Judy

STATEMENT BY

CLAY T. WHITEHEAD, DIRECTOR
OFFICE OF TELECOMMUNICATIONS POLICY

ON

FEDERAL INFORMATION SYSTEMS

before the

Subcommittee on Foreign Operations
and Government Information
Honorable William S. Moorhead, Chairman
Committee on Government Operations
U.S. House of Representatives

July 31, 1973

Mr. Chairman, I welcome the opportunity to present my views on the use of advanced information and communications technology to improve Federal information services, and to explain the responsibilities of my Office in that regard. I have with me today Mr. Charles Joyce, the Assistant Director for Government Communications in OTP.

The Office of Telecommunications Policy was established in 1970 to provide a focal point for the development of administration policy in the area of electronic communications, and to coordinate the activities of the various Federal Departments and Agencies in this area. The scope of my responsibilities includes electronic communications, and matters arising out of the joint use of computers and communications. I am not responsible for matters involving solely the use of computers, or for matters in the area of information which are totally apart from any use of electronic communications systems. But this latter point is not particularly limiting with respect to the subjects I will be discussing today since most of the issues of public concern in the area of information handling involve electronic communications in one way or another.

I will now try to cover briefly each of the areas listed in your letter, Mr. Chairman.

## OTP Role in Federal Information Systems

First, you asked about our role in providing technological services to other agencies, and in planning, operating and coordinating Federal information systems. OTP does not provide technological services to other agencies. Nor do we operate any telecommunications or information systems, except as may be needed for our own internal use.

We are responsible for providing policy guidance to Federal Agencies which do operate such systems, and for coordinating the efforts of these agencies in the interests of Government-wide effectiveness and economy. To accomplish this task in a systematic way, I have initiated a joint planning process in which Federal Agencies with similar operational missions and communications requirements will work together to optimize the communications operations in their respective areas. The five initial mission areas which have been identified for this type of planning are: National Security, Law Enforcement, Transportation, Environment, and General Administrative Communications. In each area, the agencies involved will be responsible for jointly reviewing their telecommunications plans to eliminate duplication and achieve maximum economy and effectiveness. OTP will review the resulting combined plans to assure overall consistency and adherence to national communications policy.

Sharing and Interconnection

Sharing and interconnection of systems are measures which are pursued within the Government with the objectives of achieving economy and maximizing the usefulness of communications and information systems. These are worthwhile objectives, although I am not convinced that they have been achieved in some of the present programs. In any event, interconnection and sharing are not ends in themselves, and they do entail risks of compromising privacy which must be recognized.

Safeguards

You asked for my views on safeguards needed to protect against misuses of Federal information systems, specifically the invasion of privacy and use for propaganda purposes. In responding to that, let me explain how these concerns present themselves in Government communications planning, and where responsibility lies for action.

While there is no single generally accepted definition of "privacy" or the "right to privacy," it is widely acknowledged that a reasonable freedom from intrusion is essential to normal human growth and stability. The individual should not have information thrust upon him. The "right to be let alone" implies a degree of protection from unwanted sights and sounds.

The claim to privacy in the information context is based on the dignity and integrity of the individual. These concepts are tied to the assumption that all information about a person is in a fundamental way his own, for him to determine when, how and to what extent it is communicated to others. People also recognize that much of society's business can be conducted only if confidentiality of communications is respected. By protecting this privacy, society ensures its own well-being and development.

Privacy as a fundamental value is essential to a democratic system, which has, as its highest goal, the liberty of the individual. Privacy, however, is not absolute. There is an inherent conflict, for example, between the Government's need for information to pursue justice and an individual's need for personal privacy.

Electronic technology has greatly increased the ability to acquire and disseminate information. Mechanisms to ensure individuals their privacy and the privacy of their communications have not advanced as rapidly. OTP has undertaken to investigate the adequacy of common law, statutes, and Federal regulations to protect individuals regarding the privacy of their electronic communications and the security of the systems carrying them. This is being done with the view towards identifying what policies, standards, or legislative safeguards are necessary.

