Law Quadrangle (formerly Law Quad Notes)

Volume 11 | Number 2 Article 6

Spring 1967

The Computer and Individual Privacy

Arthur R. Miller
University of Michigan Law School

The Computer and Individual Privacy

Excerpts from testimony before U.S. Senate Subcommittee on Administrative Practice and Procedure, March 14, 1967

by
Professor Arthur R. Miller
University of Michigan Law School

The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer. The same electronic sensors that can warn us of an impending heart attack can be used to locate us, track our movements, and measure our emotions and thoughts. The identification number given us at birth might become a leash around our necks and make us the object of constant governmental surveillance. Even the idea that there is no place in the world where we cannot be reached through our number is somewhat frightening. Finally, a high degree of information centralization gives those who control the recordation and preservation of data a degree of power, which, if abused, might make the alleged "credibility gap" of today look like a bridge table bidding misunderstanding. . . .

This investigation is most timely in view of the clarion in some quarters of the federal government for increased computerization of information and the establishment of a National Data Center. I am concerned, however, that the focus of the discussion and inquiry to date has been too narrow. In light of the enormous societal implications of the new technology, both for good and evil, the privacy issue should be examined in terms of the possible misuse of a communications medium that ultimately will be of national, and later international, dimensions, and not simply from the perspective of the possible abuse of a particular machine or group of machines operating in a building in Washington, D.C. Cognizance also must be taken of the fact that this new medium will consist of numerous subsystems, all having a capacity to injure our citizens and invade their privacy. Yet, almost all of these subsystems will operate under the aegis of state and local governments or private organizations rather than the federal government. The analogies between the need for comprehensive national regulation of computer communications, whether of a federal or nonfederal origin, and the need for national regulation of the airlines, railroads, radio, and television seem obvious.

To date, the proposals for a National Data Center have been modest and have suggested little more than the creation of a *statistical* center to enable federal agencies to compile and process facts and figures from governmental files and records on an aggregate basis; suggestions that an individualized *intelligence* center is in the offing have been disabused. Since the development of a comprehensive computer dossier on an individual basis is both technologically possible and may prove to be logical and economic, it would be unwise for this Subcommittee to evaluate the proposed Center's potential impact on human privacy in terms of the current suggestions or on the assumption that the Center will be a static institution. In the fullness of time, even the most innocuous of centers could become the heart of an individualized, computer-based federal record-keeping system.

Moreover, this Subcommittee should not deliberate in terms of computer capability as it exists today. The world of information transfer and data storage and retrieval is evolving at such a rapid rate that assertions that maintaining a computer file on every American is impractical, unfeasible, or uneconomic may soon be proven erroneous. New generations of computer hardware are constantly being spawned, machine storage capacity and speed is increasing geometrically, and costs are declining. Thus, at this time we cannot perceive the dimensions, the sophistication, or the intrusive abilities of the National Data Center ten or twenty years from now. Nor can we prognosticate the caliber of the techniques that may be developed to break the safeguards shrouding the Data Center or to manipulate, falsify, or extract information stored therein. . . .

". . . risks to privacy created by a National Data Center lie not only in the misuse of the system by those who desire to injure . . . but in the proliferation of people having capacity to inflict damage through negligence, sloppiness . . . and sheer stupidity . . ."

Inasmuch as the problem of privacy permeates such basic questions as who should control the operations and policies of the Center, what information should it record, who should have access to it, what protective systems should be built into the Center's hardware and software, and what types of transmission media should be used, the privacy and technical implications of these queries must be dealt with before the Center is built.

Privacy has been relatively easy to protect in the past for a number of reasons: 1) large quantities of information about individuals have not been available; 2) the available information generally has been decentralized and has remained uncollected and uncollated; 3) the available information has been relatively superficial; 4) access to the available information has been difficult to

secure; 5) people in a highly mobile society are difficult to keep track of; and 6) most people are unable to interpret and infer revealing information from the available information. The testimony elicited by this Subcommittee in its earlier hearings on privacy and a recent book authored by its distinguished chairman present an astounding, and disheartening, panorama of the ways in which the intruders in our society, aided by modern science, have destroyed our traditional bastions of privacy. Revelations concerning the widespread use of the spike microphone, a variety of gadgets for electronic eavesdropping, and cameras equipped with modern optical devices have shocked us and demonstrated that we do not necessarily enjoy privacy in our homes or offices, on the street, or while sipping martinis. . . .

We can assume that one consequence of a Data Center is that many federal agencies will go beyond current levels of inquiry and begin to ask more complex and probing questions, perhaps into such subjects as memberships in organizations, association with other people, location at different points of time and space, medical history, and attitudes toward various institutions and persons. This simple magnification of recorded information is certain to increase the risks of: 1) errors in reporting, recordation, and indexing; 2) information distortion caused by machine malfunctioning; 3) misuse of information by persons working with the data; 4) misuse by people who are at a distance from the data but who have access to it through remote terminals; and 5) violation of an individual's understanding that information furnished a particular federal agency or official would not be disclosed to others.

There are additional risks lurking in the ever-increasing reliance on recorded information and third party evaluations of a person's past performance, rather than on personal observations of his work. As information cumulates, the contents of an individual's computerized dossier will appear more and more impressive and impart to the user a heightened sense of reliability, which, coupled with the myth of computer infallibility, will make it less likely that an independent evaluation or an attempt to verify the recorded data will be made. This will be true despite the "softness" or "imprecision" of much of the data in the computer file. Our success or failure in life ultimately may turn on what other people decide to put in our file and the programmer's ability, or inability, to evaluate, process, and interrelate information. The record of our endeavors will be a hearsay narrative prepared by a computernik, much the way our knowledge of the Trojan War and the travails of Ulysses has depended on Homers filtration and distillation of earlier chronicles.

