PRIVACY LAWS AFFECTING SYSTEM DESIGN

by

L. J. Hoffman

Memorandum No. UCB/ERL M77-11

8 February 1977

UCB-CS-76-43

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

PRIVACY LAWS AFFECTING SYSTEM DESIGN

Lance J. Hoffman
Computer Science Division
Department of Electrical Engineering
and Computer Sciences
University of California
Berkeley, California 94720
(415) 642-1024

ABSTRACT

An overview of privacy legislation which regulates computer systems is presented. The provisions of the most important legislation to date, the Federal Privacy Act of 1974, are laid out and some early state and local laws are discussed, as are laws covering the private sector. Common features of these laws are extracted. Finally, some methods for keeping track of pending legislation are suggested.

KEYWORDS: privacy, security, legislation, Federal Privacy Act

This work partially supported by National Science Foundation grant number MCS76-09214

The intent of this paper is to give an overview of the existing laws and pending legislation related to the regulation of computer data banks. Many computer systems dealing with personal information are now legally required to take into consideration effects on personal privacy, access rights of subjects, and safeguards against unauthorized access.

The problem of invasion of privacy has been documented in numerous books and articles and there should be no need to rehash to the computer scientist either the general privacy problem or the special problems computers pose. Real, imagined, and feared abuses of computer data banks have led to the passage of the legislation we shall describe below and undoubtedly will lead to the passage of still more legislation.

While concern has been focused in several application areas, notably law enforcement, credit reporting, and statistics gathering, more general regulations seem to be coming into effect as legislators attempt to strike a balance between the privacy rights of individuals and the needs of government and industry for personal information on which to base programs and decisions. To cite just a few of the many works on the topic, the interested reader is referred to [1,3,4,6,8,9,11].

The 1970 words in [5] now seem prophetic: "...if any future system is to win public acceptance, it must offer persuasive evidence that it is quite seriously concerned with the rights and interests of those whose lives it will record."

HISTORICAL PHASES OF PRIVACY AWARENESS AND ACTION

Westin has observed three phases of awareness and action on the privacy/data bank issue [10]: the early warning phase, the study phase, and the regulatory phase.

In the early warning phase, the first alarms are sounded. During the early warning phase in the United States (1966-1970) for example, the controversy over whether or not to establish a National Data Bank for use in statistical work [1] took place.

This is followed by the study phase. Here, government or other commission carry out detailed studies of the problem and propose legislation to curb perceived abuses. In the United States, these studies included the National Academy of Sciences Project on Computer Data Banks [9] and the study of the HEW Secretary's Advisory Commission on Automated Personal Data Systems [6]. This time (1971-1973) was also marked in the United States by increased funding for sociological, political, and technical research into these areas.

Finally, the regulatory phase is entered where the results of all the studies begin to be translated into the law. This is where we are now in the United States (1971-). The laws described later in this chapter promise to be just the beginning of a series designed to protect individual privacy. As such, they represent design constraints on computer systems which technical people must take into consideration, especially since the cost of refurbishing older systems to comply with the laws appears to be significant [2]. But they also represent design opportunities.

LAWS OUTSIDE THE UNITED STATES

Other countries have taken legal approaches which sometimes are similar and sometimes not. The interested reader is encouraged to examine particularly the laws and committee reports in Great Britain, Sweden, France and Germany. In these countries the controls range from administrative self-regulation (i.e., no real controls) to omnibus licensing and regulation [10].

EXISTING LAWS IN THE UNITED STATES

We shall discuss here only the laws and pending legislation in the United States. The reader is cautioned that the author is a computer scientist, not a lawyer. Appropriate legal expertise should be obtained when necessary.

THE FEDERAL PRIVACY ACT OF 1974

By far the most important piece of privacy legislation enacted at this writing is that signed by the President on December 31, 1974, Public Law 93-579. All personal information systems operated by federal agencies are covered, with the exception of most law enforcement files and some personnel records. In addition, nearly all systems operated by federal contractors and grantees are covered if they are operating under contracts or grants signed after September 27, 1975.

While there are certain exceptions, the main provisions of the law are as follows:

1. Individuals (subjects) must be permitted access to information on them in the data banks.
2. Individuals may correct their own records and the agency must investigate each claim promptly. In the case of a disputed record, an individual may insert into the record his or her own perception of the facts.
3. Any individual is allowed to refuse to disclose his or her social security number (applies only to systems which go into operation after January 1, 1975).
4. Individuals must be informed of the effects on themselves, if any, of not providing requested information.
5. A data collecting agency must obtain a subject's consent beforehand, and

must record the date, nature, purpose, and recipient of each "nonroutine" disclosure.

6. Congress and the Office of Management and Budget must be informed before a new records system or a new application goes into operation. Notice must be given in the Federal Register and the public must also be given a chance to object.

7. Every data file must be listed annually by type, general contents, routine uses, and access policies in the Federal Register.

8. Agencies must establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of sensitive records.

9. Agencies must establish "rules of conduct" for "persons involved in the design, development, operation , or maintenance" of any personal records system, together with an education program which will familiarize these persons with the rules and penalties for noncompliance.

