01

SOME ASPECTS OF TECHNOLOGY AND PRIVACY*

August 25, 1976

Richard L. Garwin **

ABSTRACT: In recent years, rights guaranteed under the First and Fourth Amendments of the Bill of Rights have been violated in ways clearly foreseen by the framers of that Bill and which are in violation of specific law, as well as by the use of technologies which could not have been foreseen. Some of these latter, though probably unconstitutional, apparently violate no present law. The technical aspects of three specific types of invasion of privacy are reviewed—hidden microphones and cameras, intercept of voice and non-voice electrical communications, and the creation and search of large files—and projected to the future. It has been suggested that technology has so changed the world that these rights can no longer be maintained, but it seems that they should not be abandoned without serious exploration of remedies. Three approaches to the assurance of privacy are considered—outlawing the relevant technology, controlling its use by legislation, and restoring privacy by the use of new technology. It is concluded that carefully framed legislation and vigorous enforcement are necessary and sufficient to restore these rights without denying society the myriad uses of these technologies, and that additional assurance can be attained by technological means.

*Published as "INTELLIGENCE and TECHNOLOGY" as a staff report of the Senate Select Committee on Intelligence, Vol. IV, pp. 109-119. "Concluding Remarks" and "Abstract" are restored in the present version.

(04/23/76)

**Post Office Box 218, Yorktown Heights, NY 10598
(914) 945-2555

082576 SATF

BACKGROUND.

The First Amendment right to free speech and the Fourth Amendment right to be secure in one's person, papers, and home have been violated in recent years. Although these rights have been abridged in time-honored ways, in some cases the abridgement has taken place in ways that could not have been foreseen by the framers of the Constitution and the Bill of Rights. A partial list of means employed follows:

- breaking and entering into offices and homes,
- opening of letters in the Postal System,
- bugging or use of hidden microphones with no party to the conversation witting,
- wiretap of telephone communications,
- intercept of telephone communications without actual connection to wires
- intercept of facsimile or printer communication

Although files have existed for many years in all societies, and have sometimes been used to pernicious ends, technology has now made available to the managers of personal files greater speed and efficiency in the retrieval of data, as it has to managers of inventory files, of airline reservations, of the corpus of legal decisions, and of the United States House of Representatives Computer Based Bill Status System. In recent years, too, heightened public sensitivity and legislative activity have begun to introduce legislation, guidelines and standards regarding governmental and private files on individuals, granting the individual in many cases the right to know of the existence and the content of such a file, and to be able to challenge information which may be found in that file [Privacy Act of 1974 (P.L. 93-579); 5 U.S.C. 552A]. Computer technology may not have been instrumental in the misuse of CIA or IRS files to provide information to the White House on U.S. citizens, but the future impact of such technology must be assessed.

FRAMEWORK OF ANALYSIS.

It is a logical possibility that the modern technological tools employed in the exercise of other rights and freedoms for the general and individual good might inadvertently result in such general exposure that the First and Fourth Amendment rights could no longer be preserved, or that their preservation would require severe restriction of other rights and freedoms with major damage to society. For example, such might be the impact of (fanciful and unphysical) spectacles which, while restoring perfect vision to older people, endowed them as well with the ability to look through envelopes and walls.

A second logical possibility is that the general exercise of technology for individual good and the good of society does not in itself imperil the rights under discussion, but that specific targeting of this technology toward individuals can imperil these rights. In this case, the particular threat to these rights could of course be removed by outlawing the subject technology and enforcing such laws. It may be, however, that comparable protection of these rights may be obtainable by legal

restrictions on the *use* of such technology for such invasion, without denying society benefits which would otherwise be obtainable. If similar guarantee of rights may be achieved in this way, the banning of technology (even if politically feasible) would be an exaggerated remedy.

Finally, in some cases new technology may aid in restoring privacy against invasion by people or tools. An old example is the use of locks on doors; newer ones are the use of encryption for written communications and for the privacy of information in files. On the other hand, it would be inappropriate to require the individual to go to great cost to preserve his rights if such preservation could be obtained at lesser social cost, e.g. by restrictions of the actions of individuals who would intentionally violate these freedoms or whose activities might inadvertently imperil these rights. Thus, the expectation of privacy for the contents of a post card sent through the mails is quite different from that of a first-class letter in a sealed envelope, and the cost of an envelope is not regarded as an excessive charge for the guarantee of privacy. As the human senses and capabilities of vision, hearing, and memory are expanded by the use of new tools, what is the place for the analog of better envelopes?

