A Proposal for the Protection of the Privacy and Freedoms in the Information Society

Kim, Dong Hi*

A. Introduction

The expansion and diversification of public administration, industry, and the economy as a whole has forced our society to demand more information in both the public and private sectors. Computers have now come to the fore as the effective means of fulfilling this demand.

Computers, in spite of their late arrival, are now widely recognized as having unlimited data processing and storage potential. With the aid of these information processors, large quantities of personal and other data are being collected, processed, and stored in both the public and private sectors. Their almost unlimited capacity for data processing makes them too strong a factor...to process and store more information than is needed for a specific purpose.

Usually data needed for such a purpose are stored in a central data bank, from which they can be retrieved at any time and place by those who need them, through on-line or time-sharing systems.

In view of this, present-day Korean society is marked by the unlimited capacity of computers to collect, process, store, and distribute data. Their services are demanded by many sectors: government, other administrations, industry, and business groups.

Among the merits of a computerized personal data bank are an increased capacity for data processing, greater efficiency, and avoidance of redundancy. Because precise information on individual citizens is fundamental to efficient administration, computers can contribute a great deal to the increase of efficiency in general administration of social welfare, health and hygiene, and taxation systems, as well as in national security, public peace-keeping, and criminal investigation. Computers not only increase productivity and

* Professor, Department of Public Law, Seoul National University

reduce labor hours, but also release us from repeated, monotonous weekday chores, allowing us to engage ourselves in intellectual and creative work.

Nevertheless, if these computerized data...especially personal data...are unduly monopolized by the government or by certain businesses, we will be confronted with several serious problems.

In the first place, when a business concern or a consumer reporting agency processes and stores incorrect or out-of-date information, and uses that erroneous data in making a decision on a particular person's employment, credit, or insurance situation, it may unfairly limit or deprive him of important economic opportunities.

Second, the use of personal data bank by a private business allows the government to access data easily on the pretext of upholding the public interest; furthermore, it raises the possibility of exploitation of the data by the business itself. Obviously, such abuse of the data would be a serious problem, bacause it would infringe upon personal privacy and freedom.

Finally, the control of personal data banks by the government more seriously threatens the freedom of individuals; for many government controlled institutions for their own purposes collect data on the individual citizens, information that the gvernment may compel citizens to provide. Furthermore, data held by individual governmental institutions work not in separation but in combination, usually through a network of computers. The government holds and controls confidential information on every member of the population, which enables it to impose restrictions on its citizens and to tighten its control of them.

Even in the past, it is true, governmental institutions collected and retained data on the citizens; but in the pre-computer era, the privacy of citizens was safeguarded by the poor capacity for data processing, storage, and utilization. Now, on the other hand, the privacy of individuals is threatened by the computers with their virtually unlimited capacity for processing and exploiting information and for overcoming constraints of time and space.

When data of individual citizens are stored and exploited by governmental institutions through the use of computers, personal privacy is actually exposed and threatened, rendering people "naked" before administrative power. This spectre raises the possibility that the "fishbowl existence of human life" depicted in George Orwell's 1984 will in fact become reality.

Under these circumstances, individual privacy and freedom, even if they

are guaranteed by the constitution, are usually deprived. As long as the individual thinks that records of his past are kept and those of his present are still being collected, he will be psychologically daunted despite constitutional assurances that his privacy will be respected.

But our fear of possible infringements on our privacy cannot deter us from using computers, for using computers is the trend of the future. We should not fight the current, but instead go with the tide, while carefully maintaining safeguards. A computer is itself only a neutral machine; its effect, whether positive or negative, depends on how we use it.

Some advanced industrial countries have already taken legislative measures against the infringement of personal privacy. Typical examples are the Data Protection Act (1973) of Sweden, Federal Data Protection Act (1977) of West Germany, Law on Computer, Files, and Liberties (1978) of France, Data Protection Act (1984) of England, and Fair Credit Reporting Act (1970) and Privacy Act (1974) of the United States.

In connection with this legislation, it should be noted that the laws or acts mentioned above primarily attempt to regulate computerized personal data, but that they also have provisions concerning personal data that are recorded with manual machines or in written form. The lawmaking is based on the consideration that stored personal data other than computerized information can also be used to infringe on individual privacy and freedom.

