APPENDIX 9

Statement by Dr. Jerome Weisner, President, Massachusetts Institute of Technology; Chairman, Advisory Council, Office of Technology Assessment, before the U.S. Senate Judiciary Subcommittee on Constitutional Rights and the U.S. Senate Commerce Special Subcommittee on Science, Technology, and Commerce, on "Surveillance Technology," 94th Cong., 1st Sess., Sept. 10, 1975 . . .

I am pleased to appear before your subcommittee once again to talk about questions of electronic surveillance, communications, data banks and their potential impact on privacy, because I believe that issue is at the center of our efforts to survive as a free, democratic society.

It is heartenin, that your subcommittee retains its deep concern about the threats posed to the individual liberties and civil rights by the modern electronic communication and information processing capabilities and continues to seek ways of strengthening the laws that insure those rights.

I testified regalding these problems before this same subcommittee in 11171-albeit under different leadership. In preparation for that testimony, I investigated the issues involved rather thoroughly.

Though I have not had the opportunity to prepare myself as well for this appearance, I believe that I can make a useful contribution by reviewing my earlier testimon and bringing it Up to date, particularly with regard to possible safeguards.

We now know that individuals in this country actuallv experienced abuses of their personal liberties that in 1971 were only theoretical possibilities, or were merely suspected to exist.

We also know that these acts of surveillance and of,her violations of rights of individual privacy were not merely an occasional excess, but represented systematic behavior and therein represented a threat to the integrity of the \'ery democratic process.

In earlier hearings witnesses told about the many possibilities for employing electronic devices, computers, computer networks, and so forth m surveillance activities and the committee assembled this information into a rather frightening prospectus of dangers of the constitutionally-guaranteed freedoms of us Americans.

I recall that at the time, there was a certain skepticism about, the likelihood of the more extreme dangers described, a common belief that the committee was alarmist.

There existed then a reluctance to create adequate safeguards against the violations of civil rights that, unbelievably, I find still exists to some degree even after the revelations of the extraordinary extent and range of the violations of personal right~ of privacy that even the highest officials of the Government have condoned and, in some cases, apparentl.v initiated.

The reluctance to believe that such things could-happen stems partially from an unwllingness of some people to beleive that important persons in the Government and industry would know and systematically violate laws and, I fear, in part from the'widespread belief already alluded to by you that because the primary targets of illegal surveillance were criminals and polltlcal dlssldents, the practice was acceptable.

In my earlier testimonv, 1 said tpat the surveillance problem had become a crisis because ""informahon technology puts vastly more power into the hands of government and private Interests that have the resollrces to use it" and 'ito the degree that the Constitution meant for power to be in the hands of the 'governed', widespread collection of personal information poses a threat to the Constitution itself."

There was. I said at the time, no doubt that technology could be and had been used to assist in the violation of the Bill of Rights. How little

we imagined then. In fact, even today, we-me, you—have no way of knowing whether or not you have unearthed all of the surveillance activities directed against individuals and organizations.

The weight of evidence would seem to indicate not. Certainly the recent undenied leaks about surveillance of international commercial traffic exposes another yet unexplored facet of the problem.

This latest revelation must have a chilling effect on businessmen, though some may accept it as part of the game because the do not understand what the game really is. They are letting inividuals within government change the ru es at will and, unbeknownst to the citizens or the Congress , including suspending the Bill of Rights.

To accept such a uses just to set the stage for the ultimate elimination of the rights of all. Eternal vigilance indeed the price of liberty.

In my previous testimony, I said:

"I have wondered lately whether I am being watched as a threat, as a dangerous enemy of the realm. How do you now that you and your staff are not under continuous surveillance as you plan and carry out this investigation ?" The answer then was you dld not.

I went on to say, "I doubt that anyone is aware of the full extent of the surveillance and information collecting activities that goon in this Nation. I expect that It is the same way today.

Many people, myself included, have long operated on the assumption that our activities are being monitored. I have also operated under the premise that I should not allow myself to be inhibited by such a possibility.

I do this because I have great confidence in the basic integrity of the safeguards built into the administrative and judicial system of the country.

If I lacked such confidence and did not feel that I could defend myself,. were there to be unjust conclusions or accusations? I would undoubtedly feel much more severely restricted.

Since my early testimony, extensive abuses have been uncovered directed against almost every segment of the society. These are now so well known that there IS no need to document those situations for you.