The remainder of this paper is in two parts, the first dealing with covert observation and intercept, the second with the use of files.

COVERT OBSERVATION AND INTERCEPT.

COVERT HEARING (HIDDEN MICROPHONES). It has always been possible for a person to secrete himself, unbeknownst to the participants in a conversation, in such a way as to hear the conversation and so to violate an expectation of privacy ("eavesdropping"). No doubt mechanical aids in the form of tubes were used at times to make eavesdropping easier and less dangerous. Furthermore, rooms equipped with speaking tubes to convey orders to another part of a building were vulnerable to another kind of eavesdropping in which the use of the apparatus was other than that intended.

Microphones were in use in the 19th century for telephone communication and more recently for radio, public address, and recording. The present state of microphone technology is apparent to us all, with microphones a few millimeters across and a millimeter thick common in portable cassette recorders in use for business, education, and pleasure throughout the world. Over the last few years, the development of integrated-circuit technology and its extremely wide use in such recorders, in stereo equipment, and in calculators (as well as in more complicated instruments) has provided not only the possibility but also the widespread capability to house amplifiers in a space of a few cubic millimeters and with power consumption of microwatts. Thus, microphones can be hidden in walls or moldings of rooms, in furnishings, or in personal possessions. They can be left behind by visitors or can be introduced as part of the normal resupply or refurbishment process.

Microphones can be accompanied by self-contained recorders or can transmit the signal (usually after amplification) either along near-invisible wires or by radio. In the case of wire or radio transmission, there would normally be a recorder or more powerful relay at some small distance of a few meters to a few hundred meters. The power requirements for microphones and amplifiers can be provided by batteries, by connection to the normal building power supply, from the telephone system, or by silicon or other cells converting sunlight or roomlight into electrical power. Microphones can also be provided with power by the absorption of radio or microwave

signals, and can retransmit intelligence on the same carrier waves. In addition to dedicated wires or radio transmission, the microphone signal can also be transmitted on the building power line or on the telephone lines, if any. Under most circumstances, the ability with further advance of technology to make microphones still smaller would not be of great utility. They are already small enough to pose a near-maximum threat.

Not only are apparatus containing microphones available by the tens of millions throughout the world, but the components are also common articles of commerce and can be assembled by anyone of millions of people. Many rooms are now permanently equipped (entirely overtly) with microphones for use in recording conferences or in picking up clearly comments made by an audience during question period. Such microphones could easily feed recorders, wires, or transmitters at other times as well. Furthermore, every loudspeaker, whether built-in or part of a portable electronic device, is capable of working as a microphone in just this same way. Individuals with impaired hearing have particularly small microphone-amplifiers, some of them concealed in the frames of eye glasses.

A slightly different kind of covert hearing is said to be possible by detecting with laser beams the vibration of ordinary windows enclosing a room in which the target conversation is taking place. Another approach to overhearing conversations outdoors is to use large directional microphones distant as much as one hundred meters.

Retarding the further development of microphone technology for commercial purposes would be of little help, even if it were feasible, given the already small size of microphones. It seems likely that privacy can be adequately protected against covert hearing in the United States by proper legislation and enforcement requiring a warrant for the exercise of covert hearing capability. There being no expectation of privacy against a person present, legislation in the future, as now, should not restrict covert recording or retransmission by a person present, whether that person participates in the conversation or not. Of course, covert hearing capability can be banned administratively from designated premises, as it is now, by those in control of the premises—e.g., "no microphones, radios, recorders, etc. at defense installations" (or on premises operated by the XYZ company).

