Conference on

THE BOUNDARIES OF PRIVACY IN AMERICAN SOCIETY

Director: Mr. George B. Forgie

Fall Term 1971

Volume I

Princeton University.
Woodrow Wilson School of Public & International Affairs,
Princeton University
Princeton, New Jersey

1st Copy

CONFERENCE ON THE BOUNDARIES OF PRIVACY IN AMERICAN SOCIETY

Final report
January 4, 1972 Chairman: Samuel Alito

The Conference on the Boundaries of Privacy in American Society agrees unanimously that privacy is a value of fundamental importance. Both modern experimental psychology and the traditional image of man in the West agree on this point. Psychological studies suggest that privacy is essential for creativity; tests which investigate the effects of physical crowding on rats have alarming implications for the accelerating world population and the trend toward urbanization. More studies in both these areas would certainly be beneficial. The traditional western conception of man has laid great emphasis on the worth of the individual; if this image is to be retained, if we are not to move beyond freedom and dignity, privacy must be vigilantly safeguarded.

Compared to more traditional social values--such as liberty, equality, justice, toleration, and order--little has been written about privacy. This is certainly understandable, for only in the present age has it become possible to destroy privacy on a mass scale. On the other hand, privacy is certainly part of other political values, e.g., liberty and toleration, about which much has been written. And, at least in its exagerated forms, privacy is at odds with some traditional political values, e.g., community and attempts to achieve equality, justice, or order. All this is to say that, whereas the Conference unanimously regards privacy as a value of very great importance, we regard it as one important value among many.

At the present time, however, we sense a great threat to privacy in modern America; we all believe that privacy is too often sacrificed to other values; we all believe that the threat to privacy is steadily and rapidly mounting; we all believe that action must be taken on many fronts now to preserve privacy.

Privacy and Social Services

The vast increase in social services provided by the Federal (and state) governments since the Great Dppression has necessitated a corresponding increase in the amount of information colleated about the citizens. Although the motives of those who collect this information are almost always benevolent, the possibility of abuses exists; indeed there is a lengthy history of such abuses. The decennial census, for example, to which the citizen is required by law to respond, has included some questions which unjustifiably invaded the citizen's privacy. In addition, census information, once collected, has been improperly used and has even on occasion been distributed to industry. We recommend that Congress curb these abuses by taking the following steps: 1. Congress should clearly specify the areas in which the citizen may be questioned and required to respond; 2. all other questions included on the form should be clearly labeled optional; 3. the census bureau should not be allowed to report information on particular individuals to anyone; 4. Congress should prohibit the census bureau from reportimg any information to industry which is not available to the public.

Home visitations by social workers have sometimes been abused by federal agencies. We recommend that the law specify the number, length, hour, and frequency of permissible visits and the amount of prior notification due the person visited. Home inspections for the enforcement of federal health, fire, and building codes have also led to abuses. The Supreme Court has ruled that these administrative searches are protected by the guarantees of the Fourth Amendment. Camara v. Municipal Court, 387 U.S. 523 (1967). We, therefore, believe the judiciary should be entrusted with preventing abuses of this nature.

We recommend the creation of a three-man Federal Privacy Ombudsman to 1. hear citizen complaints about all invasions of privacy by agencies of the government not concerned with either the prevention of crime or matters of national security, 2. to watch out for invasions of privacy by the aforementioned agencies, 3. to inform the responsible agencies of its findings and recommendations, 4. to publicize its findings.

In addition, we propose that many of the regulations contained in House of Representatives Bill 9527 be enacted. These regulations, which again apply only to those agencies not concerned with either prevention of crime or matters of national security, include the following: 1. any individual on whom a personal dossier is maintained must be so notified; 2. the information contained must not be disclosed without the individual's consent unless the law expressly permits or requires disclosure; 3. except as provided by law, the individual must be allowed to request a copy of his file; 4. the individual must be allowed to add material to his file in order to refute allegedly erroneous or misleading information; 5. a list of those persons inspecting a given file and their reasons for inspecting it must be maintained.

Finally, we propose the establishment of an efficient Federal Statistics Office to handle all interagency transfers of statistics. (Again we exempt those agencies which deal with crime or the national security.) This office will insure that bulk statistics rather than personal dossiers are transfered. In addition, we believe the uniformity and centralization inherent in this approach will not only contribute to government efficiency but will make it easier to spot and eliminate invasions of privacy.

Privacy and the Computer

The cybernetic revolution has greatly magnified the threat to privacy today. Computers have made it possible to store vast amounts of information in a relatively small space and to retrieve desired pieces of stored information quickly. The potential for invasions of privacy through the use of computers is growing rapidly; more computers are installed each year; more tasks are turned over to computers; and most important, computer systems are rapidly becoming centralized. Centralization, the creation of vast computer networks, opens the possibility of bringing together an enormous amount of information about every facet of an individual's life.