Fortunately, there have also been efforts, through investigations and hearings such as this. to bring these abuses into the open and under legal control. Controls have been established on the uses and transmission of information in files and data banks and controlled access has been provided to individuals to their files.

Rut in spite of such progress as has occurred, it is not possible to say that the surveillance threat is now fully under control of the law and that individuals or organizations whose actions seriously annoy Government officials or are regarded as threatening are free of illegal surveillance.

1 stressed previously, and I want to emphasize even more strongly now, that the violations are made by humans, not by machines. Civil rights can only be protected by men—through laws—as you are trying to CIO, not by technolobgy. I still believe that additional legal safeguards are necessary.

As you attempt to find safeguards against the infringements of privacv that technology has made so much easier, it is lmportant to look ahead and try to visualize how new developments will change

the situation, both in terms of the increased capabilities for surveillance that will be provided and the safeguards that could be provided if they were sought.

1 believe that the most significant changes will come from further computer developments, both in equipment and in the sophistication of programing designed to carry out complicated information processmg tasks.

Improvements in communication technology should also make a 'difference. In particular, new transmission systems capable of carrying vast amounts of information at much reduced costs, facilitatin$_g$ communication among computers, will make possible much more extensive data exchange, information manipulation, and information search.

Three separate computer developments will play a role in the computer field and i@ expansion and extension:

1. The cost of computation continues to fall as new technologies—particularly large-scale integrated circuits are developed. There is no obvious ultimate limit to this trend.

2. More effective computers continue to be developed. Machines with-greater speed and capacity continue to emerge. Storage systems also improve in size, speed of access, and cost per unit of reformation stored.

3. Software technology also continues to improve, making the use of larger, more complex machines worthwhile for information processing tasks.

These trends, if not counteracted, mean that it will become increasin$_g$ly attractive to use computers and communications networks in complex surveillance systems and to program the network to carry out sophisticated sorting, correlation and other search procedures to ldentifv and keep track of subgroups of the population with special characteristics.

With regard to technical safeguards against i misuse of information in files and data banks, the situation remains the same—it depends upon the integrity of the system operator and must remain so.

However, with regard to protection against unauthorized entory into computer systems and communication systems, too, the situation has improved dramatically.

There are now availab!e agreed+upon encryption algorithm for the rotection of computer informatlon system? which provide a very high degree of security against outside surveillance if the user is willing to accept the slight extra complexity and cost they involve.

I suspect that as experience with that program occurs, its use will become quite common. However, I believe that strict controls and tough laws, really en forced,. remam the essential elements of protection against misuses of information technology.

In 1971, I questioned ~heth~r the Bill of Rights was adequate to protect people in their relationship to our modern state. Nothing that has transpired since has calmed my concerns.

On the contrary, the revelations of the p~ 4 years here and observations of the situation m many other countries has reinforced m-y helief thnt trends in modern states-even democratically governed socletics—put too much power in the hands of rulers, even totally honest ones.

In my earlier testimony I said that there was serious danger of Creating an "information tyranny" in the innocent pursuit of a more efficient society. Man trends in social, technical, and industrial evolution have restrictive effects upon the actual freedom of choice and mobility of individuals.

In my view, the most serious problem facing the democratic industrial societies, including our own, is the question of how to manage adequately the complex interdependent world.that is emerging.

This Issue ss closely related to the informatlon problems we are discussing. Many practices that pose long-term threats to democratic government and personal freedom are being, and will continue to be inaugurated because they provide a means of making the society function more effectively.

The exchange of computerized credit information and the exchange of criminal data are examples of this. The ever increasing scale of industry and matching growth in the size of government are also examples.

Many serious students of the social scene question whether it will be possible to preserve our democratic institutions in the difficult time ahead. Robert Heilbroner, for example, in his recent **booli,** ".4n Inquiry Into the Human Prospect," raises many questions about the viability of democratic government, in an era of confrontation politics and resource shortages.

Some sociologists believe that the overriding commitment to efficiency implicit in technolo~ical society has meant from the start that the "needs" of the system, t~e society, would inevitably be given priority over the rights of the individual, and that it was only a matter of time before the democratic processes could not handle the evolving sit uat ion.

This is the central question of our times. Incidentally, what evidence one can gather from the experiences of other countries leads me to conclude that overmanagemcnt of a societ,y actuallv reduces its effectiveness; that centralized control works considerably less effectively than our form of industrial democracy for managing a technological society.