COVERT SEEING (HIDDEN CAMERAS). Hidden cameras (whether electronic or film) can imperil Fourth Amendment rights in analogous fashion to hidden microphones. Observation through a crack or peephole; personnel observation via a partially transparent overt mirror; large automatic or remote-control cameras or TV-type sensors behind an overt mirror, small cameras behind a small aperture—this series represents the application of technology to the goal of covert seeing. Vision comparable with that of a person can be obtained through a hole about 3 mm (1/8 inch) in diameter. A 1 mm hole would permit commercial TV-quality pictures. Reading the text of papers on a desk across the room will require a larger aperture. Unlike microphones, such cameras are not yet common or cheap. A film camera taking a picture every 5 seconds would need a considerable film supply and would have to be quiet if covert; a TV camera capable of communicating even at such a rate, with human vision quality is feasible, but is at present costly. With time, the technology of fiber-optic signal communication will allow unobtrusive relay from a hidden camera. A command link could direct the view of the camera toward the interesting portion of the room, saving power and communications rate (as could built-in intelligence at a later time).

Clearly, the invasion by covert seeing of privacy would be intentional, not the result of innocent exercise of rights on the part of others. As such, preservation of such privacy can look toward legislation and the enforcement thereof, with such unconsented observation available only under warrant.

WIRETAP OF TELEPHONE LINES. Anywhere on the line running from the telephone instrument through the building to the junction box and on to the local exchange (typically a mile or so from the subscriber's instrument), connection to the line or proximity to that line will allow a high-quality telephone conversation to be provided for listening or recording. For many decades there has been no need for physical contact with the line to allow "wiretap," and no telltale click or change in quality is necessary or likely.

The technology needed for wiretap (whether by contact or non-contact) is primitive compared with that used for covert hearing. There is no way in which this technology can be outlawed without outlawing telephones themselves. However, in this field particularly, there is no necessity to abandon the protection of privacy. The intercept of communications from telephone lines may readily be controlled by legislation and by the requirement of a warrant for such actions by government bodies [Omnibus Safe Streets and Crime Control Act of 1968; 18 U.S.C. 2510-2520].

INTERCEPT OF VOICE FROM DOMESTIC MICROWAVE RELAY. In the United States, most telephone calls beyond the local area are now transmitted via microwave relay. Towers about 20 miles apart contain receiving antennas, amplifiers, transmitters, and transmitting antennas. The microwave relay system operates near 4000 megahertz and 6000 megahertz, at wavelengths on the order of 6 centimeters.

The transmitted beam from each of these relay towers has an angular width on the order of one degree and so can be picked up well over a wedge some 20 miles long by a third of a mile wide. Leased-line services such as the federal government FTS system, WATS lines, and individual corporate "private-line" networks occupy permanent positions in the frequency spectrum in those relays which are used to carry the signals (not always by the most direct path) over the fixed network. Direct-distance-dialing calls, constituting the bulk of the traffic, cannot be so precisely located. In general, however, these DDD calls are preceded by digital information which serves to direct the call to the receiving telephone number and to indicate the calling telephone number as well.

At present, an individual with an instruction manual and a few thousand dollars worth of equipment can set up a makeshift antenna and listen or record continuously calls on any desired fixed-assigned channel. In principle, even the DDD calls could, at substantially larger investment, be matched with a list of "interesting" telephone numbers so as to record only those calls originating from or directed to a given subscriber number.

These voice messages, having traveled by wire at least some distance from the telephone instrument, are legally afforded the same protection as calls carried on wire from sender to receiver [18 U.S.C 2511]. Protection of privacy of communication requires the enforcement of this law. However, questions of extra-territoriality arise. There appears to be no way in which individuals on foreign embassy and consular properties can be forbidden from listening into those microwave links which pass their territories. It must be anticipated that certain powers will use such informa-

tion not only for affairs of state[1] but also simply to earn funds by taking advantage of information which is obtained in this way. Communication in regard to commodity markets, stock exchanges, and bidding prices for large contracts, all convey information which can have substantial value.

Given this peculiar situation, one might judge that the threat to privacy from all but extra-territorial intercept is adequately controllable by a legislative ban on such intercept (and the requirement of warrants for government "search"), and that the rather limited exposure to personnel controlled by foreign powers and based outside the reach of U. S. law can be controlled by other means. Voice links carrying defense information are all encrypted. Other important information of the federal government can be rerouted to avoid some small number of possible listening posts. Direct-distance-dial calls eventually will be relayed with the destination and origination information going over separate channels. When all-digital transmission is used to carry voice, encryption can be available at negligible cost. It could be implemented with separate keys for each microwave link, or encryption could be done at the point of digitizing each signal, or both.