Korea has no laws as yet that regulate collecting and processing personal data by government and private businesses. But this does not mean that, in our country, there is no infringement of privacy and freedom by means of computerized data.

The rapid growth of urban communities and crowded apartment complexes, the increase in administrative functions and in government intervention in the national life, the acute situation of our national security, the booming of big businesses, the increase in dealings on credit—all these factors will certainly demand more and more personal information data. Because many administrative institutions and private businesses are now employing computers, and bacause our resident registration cards (or number) are utilized as identification numbers, we can easily foresee a future situation, in which computers will be universally employed to process data in both the public and private sectors. This development would mean an increase in the infringement of personal privacy and freedom.

Why the question of regulating the infringement has not been widely

raised can be explained as follows. First, it seems that our people's sense of privacy and freedom is relatively undeveloped. Second, and this seems more fundamental, Korea's problems today in national security, politics, and the economy over all other considerations.

But we must not forget that our dignity as human beings is one of the basic concepts guaranteed by the constitution, and that it is our natural and fundamental desire to enjoy our privacy and freedom. Thus it seems that legislation against the infringement of individual privacy and freedom, which results from the abundance of data in both public and private sectors, will soon emerge as a significant issue.

With this expectation, we will consider in detail the cases of the foreign countries mentioned above and will present a model framework for protecting personal privacy and freedom in the age of computers.

The Privacy Act (USA) of 1974 contains provisions discussing problems in the misuse of personal information and regulates its use to protect the privacy of the citizenry.

The Act states, in its provisions of the Congree Findings, that

(1) The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) The increasing use of computers and sophisticated informations technology, while essential to the effiecient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;

(3) The opportunities for an individual to secure employment, insurance, and credit, and his right to due process and other legal protections are endangered by the misuse of certain information systems;

(4) In order to protect the privacy of individuals identified in information systems..., it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information....

The law then proclaims that "the purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy."

We may arrive at the following conclusion from the provisions listed above. Personal information is essential to the efficient operation of both the private and public sectors. But because individual privacy is harmed by the collection, maintenance, and use of that information, it is also essential

to take legislative action to protect privacy against those actions. So the fundamental problem in formulating a privacy protection law is to achieve an adequate compromise between the need for personal information in the public and private sectors and the need to protect individual privacy.

It is from this point of view that we will examine the essential matters that should be covered by a future Privacy Protection Law.

These essentials include the following: the creation of systems of personal records; the operation of those systems; and finally, the enforcement of the privacy protection legislation. We will examine each of these areas in detail after making some necessary preliminary remarks about the character or scope of the law, the categories of the personal records that should be regulated, and the purpose of the law.

B. Some Preliminary Remarks

We must first define the scope and the character of the future Privacy Protection Law. Under this general problem, the initial question to address concerns the categories of the information to be regulated by the Law. Obviously, the scope of application of the Law shall be limited to the personal information, since its purpose is the protection of privacy of individuals. This said, there remains the necessity of defining personal information. This notion may be defined either broadly or narrowly; the latter approach would apply strictly to information concerning the private lives of citizens.

The American Privacy Act of 1974 accepts the broader definition as its basis. This Act states that its purpose is to "provide certain safeguards for an individual against an invasion of personal privacy." It provides thereafter rules applicable to records pertaining to an individual or records of identifiable personal information, without distinguishing whether this information concerns the private or public life of the individual. The German Data Protection Act of 1977 and the French Law on Data Processing, Files and Liberties of 1978 are quite similar in this respect. In our opinion, this approach is appropriate for Korea, for two reasons. First, it is difficult to distinguish private life and public activities. Second, together with that related to private life, the identifiable information related to a subject individual's public activities affects his privacy.