One can see the effects of overcontrol in our own country. Rwulations, needed or desirable for one purpose or another, have almost always restricted the ability of the regulated industries to innovate and respond to changing conditions and thus in many cases have made further controls necessary that in turn introduce further inhibitions on adaptation, and so on.

While this set of problems is perhaps bqvond th~ present interests of the subcommittee, I brin,g them to your attention for I see a major extension of the present set of th r~nts to personal frwdorns in growing controls in the economic and social system.

These trends w-ill pose less of a threat if the safeguards ngain+ misuses of information systems that you are considering are solid and functioning well.

That is why I have stressed the fact that although new technology was R factor in most of the recent excesses, they omlrrcd bemuse of the nbil ity of individuals to carrv out widespread illegal activities undetected or. at least. unreported.

Safeguards must be provided against violation of constitutional freedoms andthesecanonl be provided through legislation; they cannot be provided by technology.

In 1971, I suggested some actions that should be considered to provide such safeguards and in the interim new legislation has included some, but not all of them. I know others of these are still very active on the list of things still being considered

I made the following proposals:

1. Congress should establish a watchdog authority, perhaps an independent agency, possibly a division of the General Accounting Office, perhaps the FCC, to review regularly the public and private information gathering and processing activities within the country. The agency should have the authority to examine the nature and extent of such activities and should report its findings to the Congress and the public.

2 Congress should set rigid limitations on permissible surveillance activities and establish much stronger safeguards—penalties—than now exist against misuse of data-file inf ormatlon.

3. Action should be taken as quickly as feasible to reestablish public confidence in the sanctity of the boundaries. of an individual's physical and psychological living Space. This will require a number ofi steps. Outlawing some activities Such as the free exchange of private information, which has already been done to some extent, collecting data not needed b y an agency, and so forth,will help a good deal. Acknowledging publicly the exten Of pemisslble surveillance and by whom is also mport~n~. requiring disclosur of nonsecurity type data to the concerned Individual seems possllible in many situations. In the few situations where this will not work, as in national security matters, judicial controls should be strong.

4. The development of technical means Of insuring data security and safeguarding privacy should be stimulated and their use required for systems Storing personal information. Much of this has been done.

" These remain Sound go~ls ~nd to the degree that they are yet to be realized, they should be pursued vigorously.

I have become con~rince~ in tl~~ interiln that the s~feguard ~?wtcm needs another el~rnent. rt rn!~~t ~SSllre a greater degree of individual responsibility and accoun$ablljtj'. ~~nfo~tunately, I clo not have a satisfactory proposal to make m this connection.

I see two aspe~ts to the Xlla!ter'. First, t~~e indi.vidwd responsibility not to engage In illegal surve~ll~nee acts Of all k~nds should be firrn] established. This. does not appear ~0 present chfficult problems.

Second, there -1s q nepd to est~h!lsh some degree Of individual accountability for mstltut~onal b~ha~-l~r. Th does appear to posc serious problems.

The first objective,. estab~is~~i?g personal responsibility h:ls bem met to some degree. ~+lred hands In t~~~ ll~atergate C=.e defended their actions on the grouqds that ~h~Y ~~~re just fO~lO~lng orders. The courts, obviously> belleved that they had personal r~spcmsibility for their actions.

The law does not extend this responsibility far enough at tile present time. For example, I doubt that employees of a te~ephone company—

executives, technicians, and so on—who cooperate in an illegal wiretap are guilty of an illegal act. This obviously is a matter of considerable importance.

The second point is much more difficult, for in any obvious form establishing personal accountability for institutional behavior would involve an element of group surveillance which in itself does violence to the meaning of privacy.

Perhaps imposing a clear-cut responsibility upon a definition, small number of officials in an organization is a way to handling this problem. One needs to be extremely careful to avoid a cure that is worse than the disease. Here is an opportunity for a creative act.

I had one final recommendation in 1971 that I want to make again.

We should be prepared to accept the cost of considerable inefficiency in our various social and governmental processes to safeguard our privacy and, as I judge it, our freedom, dignity, happiness and self-respect. By costs, I mean both the financial cost and the loss of a degree of control that the state might otherwise have over genuinely threatening individuals such as criminals and violent revolutionaries and even potential foreign agents.

Our difficult task is to achieve a proper balance between the ability to cope with individual threats to the society and its capability to abridge the freedom and happiness of its members.

In countries where the legal system cannot be counted on, the people are at the mere of the administrators and they must hope that the bureaucracy will be benign. Such a situation smothers freedom. We cannot afford to take the continuation of our liberties for granted.

Thank you.