INTERCEPT OF NON-VOICE FROM DOMESTIC MICROWAVE RELAY LINKS. Many channels on U. S. microwave relay are devoted to the transmission of non-voice information (facsimile machines, teletype, telex service, other printer traffic). The comments above regarding the intercept of voice communications from such microwave links apply with equal force to the intercept of non-voice communications. There is, however, a major difference. Existing law protects only communications from which intelligence can be "aurally acquired" [18 U.S.C. 2510(4)], so there is at present no legal bar to the intercept of such non-voice communications.

At present, the value of the average non-voice communication relayed over the microwave net is probably greater than that of the average voice communication. Even when non-voice might be protected by new legislation, it would still be subject to intercept from extraterritorial sites. Fortunately, the protection of non-voice data transmission by means of encryption is far easier than is the case for voice and is practical now over all telex and printer links. Several machines and electronic devices of varying effectiveness are available to provide end-to-end transmission security. The National Bureau of Standards has begun the promulgation of a national standard for data security via encryption, which apparently satisfies the concerns of the United States Government for maintaining the privacy of non-defense information.

INTERCEPT OF VOICE OR NON-VOICE FROM DOMESTIC COMMUNICATION SATELLITE LINKS. About half the international common-carrier communications originating in the U.S. goes by satellite and half by submarine cable. A rapidly increasing fraction of purely domestic communications is now relayed by satellite. Present satellites may receive communications from any one of a number of ground stations and simply rebroadcast the signal at a different

frequency , covering the entire 48-state U.S. with the microwave beam. For some communications with multiple addressees, this large potential receiving area is an advantage; for most communications with a single addressee, the particular ground station to which the message is addressed will recognize the digital address and record or retransmit the message into the local net (or print it and put it into an envelope for delivery, etc.).

Modern relay satellites are in stationary orbit, so that a fixed antenna can be used to receive signals, rather than the tracking antenna initially required for the lower-orbit satellites. Thus, anywhere in the large area illuminated by the satellite microwave beam, a relatively simple antenna and amplifier would allow intercept of messages relayed by satellite.

The satellite transmits microwave energy not only onto the land mass of the U.S., but also onto adjacent waters and countries, including Cuba. Non-U.S. citizens on non-U.S. territory are completely free to receive satellite relay of domestic U.S. communications and to do with this information whatever they will.

Although some satellite relay is digital in nature and thus readily protected by encryption at negligible added cost, the voice communication is primarily analog (whereby the intelligence is carried by continuous amplitude or frequency modulation as is the common case for terrestrial multiplex relay). Encrypted voice communication would require a wider channel at present than is needed by analog voice, but the additional cost for privacy via encryption might be small even so, since the satellite resource is a small part of the end-to-end communications cost.

Unfortunately, domestic satellite relay, as presently practised, is an example of a case in which the indisputable benefits of technology bring with them a threat to privacy. In this case, it is not the application of technology to intercept but the technological nature of satellite transmission which makes intercept as easy outside U.S. territory as within, thus putting protection of privacy outside the reach of U.S. law. Technology in the form of encryption provides an adequate solution. This remedy is available now for non-voice communication and could be used with equal ease for digital voice. Aside from encryption, satellite voice communication could be provided some degree of protection in the near future by avoiding fixed-assignment schemes for users desiring privacy.

FILE TECHNOLOGY.

SOME EXAMPLES OF CURRENT STATUS. Among the early large computerized file-oriented systems were the airlines seat reservations systems now in use by all U. S. airlines. The overall system accommodates thousands of flights per day, with a hundred or more seats per aircraft, and can handle reservations months in the future. A reservation can be made, queried or cancelled within seconds from many hundreds or thousands of terminals. Some of the records may contain little more than the name of the passenger; others may include a complex continuing itinerary, with hotels, car rental, telephone numbers, and the like.