The second problem concerns whether the application of the Law shall

be limited to the automated personal Data Bank (England, West Germany) or be extended to manual personal data also (USA, France). At first glance, the former approach seems appropriate, since the principal object of the recent Privacy Protection Laws has been to protect the individual privacy against the use of computerized personal data. But this approach ignores the harm that misuse of manual personal files may do to personal privacy. Furthermore, if the Law is limited to the automated information, it may encourage public agencies and private enterprises to use manual files as a mechanism for storing "sensitive" personal data. For these reasons, the scope of the Law should be broadened to include manual personal files. Of course, manual personal information may be regulated somewhat differently, in view of its lesser degree of danger to personal privacy. The third problem to be addressed is whether the Law should be limited to the public sector or include the private sector also. The personal data banks maintained by public agencies are more threatening to personal privacy, because collection of the information is in most cases mandatory and the information so collected is widely disseminated through networks linking personal Data Banks of different public agencies. Nevertheless, it is evident that Data Banks operated by private sector can also, as mentioned above, affect or harm an individual's privacy and his chances of obtaining employment, credit, or insurance. In the case of private Data Banks, it is more a question of quantity than of quality. For this reason, we believe that not only the personal Data Banks of public sector but also those of the private sector should be regulated by the Law. This raises the question of whether the two sectors should be regulated by the same law or by separate laws; that is, a law related to public sector, and a law, to private sector, The second approach is favored by the USA, which uses the Fair Credit Reporting Act for private sector Data Banks and the Privacy Act for the public sector. This division in the U.S. code, however, seems to have originated more from circumstance than from logical or legal reasons. We propose therefore that future Privacy Law regulate the Personal Data Banks of both the public and private sectors, with some moderations made in the case of the private sector. As for public sector data storage facilities, there will inevitability arise the question of how to treat personal infomation that bears on national security and the public order. Because of its sensitive character, such data demands special treatment. Some foreign legislation exempts it from the application of the Privacy Protection Law (Privacy

Law, USA). Nevertheless, since this kind of information poses a greater threat to the individual's privacy, it is desirable that it also be regulated by the Law although the regulation may be subject to some moderations. We will address this question more concretely later.

The final question concerns whether the future law should be limited to physical persons or include corporations and other legal entities. This question is related to the intent of the Law. If its purpose is to be limited to the protection of privacy, we believe it adequate to limit the scope of the Law to physical persons. Some argue that the corporation or other legal entity has some rights of privacy, such as the limited right to personality. Even assuming this to be correct, we nevertheless believe it preferable to limit the law to physical persons, the privacy of physical persons, and that of legal entities of a different nature. If one defines the purpose of the Law as the protection of "legitimate interests of the person concerned [schutzwurdige Belagne der Betroffernen]," as in the German Data Protection Law, legal entities shall be included in the scope of application of the future law.

Such definition of the purpose of the Law is worthy of consideration in Korea, which has neither a concrete legal provision protecting privacy nor even one giving its concrete meaning. But because the main concern of the Privacy Law is to protect the individual, his personality, and his private life from the misuse of personal information, we still believe it preferable to limit the scope of the future law to the regulation of personal information of physical persons.

C. Requirements as to the Creation of a System of Records.

The next question is whether the creation of a system of personal records should be submitted to regulation. In this regard, no procedure is provided in either the Fair Credit Reporting Act or the Privacy Act, whereas some formalities are required at this stage in the Swedish Data Act, the French Law on Data Processing, Files and Liberties, the British Data Protection Act, and others. In view of the increasing threat of Personal Data Banks to personal privacy, we believe it preferable to regulate them immediately at the creation stage.

We do not find it necessary, however, that the legal regulation at this

stage be extended to the manual personal file, because the dangers posed by those files to privacy are much smaller than those of automated files. Furthermore, the eventual enforcement agency would be overwhelmed by the workload related to manual files.

We also believe it preferable that the creation of Personal Files in the public sector and that of the private sector be submitted to some different legal regulations, because of the different degrees of danger of those files to privacy.

Based essentially on these considerations, we propose the following procedures to regulate the creation of personal data banks in the public and private sectors. These procedures are largely based upon the pertinent provisions of the French Law on Data Processing, Files and Liberties.