Communications, computers and other information technologies lower the cost and increase the speed of large scale information collection and processing operations. These technologies can therefore expand the power of the Government and other large institutions vis-a-vis the individual. They *could*, for example, increase the ability of Government agencies to assemble confidential information about persons to the detriment of individual privacy. They also *could* increase to an undesirable degree the power of Government to influence large numbers of citizens with respect to Government policies, that is, to propagandize the public. But such results are not inevitable. They must be prevented, and they *can* be prevented if we are aware of the dangers and develop appropriate safeguards. What are those safeguards?

## Privacy

To safeguard privacy, it is essential to protect the confidentiality of data which, by law, is to be collected and used for limited purposes, such as census data, tax returns, social security data, and investigative files. The responsibility for protecting such files in most cases must lie with the agencies charged by law with collecting the data. Any breach of confidentiality must be laid squarely at that agency's door. Clear responsibility and procedures for correction are, as they have always been the best safeguards.

But this simple rule is not enough when Federal systems containing confidential data are to be interconnected, or when confidential files are to be used in shared information systems. Admittedly, there are potential benefits to interconnection and sharing in the form of greater overall economy and wider accessibility within the Government of useful information. However, such steps also contain risks or loss of effective control over confidential data. It is in resolving these conflicting considerations of Government economy and effectiveness and sound public policy that my responsibilities come into the picture.

I have been working with the Federal Agencies who have extensive telecommunications systems to clarify Federal policy on interconnection and sharing. We have not yet come to the point of issuing any all-encompassing policy document -- perhaps we never will. But we have come to an understanding that interconnection and sharing are not ends in themselves. OTP has been insisting on a clearer understanding of the magnitude of benefits and risks involved in interconnecting or combining Government systems.

Looking to the future, I expect that the planning process I referred to will provide more information, for all parties concerned, about plans for the future of Federal Government information systems. To provide guidance for this planning, we have initiated studies to determine more clearly the desirability of shared systems and the risks involved. We are closely following efforts to assess the current state of the art in technology for controlling access within information systems so that we will be well informed on the risks.

## Propaganda

The other area of concern is the possibility of abuses in the dissemination of information by the Federal Government. We must recognize that there are important needs for Federal agencies to provide certain types of information to the public. However, two types of abuses can occur: First, undue efforts to influence public opinion in favor of Federal policies, agencies or individuals, and second, extensive provision of routine information services by the Federal Government which could be provided adequately by the media or other private organizations. We are concerned here today primarily with the former possibility, an abuse which might be called propaganda. Again, the primary responsibility for controlling excessive propagandizing must be with each Federal Department and Agency.

An area which bears watching is the provision of public service announcements by Federal Agencies. Broadcasters are strongly encouraged by Federal regulators to carry public service announcements. Federal Agencies may use this opportunity to support the presentation of a wide variety of messages regarding their activities and programs. But we should be alert to possible abuse of this opportunity by Federal Agencies -- the number and type of such messages produced and distributed by the Government must not constitute an unwarranted intrusion into the public mind.

It is possible for the Government to increase its "information power" indirectly or even inadvertently, through projects designed for other purposes. Efforts to develop, demonstrate or utilize various types of information systems or technologies could possibly become new avenues for Federal propaganda, even though that is not the intended result.

One example of this concern is posed by the new warning system designed by the Defense Civil Preparedness Agency -

the Decision Information Distribution System, or "DIDS." The system, which is still being evaluated, was designed to serve a worthy purpose, namely, warning of impending attack or natural disaster. However, there is some basis for concern about how such a system, once in existence, might come to be used. In view of the possibility of misuse, however remote, I believed that it would be bad policy to force people to have a DIDS receiving device in their homes. We opposed the idea that legislation should be sought to force manufacturers to incorporate such a receiver in every new TV set. OTP established the policy that any purchase or use of home receivers for warning would be on a voluntary basis. Further, we are watching the project closely to assure that no additional functions are planned for the system which might lead to misuse or to competition with the news media or other private sources.