Seismic data bases are used by oil exploration companies to hold seismic reflection data and core logs. The former is the pattern of reflected sound waves versus time at various microphones which are sensitive to signals from a small explosion at the surface of the ground. The reflection comes from change of structure at different levels in the earth below. Core logs (or bore logs) may measure the detailed ground conductivity, water content, radioactivity content, and the like in tens of thousands of oil exploration wells. The material is kept computer accessible so that it can be retrieved and processed in a timely fashion as new tools are developed or as new information makes it desirable to compare with old information in the neighborhood.

Several government echelons have tax data bases. At the city or county level, such a data base may include details about every dwelling in the city. Such data bases can be particularly useful in case a blanket reassessment is desired.

The New York Times Information Bank ("NYTIB") provides at the New York Times building both abstracts and full texts of articles published in that newspaper. From remote terminals, subscribers can search the compendium of abstracts for all articles which have been published in the New York Times and may request photocopies of the full articles whose abstracts satisfy the search criteria. The abstract searching can be full-text search, i.e. a search on the name "Harold Ickes" might result in a sheaf of abstracts, accompanying stories most of whose headlines say nothing about Ickes, but may refer to Roosevelt.

Full-text search capability is used in several states for purposes of law and legal decisions. In addition to struggling with the often inadequate index to such a corpus, an attorney can undertake a full-text search for statutes or cases which have some characteristics in common with his current concern.

The United States House of Representatives Bill Status Office handles over 1000 telephone inquiries each day concerning the status and content of legislation which has been introduced into the House.

All these are file-oriented systems, some of which may retrieve files according to the index system under which they were prepared; others, as we have seen, have a full-text search capability, such that a file can be retrieved in accordance with its *content* rather than heading.

Computer file systems are now in common use for text preparation and editing. A draft letter, report or publication is typed at a terminal connected with a computer (or sometimes at a stand-alone system). At any time, portions of the draft can be displayed, typed out locally or on a fast printer. The typist can enter corrections into the computer system (including global changes, e.g. to change the group of characters "seperate" every place it may occur into the group "separate"), can rearrange paragraphs, append additional files, and the like.

USE OF FILES IN INTELLIGENCE WORK. The work of intelligence agencies and their analysts is in large part the production of reports. There are routine periodic reports, reports in response to specific tasking on questions of concern to national leaders, reports which are initiated internally to the agency in response to some fact or complex of facts which seems to require attention at a higher level. In presenting any such material, the analyst needs to obtain as much other information about the subject (What is the significance of the appointment of an unexpected

person as premier?) as is possible. There is a strong analogy to the NYTIB which should also serve to provide responsible reporters with other information on the subject of current interest (earlier, perhaps contradictory speeches of public officials, and the like).

Intelligence files may also have agents' reports, which are in the nature of fragmentary newspaper articles except that they are secret. Raw intelligence files may also contain the full text of foreign radio broadcasts as transcribed and circulated in printed form by the Foreign Broadcast Information Service (FBIS). If plaintext messages of a foreign military commands are available, they will also be filed, and for efficient search and retrieval preferably in a computer store.

The use of computers in all these file applications—commercial, educational, and intelligence—is motivated by the same drive for efficiency, reliability and the capability to retrieve materials at places, times, and by persons other than those who have filed them. Computers at present are not normally used to store pictures or things, but indexes to such collections can as readily be placed in the computer as can any other kind of information. In contrast with a single physical file of paper documents, the computer store never suffers from the document's unavailability because it is on somebody else's desk. Multiple copies of a micro-image store can also satisfy the requirement for multiple simultaneous use, but cannot be updated or searched so readily as can a computer store.

NEAR-TERM FUTURE FILE TECHNOLOGY—PERFORMANCE AND COST. In any case, it is not the purpose of this note to design a file system for the intelligence community, but rather to inquire as to certain aspects of privacy in regard to such files. The Privacy Act of 1974 is both the result and cause of increased interest in design of safeguards, which is at present the concern of an active subset of data-processing professionals and of a number of existing organizations,[2] including the Privacy Protection Study Commission, but a brief discussion of near-term future technology may be of help.

Obviously, concern regarding files and privacy is with the chain of information from collection through storage and retrieval. One worry is that some government organization by the expenditure of enough money, could have the capability to "know everything about everyone" at any time. Because there is no general public right of access to the files of the intelligence agencies, it is of interest to know what these capabilities might amount to, as a guide to the introduction of safeguards.