We believe the potential for invasions of privacy through the use of computers is so great that all private computer systems should be licensed by the federal government. We propose the creation of a federal regulatory agency to supervise the licensing of systems and the enforcement of all federal regulations. We suggest the agency be staffed by career civil servants and that they be appointed to serve fixed terms. It is our hope that these measures would greatly hinder undue influence by interest groups. Any suspension of a license by the agency could be appealed to a District Court.

We also urge Congress to enact requirements in the following areas for the issuance of an operating license: the nature and purpose of the system, the class of customers it will serve, the data sources upon which it will draw, the checks to be established to validate information fed into the system, and the tests to be performed on the system to assure that it operates properly. Congress should also require that every computer have the following physical safeguards to prevent illicit obtainment of information: partitioning of memory banks, simple encryption codes, and real-time monitoring and random auditing of the security system. In addition, we propose that a commission be set up within the regulatory agency to conduct research on centralization trends, technological safeguards, and the potential effect of future computer systems on information storage.

We suggest that the Congress also charge the Federal Privacy Ombudsman with examining the computer systems of the federal government with and eye to the criteria mentioned above with regard to private computers. We recommend that the state governments use the federal regulations as guidelines in evaluating their own computer systems and that each state government create an appropriate board to police its own computer systems. And we recommend that Congress provide financial incentives for the states to follow this suggestion.

Privacy and Security

It is indisputably legitimate for the government to attempt to prevent crime and subversion or, once they have occurred, to apprehend and punish those responsible. But we are convinced that in recent years government has often used improper means to gather information about individuals who posed no threat either to their government or to their fellow citizens. Many of the research papers submitted by members of the conference provide ample documentation for this point.

Most of the problem in this area involves surveillance by the federal government of persons it believes to be subversive. In general, this in the province of the Federal Bureau of Investigation and it is completely improper for the Central Intelligence Agency to enter the field as it has apparently done in recent years. It is also quite wrong for military intelligence to get deeply involved in domestic surveillance. The Army began widespread domestic surveillance in the 1960's to aid in quelling civil disturbances. As racial disturbances gave way to antiwar protest in the late 1960's the Army began gathering information on a large group of Americans including

both out-and-out revolutionaries and mild dissenters on the war in Vietnam. It is our strong conviction that domestic surveillance by the military, if it is to exist at all, must be tied closely in time, location, and scope to the strong possibility that military units may have to be used to quell a disturbance. This is admittedly a vague prescription, but in an area as secretive and sensitive as this, it is inadvisable--indeed impossible--to attempt to draw up clear regulations which must always apply.

We think a wiser policy is for Congress to set up a Joint Congressional Committee on Domestic Surveillance by the Federal Government. This committee could prevent domestic surveillance by the C.I.A. and supervise domestic surveillance by the military and the separation of Army intelligence files from Army security clearance files. Each house should elect three members, one of which should be from the Committee on Armed Services and two from the Committee on the Judiciary.

While it is clearly the responsibility of the F.B.I. to investigate internal subversion, it is the consensus of the Conference that the F.B.I. has interpreted internal subversion too broadly in recent years. It is our hope that a Joint Congressional Committee on Domestic Surveillance by the Federal Government would be able to restrain the F.B.I. from commiting similar abuses in the future.

We feel it is unjust for minors to be included in the same criminal files with adults and for the records of all those arrested or indicted not to mention that the accused was never convicted; we believe these practices must be stopped. Also, records of juvenile delinquents should be destroyed if their records remain clear for five years.

Two of the principal means of government surveillance arewiretapping and electronic eavesdropping. Since their inception, both these procedures have had a long and stormy history in the courts. In Katz v. U.S., 389 U.S. 350 (1967) the Supreme Court held that wirtepaping and eavesdropping are constitutional under "specific conditions and circumstances," where probable cause is demonstrated, and where a warrant is obtained." Katz provided the consitutional framework for the Federal Omnibus Crime Control and Safe Streets Acts of 1968. Title III of the act accomplished two broad goals: 1. it prohibited wiretapping and electronic eavesdropping by privete cigizens; 2. it specified how and in what circumstances law enforcement officials could wiretap and eavesdrop. We believe that Title III is essentially correct in its approach to the regulation of wiretapping and eavesdropping, but we would suggest the following modifications:

1. State standards should not be more permissive than federal standards. Whereas the offenses for which federal officials may conduct surveillance are enumerated, the states are permitted to conduct surveillance for any crime "dangerous to life, limb, or property or punishable by imprisonment for more than one year." The upshot is that states may wiretap and eavesdrop in investigation of almost any crime. We suggest the offenses for which the states may engage in surveillance also be listed.

   Title III allows the states to obtain warrants to conduct electronic surveillance from "a judge of any court of general criminal jurisdiction of a state who is authorized by a statute of that state." This rule is too broad; only state superior court judges should be so empowered. Likewise, the category of those officers allowed to conduct surveillance is too wide. The law presently allows "any investigative or law enforcement officer of the state or political subdivision thereof" to wiretap and eavesdrop. We recommend that only a specialized corps of officers be granted this authority.