(1) Creation of a personal Data Bank in public sector

The creation of Data Banks in the public sector should be regulated according to the rights involved. If some fundamental human rights are affected by the creation of a Personal Data Bank, it is desirable that it be authorized only through passage of a law. In other cases, approval for the creation should be granted by the minister in charge of the central administration, or by the mayor or the governor in the case of the decentralized entities. But the minister or the mayor shall, prior to decision, request the opinion of the agency charged with enforcing the Law (denominated as the Commission hereafter). The opinion of the Commission shall not be a binding decision, but if it is not favorable to the creation of the Data Bank concerned, the creation may proceed only after deliberation by the Council of Ministers, in the case of the central administration, or by the council of the decentralized entities.

(2) Creation of Personal Data Banks in private sector

For private sector Data Banks, two different methods of regulation are conceivable: the first is to submit the creation to the authorization of the Commission, and the second is to require simply a declaration to the Commission. In the second procedure, the person who is responsible for the projected Data Bank pledges to the Commission that it will conform to the provisions of the Law. The first method is that of the Swedish Data Protection Act, and the second, that of the French Law on Data Processing, Files and Liberties.

Because of the smaller threat that the Data Banks of the private sector represent to privacy, and because of the necessity to assure the sector's

autonomy, we consider the second approach adequate.

(3) Simplified declaration of conformity to the simplified rules

This approach uses a procedure in which the creation of a personal Data Bank whose data clearly do not affect the personal privacy requires only a decleration to the Commission that the projected Data Bank will conform to the simplified rules established by the Commission.

This procedure was established in practice by the Swedish Data Inspection Agency. This Agency found during the brief period that it required authorization that 90% of the personal data was of the usual character (subscription to certain magazines, clients, renters, etc.) and clearly did not affect personal privacy. The agency therefore decided to submit the creation of these categories of personal Data Banks only to the simple declaration of conformity to standard rules.

We believe that this Swedish experience will serve as a good model for Korea's future Law.

In requesting the approval of the Commission, or in making a declaration, the petitioners should list the following items:

(1) the person who is responsible for the creation of the personal data bank;

(2) the characteristics, the purpose, and the name, if any, of the data bank;

(3) the categories of data maintained, their sources, the period of their conservation, and the categories of the users of the data;

(4) the categories of the persons who can gain direct access to the data by virtue of their positions;

(5) all the forms of networks that will link data banks in the future;

(6) the procedures whereby an individual can exercise his right to gain access to information pertaining to him;

(7) the measures taken to ensure the security of the data and to guarantee the secrets protected by the Law;

(8) whether the data are to be disseminated to a foreign country.

In a request for approval of the Commission concerning the creation of Data Banks related to national security, national defense, and the enforcement of criminal laws, some of the items mentioned above may not apply.

We have limited the application of the procedures related to the creation of the Data Banks to cases involving automated data, because the storing of manual personal data holds less danger to privacy. Nevertheless, those

data certainly affect personal privacy. We therefore believe the other rules or requirements of the future Law examined hereafter should be extended to both automated and the manual systems of records.

D. Rules Related to the Collection, Recording, Use and Dissemination of the Information.

1. Rules related to the collection of information.

In data collection, the ideal solution to ensure personal privacy may be to permit only the collection of the personal information directly from the individual concerned; but it is, of course, not a practical solution. None of the actual legislation contains a provision of this kind.

The French Law on Data Processing, Files and Liberties places only the following restrictions on data collection: "It shall be prohibited to collect the personal data by fraudulent, unfair or unlawful means."

The American Privacy Act addresses the matter thus: "Each agency that maintains a system of records shall collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges."

If the information is collected directly from the individual, the collecting agency should reveal to him:

(1) whether the disclosure of such information is mandatory or voluntary;
(2) the effects on him, if any, of not providing all or any part of the requested information;
(3) the ultimate users of the information;
(4) the existence of a right to access and of correction.

2. Rules related to the recording and the conservation of the information.

As to the rules regarding the recording of the information, we will examine only the desirability of prohibiting the recording of some sensitive personal data. Neither the Privacy Act nor the Fair Credit Reporting Act contains any concrete provisions along these lines. The Privacy Act provides only: "Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevent and necessary to accomplish a purpose of the agency required to be accomplished

by statute or by executive order of the President."