In order to provide some intuitive feeling for the magnitudes involved, consider the storage of full page, double-spaced text. Such a page may have thirty lines of sixty-five letters or digits, or about 2,000 characters per page. Except as noted, it is assumed that a character requires one "byte" (8 bits) of storage, although by appropriate coding of text, one can store as many as three characters per byte.

Using a typical modern disk-pack magnetic storage device, storage of 300 million bytes can be obtained for a rental of about $1500 per month, or some $5 per month per million characters. Such a device can transfer about 1.2 million characters per second, so it would require 250 seconds to search its entire contents if the logical search device could operate at the storage data rate. Search is normally done by a query, looking for an exact match in the data stream as it is brought from the store. Examples of simple queries are: "theft of service" in the case of the legal corpus;

"Chamberlain/Munich" in the case of the NYTIB (where the "/" simply means that both "Chamberlain" and "Munich" should be in the same document); "seperate" in the case of ordinary text processing where the properly spelled word "separate" is to be substituted. Such queries against a small data base are handled well by a general purpose computer. Indeed, large data bases also have some structure which can often be used to reduce by large factors the amount of data which actually has to be searched. But even if the data base has little structure, one could imagine streaming the entire data base past some modest special-purpose electronic device (a "match register") which may detect a match against the query and divert the matching document into a separate store, where it may be brought to the attention of the analyst. In large production, such a match-register might be bought for $100 in modern integrated-circuit technology. In any case, the cost of special-purpose match-registers would be small compared with the cost of the massive store and will henceforth be neglected here.

By such techniques, as many queries as are desired may be entered from terminals and simultaneously matched against the entire data stream. If the data base is entirely in this type of storage (at a present cost of $5 per month per megabyte, or 50 cents per month per nominal file of 50 typed pages) any query can be answered within five minutes. Of course, a single query might lead to many other sequential queries before all the desired facts are at hand, but the time is measured in minutes, not months.

Given that most queries need not be answered in minutes, one can ask the cost of a slower system. There are now commercially available tape library products, of which a typical one can store 35 billion characters at a cost of about $18,000 per month (so 50 cents per million characters per month). This particular device can deliver data at a rate of 0.8 million characters per second, so that it would require some twelve hours for such a store to be searched entirely for as many queries as have been presented. The range of cost associated with such a system with current technology and twelve-hour response time thus goes from $10 million per month for a system capable of storing 50 pages on each of 200 million individuals (without encoding) to about $200,000 per month for a system storing the same amount of information on each of 10 million individuals, with the characters compacted into more efficient form for storage.

So much for the near term technology. It is being developed in this country and abroad entirely for commercial purposes. It serves highly important functions in allowing any organization—commerce, industry, government, and the professions—to manage information quickly and accurately.

Yet fresh in our memory is the use by the White House of the CIA to provide a "psychological profile" on Daniel Ellsberg. An ordinary file drawer would be adequate if one knew long in advance that information would be requested on this particular person. Given the unusual nature of the case and the non-existence of that particular file drawer, it would be technically possible to search all government files for documents which mentioned the name in question. This would bring to light, of course, income tax returns, military service history, all employees for whom social security tax had been paid in the past by the individual in question, names of relatives, etc. etc. This material would not be found in *intelligence* files, but it could be found if the queries were made available to cooperating individuals with access to files in non-intelligence agencies like the IRS, the SSA, Selective Service, and the like. Additional important information might be available by use of the NYTIB as a commercial subscriber.

Thus the problem in regard to those intelligence agencies with large files of raw data is to ensure that these files are used only in support of the authorized mission of the agency and are *not* exploited for purposes of improving prospects of incumbent officials in an election, of punishing those on an "enemies list," and the like. But it is no longer enough to proscribe the creation of specific files on U.S. citizens; it is now possible to recreate such a file from the central file in less than a day, or to answer questions from the central file without ever having a manila folder or file drawer labelled "John Smith." There must therefore be control over the queries asked of the file, of whom, and by whom. It is just as important to ensure that information given freely by individuals to non-intelligence agencies is not exploited for unauthorized purposes and is not accessible to unauthorized individuals.

