The Revolution in Law Enforcement Technology Has Produced... Post 2/27/72

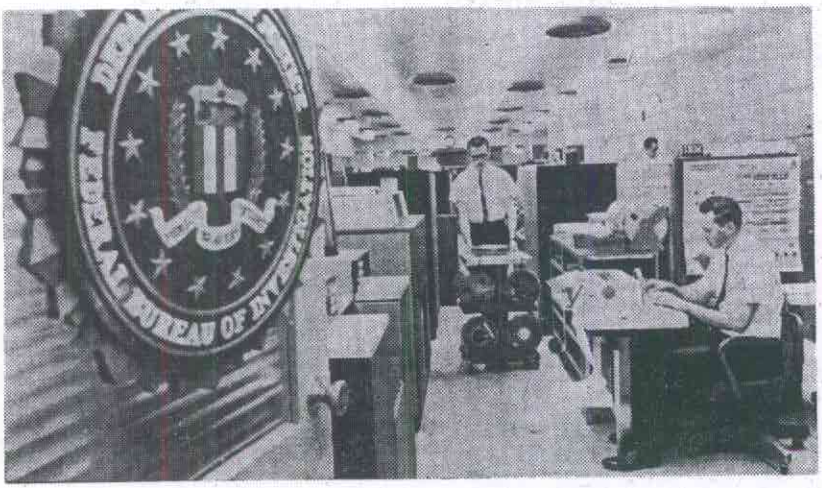
An Information Monster That Threatens Our Privacy

By Roger Wilkins

A silent creeping—one might even say creepy—revolution is taking place in the technology of law enforcement data collection and dissemination. The computers have entered the field and their potential for severely denting—if not destroying—the individual's right to privacy is growing by leaps and bounds.

Last year in a privacy case in the U.S. District Court in the District of Columbia, Judge Gerhard Gesell wrote:

"A heavy burden is placed on all branches of government to maintain a proper equilibrium between the acquisition of information and the necessity to safeguard privacy. Systematic recordation and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom to speak; to work, and to move about in this land. If information available to government is misused to publicize past incidents in the lives of its citizens the pressures for conformity will be irresistible. Initiative and individuality can be suffocated and a resultng dullness of mind and conduct will become the norm."



"Late in the 1960s, the first tendrils of what is fast becoming a patchwork—but nonetheless enveloping—information giant were beginning to emerge in the form of the FBI's National Crime Information Center system" (above).

Judge Gesell went on to decide that while the arrest record of a person who had been convicted of no crime could be maintained for federal employment and "strictly law enforcement purposes," the FBI is "without authority to disseminate arrest records outside the federal government for employment, licensing or related purposes."

Unfortunately, this lucid principle is being eroded by a voracious computer industry, two powerful and competing federal bureaucracies, hardware-loving police departments around the country and by a Congress which seems not to have the sensitivity, the will or the capacity to do anything to arrest or reverse the trend.

LATE IN the 60s, the first tendrils of what is fast becoming a patchwork — but nonetheless enveloping — information giant were beginning to emerge in the form of the FBI's National Crime Information Center system (NCIC). That system was designed to provide simple computerized information to law enforcement people on wanted persons, and identifiable stolen property such as license plates, securities, boats and guns. At the same time, from 1966 through 1968, the Justice Department's Office of Law Enforcement Assistance was providing various police jurisdictions about one million dollars a year to develop electronic data retrieval systems.

Then came the deluge. Since 1968, the Law Enforcement Assistance Administration, the much better funded successor to OLEA, has dispensed more than $46 million for a variety of such projects all over the nation. Some went to states for development of a greater organized crime intelligence collection capacity. Other states began using LEAA funds to develop systems related to civil disorders. Whereas earlier efforts had been fairly clearly directed toward information useful in crime detection and prevention, the guidelines began to become murky in the civil disorders field. One state, for example, indicated in its grant application that it would collect the names and information about people who "actively pursue their constitutional rights."

The most significant of the LEAA funded projects, however, was Project Search, which began as a cooperative effort among six states to standardize and computerize personal criminal history records and tie them into a central index and switching center in order to provide each participating state with quick and easy access to the relevant records of each of the others. By the summer of 1971, the number of states in the project had grown to 20 and the problems had grown proportionately.

THE FIRST strains emerged when Project Search's Committee on Security and Privacy

Center System. LEAA and the states balked. They argued that the original concept of Search was a bulky central index of criminal activity—like a telephone book—with the basic records being retained in the states rather than the creation of a federally controlled national criminal information and intelligence data bank.