On the contrary the French Law on Data Processing, Files and Liberties and the German Data Protection Law prohibit the recording of some personal data. The French Law, for example, prohibits the recording of information related to an individual's racial origin, political or religious opinions, or membership in labor unions, unless the subject individual consents to it expressly. This provision is reported to have the principal purpose to prevent discrimination based on those matters. The law provides two exemptions to this general prohibition:

(1) The press agencies may maintain the information related to those matters under some conditions.

(2) This category of information may also be maintained for public interest (interet public) if the Commission approves it.

In view of the particularly sensitive character of the information related to those matters, we believe the second approach is preferable, although the items of sensitive data may vary according to the country. In Korea, the prohibition of maintaining an information related to racial origin is meaningless; virtually all Koreans are considered to belong to a single race.

As to the operation of system of records of the private sector, an individual should have the right to oppose to the recording of any personal information for rightful reasons. The legitimacy of his reasons may be judged principally by referring to the purpose of the Law.

The Law should prohibit the recording of obsolete personal information; it should also prohibit the retaining of personal information beyond the period specified in the act of request of opinion or in the declaration. This provision is essentially the expression of what the French authors call "right to be forgotten (droit à oubli)." What constitutes "obsolete" information may be specified in the ultimate executive order; the Fair Credit Reporting Act contains some concrete provisions that may serve as good examples.

The person who is responsible for the system of records should take any measures necessary to ensure the security of the records maintained, and especially to prevent them from being damaged deteriorated, or disseminated to a unauthorized third person.

E. Right to Access to Information

It is not easy either to define the notion of the right to privacy. Its essential elements, however, are the right to be left alone and right to control the information pertaining to him. In a modern information society, the second element seems more fundamental, as the individual is exposed to numerous information sources voluntarily and involuntarily.

To ensure the individuals right to access to information pertaining to him, the following conditions must be fulfilled:

(1) Each individual must have the right to be informed at his request whether or not a system of records contains information pertaining to him;

(2) He must be able to gain access to his records and review them;

(3) He must have the right to request the correction of the information pertaining to him which is not correct, relevant, or timely.

Thus the relevant provisions for this section of the future Law should be as follows.

Any person proving his identity shall have the right on his request to an agency that maintains a system of personal records to be notified whether the system contains a record pertaining to him.

He shall have the right to gain access to his records, review them, and request a copy of all or any portion thereof in a form comprehensible to him.

The Commission may authorize the agency that maintain a system of records to deny an individual access to his records if the requests are clearly excessive in number or are too repetative.

The entitled person may request the correction of a record pertaining to him that he believes is not accurate, relevant, timely, or complete. He may also request the deletion of a record pertaining to him, if its collection, use, storage, or dissemination is prohibited by the Law.

In cases of dispute, the burden of proof for the accuracy of the record concerned is imposed upon the agency which maintains the record, except when the information concerned was supplied by the subject individual or with his consent.

A record shall also be amended ex officio by the agency that maintains

a record when the agency becomes aware that it is incomplete or inaccurate.

If information was disseminated to a third person, its amendment or deletion shall be reported to him.

In the case of a system of records related to national security, national defense, or activity of enforcement of criminal laws, requests for access may be made only to the Commission, which will then appoint one of its members to investigate and, if necessary, to amend the information.

The person concerned shall be notified of the measures taken in response to his request.

The American Privacy Act exempts from the application of the law the systems of records of those categories, but we beleive that the Law's framers should take some measures to protect personal privacy even in these fields.

The medical information maintained by an agency shall be released only to the doctor whom the person concerned has appointed for this purpose.

F. Law Enforcement Agency

1. Status and composition

In deciding on an agency to enforce the Law, legislators have several options.

They may choose not to establish any special agency, as in American Privacy Act, which established only a study commission. The law enforcement authority may be an existing agency as in American Fair Credit Reporting Act, which charged the Federal Trade Commission to enforce the act.

In most privacy legislation, a special agency is created by the law solely to enforce it. In its concrete form, the functions and powers of the agency are exercised either by a single person, as in German Data Protection Law, or by a commission, as in Swedish Data Protection Act or French Law on Data Processing, Files and Liberties. In the first case, the status of the person who is responsible of the enforcement of the law may be more of less similar to that of Ombudsman.