The computer technology which makes possible rapid access to large masses of information also allows in principle for control of access to that information. Measures for preventing illegitimate use of government files must be proposed by the Executive, which can obtain help from equipment manufacturers, organizations experienced in computer use and analysis, and from the scientific societies. Such measures could be embodied in Executive Orders. Their adequacy and the need for legislation providing criminal and civil penalties should be the subject of Congressional hearings and research.

SAFEGUARDS which are being considered and partially implemented in non-intelligence files are the following:

1. There should be a limitation as to who can keep files on individuals. (But clearly the New York Times is allowed to put their own newspaper into computer-readable form. And is it a file an individual if the individual's name is only mentioned in a larger document?),
2. Individuals should be allowed access to their files (for repayment of the actual cost of search) and to receive the information in the file on them. (But if the file is very large, such access might be *made* very expensive. On the other hand, if the access were treated like an ordinary query in the example above, the cost might be quite reasonable.),
3. The individual should be allowed to write into the file in order to contest the facts or in order to present his own point of view,
4. There must be limitations on those who can gain access to the file or who can receive information from the file,
5. Duplication of the file must be limited and unauthorized access prevented,
6. There should be an indelible record of *who* has queried the file and *what* questions were asked, so that failure of access limitations will not go undetected.

Among the safeguards for any system should be adequate requirements for identification of terminals from which queries are being made, identification and authorization of the individuals who query, a complete record of the queries (with terminal and individual identification), adequate security against transmitting large amounts of information and the like. The moment-by-moment execution of these controls on access is the task of the set of computer instructions known as the "operating system."[3] Although the design of an adequate operating system is a difficult task, the detailed specification of the controls is itself non-trivial and must be done with some understand-

ing of what is technically feasible at present. Fundamental to the continued effectiveness of such safeguards is the maintenance of the integrity of the main program which controls the computer. Even in highly classified applications, there is no reason for this main operating program to be classified, and a source of strength should be public scrutiny of this operating system. Clearly, the introduction of access controls should not wait for the perfect operating system.

No matter what the safeguards, individuals might be able to gain access to some information for which they are not authorized. Adequate legislation, criminal penalties, and the enforcement of these laws should deter many who might otherwise try. Data security measures, such as encryption of the file itself, can help also.

What must be particularly guarded against is not so much the misuse of intelligence files but the misuse of information freely given or collected for authorized purposes and which is then turned to an improper use. Indeed, open analysis by all those concerned should lead to an understanding of the protection which may be provided.

CONCLUDING REMARKS.

Appropriate legislation must be enacted for the protection of First and Fourth Amendment rights against abuse by the threats considered here—covert hearing and seeing, intercept of voice and non-voice communications, and misuse of files. Portions of such legislation should be drafted with the participation of competent elements of the Executive (the National Bureau of Standards, the Intelligence Community Staff, and the like), legislative elements (e.g., Office of Technology Assessment), professional societies, and various commissions charged with study of the protection of privacy. Equal attention must be paid to the non-technical portions of the legislation—clear statements of the conditions for issuing of warrants; assignment of individual personal responsibility to government officials and others who violate the law, with substantial criminal and perhaps civil penalties prescribed. Such legislation should not be so narrowly drawn as to fail of protection against present technology or that which may arise in the future. Even appropriately broad legislation will have to be reviewed periodically in the light of experience and new technology, to ensure that these rights are protected against the actions of government and of private individuals.

REFERENCES.

1) "Report to the President by the Commission on CIA Activities Within the United States" (June 1975), p. 8.

2) See for instance National Bureau of Standards Publications:
FIPS PUB41—"Computer Security Guidelines for Implementing the Privacy Act of 1974 (SD Catalog Number C13.52:41), and
"Executive Guide to Computer Security (Available from the Institute for Computer Sciences and Technology, NBS, Washington, DC 20234).

3) An introduction to the problem may be found in, e.g. "The Protection of Information in Computer Systems," J. H. Saltzer and M. D. Schroeder, Proc. IEEE, Vol. 63, No. 9 (September 1975), pp. 1278-ff.