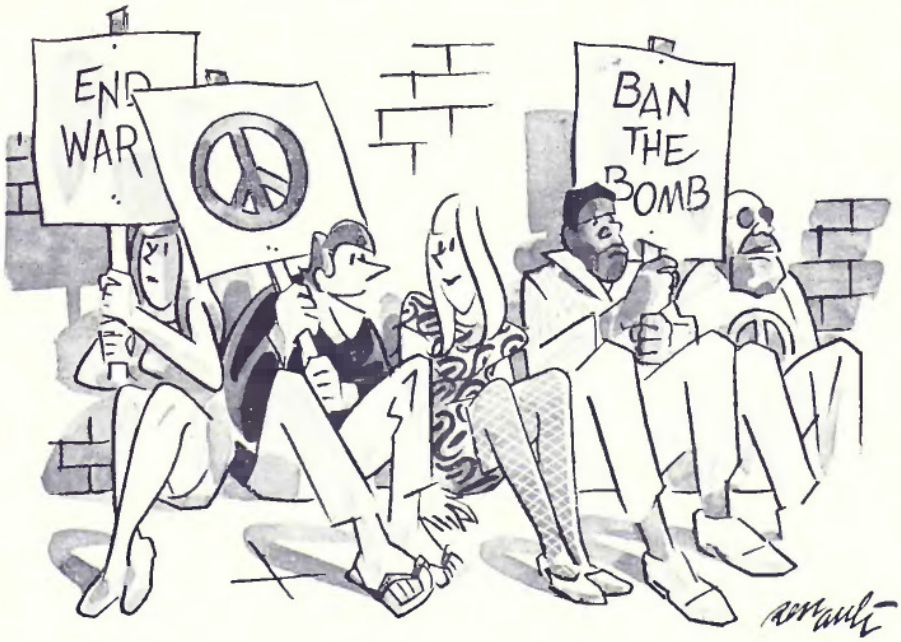
Though Senator Long held a two-day hearing that explored the Dunn report, the full-dress confrontation on the national data center came in July 1966, when the Gallagher subcommittee called Executive agency officials in to testify. The principal witnesses were Edgar Dunn and Raymond T. Bowman, Assistant Director for Statistical Standards of the Budget Bureau. Both explained that the data center was only a tentative idea in development stage, not a finished "decision." They also acknowledged that the S. S. R. C. report and the Dunn report had not been "careful enough in their wording" and had been faulty in failing to discuss in detail the problem of safeguarding privacy. As their testimony proceeded, they stressed that only statistical socioeconomic data would go into the center, not "personal" matters such as educational or court records, psychological test results, etc., and that the data would be used solely for statistical analysis. Information about named individuals would not be used for regulatory or law-enforcement purposes; this was to be a statistical and not an intelligence system.

As for the need to create such a data center, the Executive spokesmen noted that hundreds of millions of dollars of Federal money were being spent for socioeconomic programs about which the Administration, Congress and the public had inadequate or, sometimes, no significant data on which to plan or judge policy alternatives. Finally, the witnesses explained that everyone associated with the data-center idea had simply assumed that statutory provisions would be enacted to limit the uses of the data to statistical purposes and forbid all regulatory or prosecutive use and that administrative rules would have been set to enforce anti-disclosure and confidentiality laws. The model they had taken for granted was the Census Bureau, which has a tight statute, strict rules and no known instances of misuse of its data since it began operations at the start of the American republic.

However persuasive this Executive case for the data center might seem when summarized here, it was completely shot down in flames at the Gallagher hearings. The first missiles came from several computer specialists, particularly Paul Baran of the RAND Corporation. These witnesses informed the Congressmen that, as long as the identities of individuals were kept attached to the data put into the center, there was always the possibility that those managing the center or those obtaining access to it could convert it into an intelligence system and obtain a comprehensive print-out of all the information about a target individual. They also showed how much personal and potentially damaging information about individuals and businesses could be extracted by trained intelligence personnel from the kinds of data that would be going into the proposed center.

When pressed by Congressman Gallagher about these problems, the Executive officials admitted that they could not separate identities from data. The center had to have the name, the Social Security number or some personal identification system permanently linked to the data so that the income-tax files of Roger Smith could be linked to his Social Security and Census files and so that the progress of identified individuals could be traced through time. Thus, even though the identities would not appear on any of the statistics drawn, the very nature of the system made it impossible to prevent intelligence files from being obtained on particular individuals. Though several computer specialists indicated that elaborate safeguards against outside intrusion and many types of inside misuse had been developed for national-security computer systems, none of these technological safeguards had been considered as yet by the data-center proponents. In fact, they displayed considerable ignorance about design and machine techniques for assuring privacy.

