Federal Monitors—Or Keyhole Kops?

ARTHUR R. MILLER

ANN ARBOR, Mich. — "Much ado about nothing." With that Shakespearean allusion a Federal judge recently dismissed a lawsuit to halt Army spying on the lawful conduct of citizens. Characterizing military intelligence as an "assemblage of Keystone Kops," the judge was unimpressed by the alleged ill effects of surveillance. Taken alone, the Army's activity may be insignificant, especially since the public *mea culpas* by former agents have helped abort its expansion. But military spying is symptomatic of growing governmental intrusion on our lives and heightened threats to constitutionally guaranteed rights.

To most of us, Orwell's 1984 is exaggerated science fiction. Yet revelations before Congressional subcommittees have sketched a disheartening panorama of how many traditional bastions of physical and informational privacy are being destroyed. Today Americans are scrutinized, watched, counted and interrogated more than at any time in history. A dossier is opened whenever we file a tax return, apply for life insurance or credit, seek government benefits or interview for a job. And when we fly, reserve a hotel room or rent a car, we often leave electronic tracks in a computer's memory—tracks that may later betray our activities, habits and associations.

Americans are generally unaware of the extent to which Federal agencies are using computers and microfilm to collect, store and exchange personal information. People erroneously assume that the Government only monitors society's "crazies." Yet in recent months the existence of H.U.D.'s adverse information file, N.S.F.'s data bank on scientists, the Customs Bureau's computerized bank on "suspects," the Civil Service Commission's "investigative" and "security" files, the Secret Service's dossiers on "undesirables"—as well as the Army's surveillance of elected officials, clergymen, the N.A.A.C.P., the A.C.L.U. and the Women Strike for Peace—has come to light.

Unless the security and integrity of data banks are assured, their dangers may outweigh their benefits. This is particularly true in the law-enforcement field, where arrest records are beginning to be computerized despite their notoriously misleading character (many arrests never lead to prosecution, even fewer to convictions, and many occur during *lawful* demonstrations).

If this data is added to the F.B.I.'s National Crime Information Center, it will be available to thousands of local police stations through remote access terminals. No one disputes the legitimacy or importance of police agencies sharing arrest records. But absent effective controls, what will prevent moonlighting officers from checking on prospective insurance or real estate customers or peddling these unreliable records for other inappropriate purposes?

Demands for governmental efficiency will produce even more comprehensive information networks. Federal funding already is supporting a sensitive but virtually unprotected Migrant Worker Children Data Bank and President Nixon's proposed welfare program will give H.E.W. authority to exchange individualized data with state agencies. Given the polarity of today's student activism and public reactivism, Federal surveillance systems and educational data centers ultimately may be linked, under the long-range implications of the President's request for funds to infiltrate university campuses with 1,000 new F.B.I. agents.

Building dossiers or spying on people engaging in lawful social and political activities often has little relevance to legitimate governmental functions and typically ignores its "chilling" effect. Citizens who fear they are on file may develop a "record prison" psychosis and become willing to "stick their necks out" to pursue constitutional rights of speech, assembly and petitioning the Government. If so, today's surveillance efforts contain the seeds of a police state or a return to McCarthyism. Thus, claims of governmental efficiency or the quest for the holy grail of "law and order" must not be allowed to justify every demand for gathering personal data.

> *"Too often, in the Congress as well as in the nation, there is an unwillingness to protect the privacy of our fellow men when they are of different political persuasion, different economic status or different mode of life. Until Americans learn to distinguish tyranny in any form, until each of us has the courage to protect the other man's privacy, we shall not be truly free."*
>
> —SENATOR ERVIN

There are no effective restraints on the Government's data activities and no one has undertaken to guard against the abuse of our informational privacy. As a result, the citizen-Government balance is changing so drastically that revitalizing the judge-made right of privacy or expanding the First Amendment freedoms is an insufficient response to the challenge.

Direct Congressional intervention to safeguard these rights is indicated. Detailed Federal legislation at this time probably would be difficult to draft, politically unfeasible and potentially unsatisfactory. However, creation of a watchdog organization staffed by privacy experts exercising continuing supervision over governmental data activities should be explored.

The need for Federal action is clearly perceived by Senator Sam J. Ervin Jr., chairman of the Subcommittee on Constitutional Rights. He plans wide-ranging hearings on Federal information gathering starting Tuesday. Continued ventilation of this problem is essential to generate public awareness of the threat to our privacy and First Amendment freedoms. Otherwise we shall stumble from one surveillance exposé to another but never arouse our lawmakers to halt the steady erosion of our rights by bureaucrats and computerniks. A dictatorship of dossiers and data banks rather than of hobnailed boots is nonetheless a dictatorship.

Arthur R. Miller is a law professor at the University of Michigan and the author of "The Assault on Privacy: Computers, Data Banks and Dossiers."