2. "Consent surveillance" should be regulated by a uniform federal standard, but Title III leaves "consent surveillance" unregulated.

3. The "emergency authority" to intercept communications should be contracted. Officials should begin to seek a warrant while, not after, the equipment is put in place. The 48 hour period of grace may well be too long; studies should be conducted to see if it could be shortened.

4. The interception of privileged communication, e.g., lawyer-client, doctor-patient, should be prohibited.

5. The present 30 day limit for surveillance should be reduced.

6. A Federal Court of Warrants should be created to issue warrants for electronic surveillance in all cases involving the national security. It is not yet perfectly clear what the powers of the President and the Attorney General are in national security cases, but in the pending Smith-Plamendon case, the government is contendidng that in these cases the President and Attorney General should have the power to decide what consitutes probable cause for initiating surveillance. Recognizing both that the usual procedures may be inappropriate in cases involving the national security and that the system proposed by the government is highly susceptible to abuses, we propose that a Federal Court of Warrants be created solely for the purpose of hearing these cases.

The members of this court would be appointed in the same way as are other members of the federal judiciary.

Laws concerning Homosexuality

The Conference voted to recommend that the current sodomy laws be changed. The Conference believes that no private sexual act between consenting adults should be forbidden. Of course, acts of a coercive nature, acts involving minors, and acts which offend public decency should still be banned. Discrimination against homosexuals in hiring should be forbidden.

Privacy and the Private Sector

Only recently has the issue of invasions of privacy by private firms received much public attention, and even today relatively little has been written on the subject. Members of Commission III very ably reported on three aspects of the problem: the consumer reporting industry, physical and psychological surveillance, and invasions of privacy by the communications industry.

There are basically two types of private organizations which gather data on private citizens: credit bureaus and investigative reporting agencies. Credit bureaus have grown to immense sizes and show all signs of continuing to grow; by 1967, TRW had files on at least 27 million persons. Fortunately these bureaus collect only hard data, e.g., vital statistics, employment records, data from the public record, and credit records. Although we recognize the potential for abuses by these bureaus, we believe that on the whole they perform a valuable public service, and we do not recommend any substantial new regulation of them now.

The investigative reporting agencies are another story. They deal largely in information on personal habits, e.g., health history, reputation, and interests. Their sources of information, which include neighbors, friends, and enemies of the subject, are notoriously unreliable. Furthermore their investigators are often poorly trained, overworked, and under pressure to discover derogatory information.

We propose the following measures to prevent invasions of privacy by private consumer reporting agencies: 1. only "hard," factual verifiable data should be collected; 2. only authoritative sources, such as employers, doctors, and public records should be consulted to obtaininformation; 3. only "relevant" information should be collected; 4. the qualified privilege against libel and defamation suits now granted to consumer reporting agencies should be rescinded.

Private electronic surveillance has become common in almost all areas of modern life in America despite the fact that Congress forbade "the manufacure, distribution, possession, or advertising "of any bugging device with the knowledge that the device would be sent through the mail or transported in interstate or foreign commerce." This law has been very poorly enforced; we recommend strict enforcement. Furthermore, we

suggest that all states ban the intrastate manufacture, distribution, possession, or advertising of bugging devices.

The use of polygraph testing is a potential danger to privacy; the te itself is sound, but the examiners are often poorly trained. We propose in this regard that 1. all states permit the use of the polygraph test, 2. that all states license polygraph examiners and require adequate training as a precondition for certification, 3. that all states prohibit discrimination in hiring and dismissal on the basis of compliance with an employer's request to take a polygraph test, and 4. that the profession of polygraph examiners be encouraged to develop a code of professional ethics.

The common use of personality tests poses much greater problems. Questions on these tests are often of a highly personal nature and include such topics as religion, sexual desires, and personal feelings and relationships. Here not only are those who administer the test often inadequately trained, but the validity of the test itself is debatable. Our research also indicates that in almost all cases the administration of these tests is not essential. We therefore recommend the prohibition of tests which employ the type of sensitive questions mentioned above except when administered by a professional psychologist (with an M.A. degree) to a child in a school, clinic, or hospital and when parental permission has been obtained.

Our Conference is well aware of the great potential for invasions of privacy by the communications industry, but we could not devise any means of eliminating or even substatially reducing that potential without, at the same time, abridging freedom of the press. We submit then that the best approach is self-regulation by the media and that because the media enjoys special protection under the Constitution it must take upon itself the added responsibility to be especially wary of unjustifiably invading the privacy of individuals.

* * * * * * * * *

The erosion of privacy, unlike war, economic bad times, or domestic unrest, does not jump to the citizen's attention and cry out for action. But by the time privacy is seriously compromised it is too late to clamor for reform. We must begin now to preserve privacy, and the first step is for Americans to understand the threats to privacy we now face and the threats inherent in our technological society. We hope that this report may contribute in its small way to the intelligent debate on the problem of privacy which is now under way and which must precede any effective reform.