As for the future privacy law in Korea, we believe the creation of a special commission is preferable for the following reasons. The complexity of protecting privacy against the dangers of data banks—and especially of automated data banks—requires the expertise of specialists in various fields,

including law, economics, and computer and other technology. The commission is an effective vehicle for providing such expertise. It may also serve to guarantee and enhance the independence of the enforcement agency.

In this regard, the status and composition of the French Commission on Data-processing Liberties are worthy of consideration.

This Commission, "an independent administrative agency," is commposed of 17 members as follows:

—four members of the Parliament, two each elected by the National Assembly and Senate;

—two members of the Economic and Social Council, elected by the Council;

—six members or former members of the supreme judicial authority, including:

(i) two members or ex-members of the Conseil d'Etat;

(ii) two members or ex-members of the Cour de Cassation;

(iii) two members or ex-members of the Cour des Comptes;

—two members appointed by the government for their knowledge and expertise in computer technology, one each nominated by the president of the National Assembly and the president of the Senate;

—three members appointed by the government for their authority and knowledge.

In part, the composition of this commission reflects the outcome of political negotiation and the particular features of political or judicial institutions of France. Nevertheless, it seems desirable to include in the future commission some members of the judicial branch in addition to the specialists in law, economy, ard computer technology.

The idea of including members of the parliament in the commission naturally poses some problems, but one cannot deny its utility, considering that the protection of privacy in this field is a national concern and that their inclusion may guarantee the independence of the future commission. The Swedish Data Inspection Commission includes four parliamentary members each representing a different political party.

The French law provides on the incompatibility of the functions of the members of the Commission with those of the members of the government and with those in private enterprises engaged in production of materials used in data proceeding and telecommunication, etc.

We believe some incompatibility clause should also be included in the future Korean law to ensure the autonomy of the commission. The members of the commission should assume a general obligation not to divulge any information that they have learned by virtue of their position. The commission shall not, however, receive any instruction from the government in exercise of its function.

2. Powers and functions

The powers and functions of the commission should essentially be as follow.

(1) Mission of information

The Commission should publish periodically in its official gazette the list of systems of records, specifying for each system:

(i) the law or administrative act that approves the creation of the system, or the date of acceptance of the declaration;

(ii) the name and the purpose of the system;

(iii) the procedures wherby the right to access can be exercised;

(iv) the categories of recorded personal information and the persons entitled to gain access to the information.

The Commission should also present to the President and the Congress an annual report on its activites. This published report should specify the procedures and the operational methods followed by the Commission.

(2) Function of quasi-authorization

Quasi-authorization is the control function the Commission would exercise before the operation of a system of records in a data bank. We have already described the procedures—that is, request of the Commission's opinion or declaration to the Commission—that should be required before the creation of a system of records. In case of the procedure of a declaration, the Commission may naturally examine the conformity of the system of records projected to the law.

(3) Rule-making powers

The Commission should make internal rules bearing on its own organization and functions. It should make simplified rules that are applicable to a declaration of a creation of a system of personal records of usual character that clearly do not affect the personal privacy.

It should also be able to make standard rules to ensure the security of a system of records.

(4) Control functions

To strengthen enforcement, the Commission should have at least the power to proceed to an on-the-spot inspection of a system of records. It should be able to request presentation of all the documents and information that are necessary to the proper exercise of this mission.

The Commission should be able to send a warning to a person who is reponsible for a system of records in violation of the law, or to denounce him to the public prosecutor.

The Commission would be able to receive petitions or complaints, but it shall not have any judicial power to act on them. In any case, the person who is responsible for a system of records should take any useful measures to facilitate the exerise of the functions of the Commission.

(5) Function of consultation

The Commission should be authorized to issue a consulting opinion at the request of any agency, public or private, and at that of any person. This consulting function is not mandated expressly in most legislation, but, in fact, it is one of the main activities of the enforcement agency of the law. It might serve as a practical means of solving disputes that may arise between an agency that maintains a system of records and an individual; it also helps to prevent tension between the agency and the Commission.