The other attack on the data center came from legal and civil-liberty experts testifying before the subcommittee. Congressman Gallagher and his colleagues drew from the Executive witnesses damning admissions that they had not thought through the constitutional and legal protections that ought to be attached to personal information given to the Government for one purpose and then compiled into a centralized data pool for other uses. The legal specialists showed that the system could have enormous potential effects on the citizen's privacy and could lead to a major increase of power in the hands of Federal



"After the sit-in, how about a lie-in at my place?"

officials who might use the data for intelligence purposes. Given these possibilities, Congressman Gallagher argued that thorough analysis of the full range of problems was called for in advance of any decision to start a center. Yet the Gallagher subcommittee established that no committee or advisory group had been called in to consider the technological, psychological, constitutional and political implications of the data center, despite the availability of experts on all of these matters.

The Gallagher hearings ended with a promise by the Budget Bureau spokesmen that no start on the data center would be made without seeking approval from Congress. Publications as diverse as the *Nation*, *The Wall Street Journal*, *The New York Times* and the *NAM* (National Association of Manufacturers) *Reports* applauded the Gallagher subcommittee for its work in halting the "computerized garbage pail" and "biggest Big Brother." Several publications, noting the weakness of the Executive presentations, predicted that the proposal was probably dead.

This was one of the most premature obituaries in history. In October 1966, the Kaysen committee issued its report recommending establishment of the data center. Having been warned by the Congressional hearings and press attacks, the men who wrote the report included an appendix discussing means that should and would be taken to guarantee privacy. While far more informed and thoughtful than the Dunn report or the Bowman testimony on this issue, the Kaysen discussion of privacy still left the issues of design safeguards and legal standards disturbingly vague. Congressman Gallagher published an angry letter he had written to the director of the Budget Bureau expressing dissatisfaction with the Kaysen report and insisting that a clearer showing of the need for one central facility, a concrete description of what was going into it and advance planning by computer specialists and constitutional experts were all prerequisites for any further action.

In March 1967, Senator Long's subcommittee held further hearings on the data center, questioning Kaysen and Executive-agency proponents and hearing civil-liberties objections from a law professor and the Washington director of the American Civil Liberties Union. Throughout the rest of 1967, the data center was debated at national meetings of groups from the American Bar Association to the Joint Computer Conference, and dozens of newspaper articles and magazine pieces explored its implications.

In January 1968, the Long subcommittee held hearings at which it published a comprehensive survey of the information about individuals that is presently collected by each Federal agency. The survey found that many Federal agencies were collecting more personal

and intrusive information than even the most charitable concept of their legitimate needs or missions could justify. Furthermore, the Long-subcommittee survey found that a substantial segment of these records was not presently protected by legal guarantees of confidentiality against disclosure. The Long hearings also went into the rapid growth of other kinds of computer data centers—credit-bureau computer systems, employment data banks, law-enforcement systems and a host of other burgeoning data pools, some private and totally unregulated, some governmental with careful privacy safeguards and others lacking such measures.

As of this writing, there is no national data center. There has been talk by Budget Bureau officials of attempting a small (two-percent) sample of the various data that would go into the full center, in order to design the system, see how it might operate and demonstrate it for Congressional review. There has also been talk of creating an advisory panel of constitutional lawyers, Executive officials, Congressmen, social scientists and computer specialists to help the Budget Bureau devise the package of necessary safeguards—a thorough statute, administrative regulations and audit-review procedures. Some original advocates of the center now talk of concentrating on the design of a limited data pool to provide statistical analyses in a few of the most pressing areas of national socioeconomic policy, such as poverty programs or Medicare, and build slowly outward from there.

Whether any of these plans go forward is now a White House decision. The costs of starting another furor in Congress may not have high appeal in an election year, and many Washington observers expect the national data center problem to be deferred until after 1968.