We have also been concerned for some time with Government sponsorship of broadcasting-type communications projects, including the development of broadcasting capabilities on NASA's ATS series of satellites. NASA is discontinuing such development projects, with OTP's concurrence, after the launch of the ATS-F next year.

Our concern is not directed only, or even primarily, toward high technology projects. Indeed, the use of very commonplace equipment can be a cause for concern. Through the simple expedient of an automatic telephone answering device, some Federal Agencies have made it very simple - perhaps too simple - for radio stations to record and retransmit announcements about Federal programs which were pre-recorded by Federal spokesmen. The technology involved here is trivial. The impact of such arrangements, however, and the potential for abuse, is great. It is important to be aware of this.

## Application of Technology to Information Activities

You asked my views about the development of systems to serve the needs of the public for information of all kinds, and about the agency or agencies which should plan and coordinate the use of technology for such activities. I do not believe that any one agency should be charged with developing information systems for the delivery of all kinds of information to the public. Such an arrangement would in all likelihood lead to the design of a massive delivery system which would then have to be filled with all kinds of data to justify it. This would bring the Federal Government into direct competition with numerous elements in the private sector such as publishers, research organizations, and computer service firms. Furthermore, the control which a central agency could exercise in selecting and editing the information to be contained in such a system would be an open invitation to use it to manipulate public opinion.

Any proposal for the use of a Government controlled, electronic communications system for this purpose should be carefully reviewed by higher levels within the Executive Branch and by Congress. Such a review should evaluate the dangers involved, and determine why there is no alternative way to get the job done. OTP has a responsibility to conduct such reviews, and we look at projects which come to our attention from this point of view.

## Communications for Social Needs

I am aware of the Committee's interest in the report entitled "Communications for Social Needs" which was produced by NASA in connection with certain other agencies in 1971. The report was prepared as one part of an effort to determine whether and how the research and development capabilities of the nation could be directed, through Federal policy and funding, toward meeting specific national needs.

We provided our views to NASA during the preparation of this report, but their report was not in accordance with those views. Among the deficiences I noted was too great an orientation toward Federally owned and controlled systems rather than toward private ownership and control, with the inherent dangers I have just described. I strongly opposed the adoption of this report, and it was never presented to the Domestic Council or the President. Thus, the report never received any Administration approval.

This does not mean that all of the ideas contained in the report were bad. The Post Office has been studying electronic mail handling for some time. The warning satellite idea had been considered by our own warning study group, but rejected in favor of the DIDS system.

Such ideas must be considered openly and each evaluated on its own merits. For example, although the "Wired City" proposal as presented in the report was ill-conceived, there is a need for sensible evaluation of the feasibility of providing public services over broadband cable communications systems. Though there is much talk about the potential for the delivery of educational and social services over cable systems, cable today is devoted almost exclusively to entertainment. Cable's full potential for public service is not likely to be developed by private industry, and I think that some Federal program in this area is appropriate, with adequate safeguards against the dangers I have described.

In summary, Mr. Chairman, I believe that the potential value of information technology for Government, for society, or for the individual is very high. Much of that potential can best be realized by the private sector in the marketplace. Valid Government functions can also be improved. There are dangers of a subtle but pervasive expansion of Federal influences and activity through the use of these technologies, but such adverse results are not inevitable. They can be overcome, if we set ourselves to the task, by adequate law and policy to assure that only the desired functions are performed. Our responsibility for communications policy, and our location in the Executive Office with a broad overview of Federal activities, gives OTP important responsibilities in the area of protection of the rights and freedoms with which your committee is concerned.

This concludes my prepared statement, Mr. Chairman, and Mr. Joyce and I will try to answer any questions which you and the other members of your Committee and staff may wish to ask.