These prospects are made even more depressing by the realization that the great bulk of the information likely to find its way into the Center's files will be gathered and processed by relatively unskilled and unimaginative people who will lack the discrimination and sensitivity necessary to warrant reliance on their judgment. Finally, a computerized file has a certain indelible quality—adversities cannot be overcome with time absent an electronic eraser and a compassionate soul willing to use it —and there are many who will utilize the record in an unthinking and heartless manner. Small wonder that people are concerned over the incessant recordation of information about them.

But there is more. The very existence of a National Data Center magnifies the risks to individual privacy by providing a fruitful and central source of information for federal officials and may even encourage their penchant for questionable surveillance tactics. For example, in the future optical scanners may be used for mail cover operations. Perhaps the information drawn in by the scanner will automatically be transferred into the investigation subject's file in the National Data Center. Then, with a press of the proverbial button, the files of all of the subject's correspondents will be produced, examined, and appropriate entries—"associates with known criminals," perhaps—made therein. These tactics, as well as the possibility of coupling wiretapping and computer processing, undoubtedly will be extremely attractive to over-zealous law-enforcement officers. Similarly, the ability to transfer quantities of information maintained in nonfederal files—*e.g.*, credit information, educational information from schools and universities, local and state tax information, and medical records—into the National Data Center will facilitate and encourage governmental snooping. . . .

In still another respect the risks created by the Center are not simply those of expanding access and increasing reliance on greater quantities of detailed personal data. The centralization and compilation of information from widely divergent quadrants of the government by unskilled or semi-skilled personnel create serious problems of accuracy of the information. At this juncture I am not simply speaking of the accuracy of what is input and recorded. Information can be entirely accurate and sufficient in one context and wholly incomplete and misleading in another. For example, the bare statement of an individual's marital status has entirely different connotations when examined by the selective service, a credit bureau, the internal revenue service, and the social security administration. Consider the different embellishment on an unexplicated computer entry of "divorced" that is necessary in each of those contexts to portray an accurate picture of an individual's personal situation.

". . . it has long been technically 'feasible,' and from some perspectives, 'desirable,' to require . . . passports when moving through the country or to require universal fingerprinting. But we have not done so . . ."

Understandably, there is considerable concern that information recorded in the Center will be used in ways that are irrelevant to the purpose for which it originally was gathered. The question of context is most graphically presented in terms of one of the most dangerous types of information—the unexplained and incomplete arrest record. Is it unlikely that a citizen whose file contains an entry "arrested, 6/1/42 convicted felony, 1/6/43; three years, Leavenworth" will be given federal employment or be accorded the governmental courtesies given other citizens. Yet our subject may simply have been a conscientious objector. . . .

The risks to privacy created by a National Data Center lie not only in the misuse of the system by those who desire to injure others or who can obtain some personal advantage by doing so. There is a legitimate fear of the over-centralization of individualized information and the proliferation of people having capacity to inflict damage through negligence, sloppiness, thoughtlessness, and sheer stupidity. These people are as capable of damaging others by unintentionally rendering a record inaccurate, or losing it, or disseminating its contents to unauthorized people as are people acting out of malice or for personal aggrandizement. It is unrealistic to expect subtle standards of care and basic principles to be understood or implemented by people in clerical positions. . . .

The only completely effective guardian of individual privacy is the imposition of *strict* controls over what can be input into the National Data Center. None of the procedural and technical safeguards described below is immune from abuse by governmental and private personnel or mechanical failure. To insure the preservation of our traditional and cherished freedom from governmental intrusion, Congress must establish reasonably precise standards regarding the information that the Center can record in the legislation authorizing the creation of the Center.

Certain types of information should not be recorded even if it is technically feasible to do so and some legitimate administrative objective would be served thereby. It has long been technincally "feasible" and, from some perspectives, "desirable" to require citizens to carry and display passports when moving through the country or to require universal fingerprinting. But we have not done so because these encroachments on our liberties are inconsistent with the philosophical fibre of our society. By the same token, absent an absolutely overpowering demonstration that the preservation of sensitive or highly personal information in a central, computer-based, federally operated, data bank is essential to some fundamental national policy, the scrivener's hand should be stayed and the data permitted to be lost to man's memory. Prohibitions against recordation are especially necessary in areas in which the testimony before this Subcommittee demonstrates a risk of abuse. Thus, for example, medical and psychiatric information (particularly the results of tests such as the Minnesota Multiphasic Personality test when administered by a government office) should not be permitted in the Center unless those who advocate its recordation can show that human life depends upon doing so. . . .

Given the extensive governmental efforts at electronic eavesdropping and related activities, attempts undoubtedly will be made to crack the security of any Data Center that maintains information on an individual basis. Thus, it would be folly to leave the Center in the hands of anyone who might fall prey to pressures exerted by other federal agencies or to place the Center in any agency whose personnel have been shown to engage in anti-privacy activities. Similarly, policy control over the Center must be kept away from governmental officials who are likely to become so entranced with operating sophisticated machinery and manipulating large masses of data that they will be insufficiently sensitive to the question of privacy.

To me the conclusion is inescapable; control over the proposed Center must be lodged outside the existing administrative channels. As repugnant as it may sound in an era of expanding governmental involvements, it is necessary to establish a completely independent agency, bureau, or office that can establish policy under legislative guidelines directing the Center to insure the privacy of all citizens. . . .