Ironically, much more attention was given by Congress and the press to possible misuse of this statistical system than to the quiet initiation by the FBI of its National Crime Information Center in 1967. This uses a central computer to collect and distribute national, state and local information on stolen cars, stolen property and certain wanted persons. While the system is presently narrow in scope, the plans are to expand it in the future to collect much more intelligence information. Which names will go into files and what information about them will be collected remains to be seen. What safeguards will control the FBI operation has not been aired in the press or questioned in Congress. The Congressional committees that went after Budget Bureau and Census Bureau officials with sharp inquiries have shown no desire to put questions to J. Edgar Hoover.

Looking at the national data center debates of 1966–1967, we can see three distinctly different approaches to the problem of new computer technology and privacy. The first position, reflected in the initial thinking of most of the Executive-agency officials, computer manufacturers and behavioral scientists, assumed that a modest adaptation of traditional administrative and legal safeguards, plus the expected self-restraint of officials who would manage any statistical system, would be enough to protect the citizen's privacy. The more reflective spokesmen in this group would add that our society is requiring greater visibility of certain individual and group activities, in order to carry out rationally important socioeconomic programs that have the deep support of the American public. Since privacy has never been an absolute value, they reason, we should accept certain minimal risks to privacy as part of the balancing of values in a free society.

The second position, reflected by the initial views of most newspaper editorials, civil-liberties groups and Congressional spokesmen, is to oppose creation of a data center completely. The need of Government officials and behavioral scientists to have better statistics for policy analysis is seen as simply inadequate when weighed against the increase in Federal power that such a system might bring and the fears of depersonalization and loss of privacy that it could generate among citizens. The only situation that would satisfy these critics would be a "tamper-proof" system in which all identities were removed from the data.

The third position is the one that seems most persuasive and that may be the ground on which the two initial positions will meet, now that the privacy considerations have been thoroughly aired. This sees the added threats to privacy from centralized data systems as requiring a new legal and technical approach to sensitive-information management by Government. While this approach would be applied differently, according to the type of data center involved—statistical, social-service or law-enforcement—it is the statistical center that concerns us here.

At the outset, we must recognize that the individual's right to limit the circulation of personal information about himself is a vital part of his right to privacy that should not be infringed upon without showing strong social need and satisfying requirements as to protective safeguards. When Government takes information from an individual for one purpose, such as income taxation, census enumeration or Social Security records, and uses it to influence, regulate or prosecute the individual on unrelated matters, this strikes a blow at the individual's autonomy and violates the confidence under which the information was originally given.

Following this view, a statistical data center must have both "machine system" safeguards to limit the opportunities for misuse, and legal controls to cover those human abuses that cannot be averted by technology itself. At the system level, we should realize that storing data in computers allows us—if we want to—to create far more protection for sensitive information than is possible when written files are available for physical inspection. Information bits in the memory banks can be locked so that only one or several persons with special passwords can get them out. Computers can be programed to reject requests for statistical data about groups that are really designed to get data on specific individuals or business firms. (For example: "All the records on elected Federal officials from New York State who are under 45 and served in the President's Cabinet in the past ten years.") Furthermore, a data system can be set up so that a permanent record is made of all inquiries. Such an "audit trail" can be reviewed annually by the management of the center, Congressional committees and an independent "watchdog" commission of public officials and private citizens set up for that purpose.

Though many additional ways of guarding a data center from outside intrusion or inside misuse could be outlined, one clear fact remains. The system can still be beaten by those in charge of it, from the programmers who run it and the mechanics who repair breakdowns to those who are in charge of the enterprise and know all the passwords. This means that a package of legal controls is absolutely essential. For example, a Federal statute could specify that the data was to be used solely for statistical purposes; could forbid all other uses to influence, regulate or prosecute, making such use a crime and excluding all such data from use as evidence in courts; and could forbid all persons other than data-center employees from access to the data-center files. The data could be specifically exempted from subpoena. An inspector general or Ombudsman type of official could be set up to hear individual complaints of alleged misuse, and judicial review of the decisions in such cases could be provided.

What this all boils down to is the fact that American society wants both statistical data *and* privacy. Ever since the Constitution was written, our efforts to secure both order and liberty have been successful when we have found ways to grant authority to Government but to control it with the standards, operating procedures and review mechanisms that protect individual rights. Such a balance of powers is possible with a data center, if both the fears of the critics and the enthusiasm of technical proponents can be turned to constructive measures. For the Roger Smiths, 1975 demands effective Government as well as freedom from a data-file Big Brother. A free society should not have to choose between these values if we apply our talents for democratic government.