As the dispute raged, Search oozed beyond its original confines into areas never envisaged by the original concept. Under the

"Any state or locality may, on its own initiative, store additional information in a system that later may be 'interfaced,' to use a term of the trade, with the federal data bank." Above, the records room at District police headquarters.

issued a study which attempted to formulate procedural guidelines safeguarding the public. Among the committee's recommendations were limitations on the type of data to be collected, periodic re-evaluation of the data in order to ensure accuracy, the development of procedures for an individual to have access to his file and stringent security precautions to prevent unauthorized individuals from obtaining access to the stored information. The head of the FBI's NCIC system argued that if such guidelines were needed at all, Project Search was the wrong organization to develop them and that in any event, it was too early to conduct such studies.

Shortly thereafter, it became clear that the FBI hoped that Search would be controlled, not by the states, but by the FBI and that its electronic systems would be tied to the Bureau's National Crime Information

rules developed by LEAA, such charges as juvenile and public order offenses, drunkenness and vagrancy would be excluded, but serious crimes would be recorded. Those might include bigamy, cruelty to animals, failure to provide support to one's family and adultery as well as the traditionally serious crimes of murder, assault, burglary and robbery.

Meanwhile, the FBI won its fierce bureaucratic battle within the Department of Justice with LEAA. On Dec. 10, 1970, the Attorney General transferred Search to the FBI. A year later, the Senate included in the FBI's appropriations bill language which appeared to restore to the FBI authority to share its information with certain classes of banks and also, in appropriate circumstances, with state agencies for employment and licensing purposes. In all the flurry and growth, the model codes for protection of citizens' privacy and the code of ethics drawn up by Project Search's Committee on Security and Privacy got buried.

At this point the situation remains cloudy, but ominous. LEAA still makes the grants for the acquisition of computers and is pressing for expansion of the system. The FBI is tightening its control while also

be placed on the machines' almost unlimited capacity to pry, to store and to regurgitate indiscriminately, mindlessly and on command.

Right now only the Lawyer's Committee for Civil Rights under Law, aided by the National Urban Coalition, is monitoring the growth of the beast and, laudable as that effort may be, it is not enough.

The Washington Post

EUGENE MEYER, 1875-1959
PHILIP L. GRAHAM, 1915-1963

KATHARINE GRAHAM
Publisher

JOHN S. PRESCOTT, JR.
President

BENJAMIN C. BRADLEE
Executive Editor

Philip L. Geyelin, Editorial Page Editor; Howard Simons, Managing Editor; Gerald W. Siegel, Vice President and Counsel; Robert P. Thome Treasurer; Joseph P. Lynch, Vice President-Advertising; Jack F. Patterson, Circulation Director; Julian J. Eberle, Production Operations Director.

Published by The Washington Post Company:
FREDERICK S. BEEBE
Chairman of the Board
KATHARINE GRAHAM
President
JOHN W. SWEETERMAN
Vice Chairman of the Board

pressing for ever greater membership. The states, having warned the Attorney General prior to the transfer of Project Search to the FBI that "no matter what the Feds do, the states will continue to develop their own system or systems," are presumably doing just that. And any state or locality may, on its own initiative, store additional information in a system that later may be "interfaced," to use a term of the trade, with the federal data bank. For example, the Kansas City, Mo., police department has stored, among other things, information on outstanding parking tickets, college students known to have participated in disturbances and "area dignitaries."

WHILE THIS information-gathering monster grows and spreads, there is really no effective federal or state regulation of the whole system. Senator Ervin's Constitutional Rights Subcommittee heard some testimony on the subject both from administration proponents and from concerned and frightened citizens. Senator Mathias slipped an amendment into Title I of the Omnibus Crime and Safe Streets Act requiring LEAA to develop legislation regulating the activity. In response in September, 1971, Senator Hruska introduced the Criminal Justice Information Systems Security and Privacy Act of 1971. To date, no hearings have been held on the Hruska bill.

Without debating the details of the Hruska bill, it is fair to say that it assumes that computerized dossiers collected by state and federal police organizations are part of our national life, that they are useful and that they are here to stay. And that is just the point. We apparently are off on another technological toot that leads God knows where without giving it a second thought. Nobody knew when Henry Ford rolled out his first Model A that the internal combustion engine would someday foul our cities. But now we ought to be sophisticated enough to know that a ride on the tiger's back is sure to cost at least a healthy nip on the nose, if not a great deal more.

The issues raised require urgent analysis and broad national debate before the information monster entirely devours our privacy. Because of the complex interstate nature of the system and the federal government's deep involvement in its development, there is only one place where the debate can appropriately take place—in the Congress of the United States. And the first question that needs to be taken up is whether the public wants or needs this system. If Congress' answer is yes, then there is a pressing need for it to define a citizen's right of privacy and the limits which must