10. An agency or contractor employee who willfully discloses or maintains a record in violation of the law, or anyone who requests or obtains a record in violation of the law is guilty of a misdemeanor and subject to a fine of $5000. Civil penalties are provided as well.

11. A Privacy Protection Study Commission established to investigate and recommend further regulations in this area.

STATE AND LOCAL LAWS

The new federal law promises to be supplemented by state and local laws, much like federal air pollution regulations. The National Association of State Information Systems (NASIS)* has developed model state legislation in an attempt to bring some degree of commonality to what otherwise might be fifty widely differing state laws. Highlights of this model legislation, already enacted in some states, are given in Table 1.

---

*Iron Works Pike, Lexington, KY 40505

1. Establishes a register of data banks and their general contents and purposes.
2. Establishes an Information Practices Board to regulate data banks.
3. Requires agencies to inform individuals of the effect, if any, of not furnishing personal information for a data bank.
4. Allows individuals to see the records kept on them.
5. Allows individuals to add their own statements to the records in the case of a dispute between the agency and the individual.

Table 1. Highlights of NASIS Model Legislation.

But already some states and municipalities are in the forefront of legislation to control privacy in computer systems. Minnesota passed the first omnibus law regulating state and local government data banks in April 1974. The highlights of this law are shown in Table 2.

1. Regulates all records kept by state or local government.

2. Mandates a registry of all government data banks on individuals. His registry must specify:

    a. What information is kept and why.

    b. All uses of the information.

    c. Policies and practices regarding data storage, retention, and purge.

    d. Procedures for access and challenge by an individual.

3. Requires "reasonable and appropriate safeguards" to assure that the data is accurate, complete, and correct. Specific emphasis is placed on computer-based files accessed directly via telecommunications.

4. Gives certain rights of subjects in these data banks:

    a. The right to know the purpose of the intended use of the required data.

    b. The right to know whether supplying data is mandatory or not and the consequences of refusal to supply the data.

    c. The right to know whether he or she is a subject in a given data bank.

    d. The right to know the content and meaning of the data on himself or herself at no charge.

5. Any person who is damaged can sue the state for damages. Exemplary damages are also recoverable in the case of willful violations. Willful violation is a misdemeanor.

Table 2. Highlights of the 1974 Minnesota Privacy Law (H.F. No. 1316, Chapter No. 479)

Participants from 40 states agreed at a seminar cosponsored by the Council of State Governments and the Domestic Council Committee on the Right to Privacy in December 1974 that local governments also have a role to play. Indeed, some have already started to play this role. In 1974 the city of Berkeley, California, decided to require a "social impact statement" for all municipally funded or controlled automated personal information systems. The provisions of the Berkeley ordinance are summarized in Table 3.

---

1. Deals with all systems controlled or funded by the city.
2. Allows only planning until a social impact statement is written.
3. The social impact statement must address:
   a. impact of the system on members of the public
   b. any adverse effects on privacy
   c. any adverse effects on acquisition or retention of credit, employment, or insurance
   d. alternatives to proposed system or system addition; these must include the alternative of doing nothing, and its impact.
4. Social impact statement (or summary) must be published in local newspaper.
5. Social impact statement must be sent to each member of city council.
6. Social impact statement must be sent to every person or organization with a standing request on file.
7. A public hearing must be held on the social impact statement.
8. Significant changes or additions to the system after approval of the social impact statement require an additional social impact statement.

Table 3. Highlights of Berkeley Social Impact Statement (Ordinance No. 4732-N.S.)

This last is particularly interesting because the impact statement was actually mentioned by then Vice-President Gerald Ford in a speech to the National Computer Conference of 1974. A month later, one of his principal advisors, Philip Buchen, suggested in a speech to the Data Processing Management Association that even legislation which fails "may very well signal what you as managers of information systems can expect in future years" if the privacy problems addressed by these bills are not otherwise overcome. According to Computerworld of July 3, 1974, he also stated that legislation currently intended for the public sector "may set patterns for the eventual treatment by law of information systems in the private sector."

LAWS AFFECTING THE PRIVATE SECTOR

The first of these private sector laws has already appeared. It is the 1971 Fair Credit Reporting Act (Public Law 91-508) which regulates credit bureaus and similar organizations. Basically, it requires that consumers be allowed to see their own records, to contest them, and to file a 100-word statement as part of the record in the case of a disputed item.

OMNIBUS FEDERAL LEGISLATION FOR BOTH PUBLIC AND PRIVATE SECTORS

A new bill was introduced in Congress in early 1975. With the well-chosen number H. R. 1984, it covers every public and private manual and automated personal information system except government-maintained criminal information systems, news agency files, and mailing lists--provided the organization maintaining the mailing list voluntarily removes an individual's name upon request.

This bill establishes a federal privacy board of five public members which can inspect the premises of any data processing facility. This board would be required to be informed three months in advance by any organization planning to use a new system containing personal data or planning to modify an existing one.

As with the FCRA, any subject of a data bank would be allowed to file a rebuttal (in this case, up to 200 words) of the information in the data bank which would then have to be included in subsequent reports. Past recipients of records would be required to be notified any time the record is corrected or purged.

Each operator of a system would be required to, within two years of the bill's enactment, tell every individual whose record is on file what information the record contains.

The social security number would be not required for any business transaction or other activity except as required by federal law. And without "the express authorization of Congress, no organization can develop or utilize a universal identifier common to any other personal information system."

COMMON FEATURES OF UNITED STATES LEGISLATION

Having discussed existing and pending legislation in the United States, can we extract any common elements? If, as seems likely, this type of legislation will soon cover most public and private computer systems containing personal information, the system designer should attempt to incorporate the most common features of the legislation into the design of new systems at the start to avoid painful retrofits later. Some of these common features are shown in Table 4.

1. Individuals are permitted to see and challenge information kept on them and to file dissenting statements. These statements must be incorporated as part of the record or at least sent out with it.
2. Security and accuracy safeguards are mandated.
3. Disclosure restrictions are institutionalized.
4. Social Security Number cannot be required in new systems.
5. Logging of nonroutine disclosures is required.
6. Impact statement or filing of Intent to Operate statement is required for new systems or significant additions or modifications of old ones.
7. Criminal and civil penalties for willful violation are provided.

Table 4. Common Features of Current Legislation.

Provisions for handling these common features should certainly be designed into new systems. The system designer may also wish to provide some of the other privacy and security features mentioned above in anticipation of future legislation.

Legal requirements will have technological ramifications. Special printouts, data fields, personnel, procedures, and logs may be necessary to comply with new laws [7].

KEEPING TRACK OF PENDING LEGISLATION

There are other federal, state, and local bills pending as well--too numerous to discuss here. By the time this is printed, much of the legislative features described as "pending" in this paper may well be the law. Good systems design involves being aware of these trends and taking them into account before they become realities. How can one keep abreast of current developments in the legislative domain?

At this writing, here are some methods to track pending legislation and its status:

1. The Computer Business and Equipment Manufacturers Association puts out a monthly status list of legislation concerned with computer privacy and security (CBEMA, 1828 L Street N. W., Washington, D. C. 20036).
2. The Privacy Report and Privacy Journal track privacy issues from a civil liberties viewpoint. The Report is issued by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation, 22 East 40 Street, New York, N. Y. 10016. Subscriptions are $15 per year ($5 for students) for 12 monthly issues. The Journal is independent. Subscriptions are $15 per year from P.O. Box 8844, Washington, D. C. 20003.
3. Computerworld, the trade weekly, has timely coverage of computer privacy issues (Computerworld, 797 Washington St., Newton, Mass. 02160, $15 per year for 51 issues).

SUMMARY

This paper has presented an overview of current and proposed legal constraints on data banks. It pointed out that the United States has moved through the early warning and study phases to the regulatory phase, and set forth in detail the provisions of the most important legislation to date, the Federal Privacy Act of 1974. State and local laws and laws covering the private sector are becoming more numerous, and some of the early ones were discussed. Common features of nearly all the laws include a) an individual's right to challenge records and to file dissenting statements; b) prohibition against using the Social Security number; c) logging of nonroutine disclosures; d) impact statement or intent to operate statement filing; e) criminal and civil penalties for willful violation. Finally, some methods of tracking pending legislation were suggested.

ACKNOWLEDGMENT

I wish to thank Dr. Rein Turn for his useful suggestions on how to improve an earlier draft of this paper.

BIBLIOGRAPHY

1. Dunn, Edgar S. Jr., "The Idea of a National Data Center and the Issue of Personal Privacy", American Statistician, 21, (Feb. 1967), pp. 21-27.

2. Goldstein, Robert C. and Nolan, Richard L., "Personal Privacy vs. the Corporate Computer", Harvard Business Review, March/April 1975, pp. 62-70.

3. Hoffman, Lance J., "Computers and Privacy: A Survey", Computing Surveys, 1, 2 (June 1969), pp. 85-103.

4. Miller, Arthur, The Assault on Privacy, University of Michigan Press, 1971.

5. Project SEARCH, "Security and Privacy Considerations in Criminal History Information Systems", Technical Report No. 2, July 1970, Project SEARCH, Sacramento, Ca.

6. "Records, Computers, and the Rights of Citizens", Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U. S. Department of Health, Education and Welfare, July 1973, U. S. Government Printing Office Bookstore Stock No. 1700-00116.

7. Turn, R., "Privacy and Security in Personal Information Databank Systems", RAND Corporation Document R-1044-NSF, March 1974.

8. U. S. Senate Committee on Government Operations, Report No. 93-1183, "Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information".

9. Westin, A. F. and Baker, M. A., Databanks in a Free Society, Quandrangle Books, New York, 1972.

10. Westin, Alan F.; Lufkin, Daniel; and Martin, David B. H., The Impact of Computer-Based Information Systems on Citizen Liberties in the Advanced Industrial Nations. A report for the German Marshall Fund of the U. S., Washington, D. C., 1973.

11. "Whose Right to Know" and "What Every Executive Should Know about Privacy in Information Systems", Videotapes on privacy and security with a "Session Leader's Guide", IBM Document G320-1379.