UNIVERSITY OF MINNESOTA
TWIN CITIES

School of Management
271 19th Avenue South
Minneapolis, Minnesota 55455

December 8, 1981

Senator Robert J. Tennessen, Chairman
Senate Commerce Committee
309 State Capitol
St. Paul, MN 55155

Dear Bob,

As I mentioned to you over the phone, enclosed is a copy of a recently completed report entitled, "Two Approaches to Data Privacy Legislation: The Minnesota Government Data Practices Act and the Uniform Information Practices Code". Please arrange to have a copy bound and placed in the Legislative Library. Also notify any others in our legislature who would have an interest in the results of the study.

The main purpose of the report was to provide a side-by-side, provision-by-provision compairson of the Minnesota Statues and the proposed Uniform Code. In addition, the report makes several observations and comments about each, including their relative strenghts and weaknesses.

It is our hope that this will be useful in preparing legislation for the 1982 session to consider in amending our own Minnesota statute.

Don't hesitate to call if you or your researchers have any questions or would like to talk about this further. I hope I can get to some of the subcommittee hearings this coming year.

Yours truly,

Gordon Everest
Professor, Management Sciences

cc: Senator John Keefe
Senator Gene Merriem
Senator Randolph Peterson

GCF:KAW
Enclosure

P.S. Please be sure I'm on your notification list.

TWO APPROACHES TO DATA PRIVACY LEGISLATION: THE MINNESOTA GOVERNMENT DATA PRACTICES ACT AND THE UNIFORM INFORMATION PRACTICES CODE

by

Gordon C. Everest
Associate Professor

Joanne Tsuyuko Kamo

School of Management
UNIVERSITY OF MINNESOTA

1981 August

Table of Contents - continued

TABLE OF CONTENTS

TABLES

CHAPTER 1

INTRODUCTION

The concept of data privacy focuses on the claim that individuals have in determining the extent to which personal information is used, for what purposes, and to whom the information shall be disclosed. Unauthorized and inadvertent disclosures of personal information intrude upon the individual's privacy--possibly causing irreparable damage. An intensified interest in data privacy has perhaps been spurred with the increasing use of the computer, even though data privacy issues exist with manual record keeping systems as well. A tool which enables vast amounts of data to be collected, stored, manipulated, and disseminated quickly and to remote locations, the computer introduces invaluable verifying, editing, monitoring, and security features which were previously never available to record keeping systems. It is only when people mishandle the data that data privacy abuses occur.

Minnesota has been a pioneer in adopting data privacy legislation. It first passed its privacy law in 1974. Popularly called the "Data Privacy Act," this was an omnibus bill aimed at state and local government agencies. Since 1979, this Act

has been officially entitled the "Minnesota Government Data Practices Act." The provisions in the Act are extremely controversial and complex, which is the reason why the Act has been amended every year since its inception.

The Uniform Information Practices Code is the motivating source of this research. Approved by members of the National Conference of Commissioners on Uniform State Laws at its annual conference in 1980, this Code was drafted with the purpose of establishing uniform legislation which could be adopted by all 50 states. It offers an alternative for state governments, along with other benefits which accompany uniformity. However, approximately 25 states have already implemented their own laws with regard to information practices,[1] and Minnesota was the first state to enact data privacy legislation. Thus, the question arises as to whether Minnesota should replace its data privacy statutes in whole or in part with the Uniform Information Practices Code.

1.1 UNDERLYING PURPOSE OF THIS STUDY

There is a paucity of research on privacy legislation at the state level of government. Although information can readily be obtained on federal acts, such as the Privacy Act or the Freedom of Information Act, there are very few guidelines that legislators can use in deciding upon state privacy legislation.

This research provides a basis for drafting amendments to the Minnesota Statutes, or a new statute which takes the best of both the Minnesota Statutes and the Uniform Code, and is acceptable to Minnesota. For those outside the state of Minnesota, it provides a substantive resource from which to begin drafting their own proposed statute.

1.2 OBJECTIVES OF THIS STUDY

A resource is needed to enable legislators to see the similarities and differences between the Minnesota Government Data Practices Act and the Uniform Information Practices Code. Therefore, the primary objective of this research is to provide legislators with a direct provision-by-provision comparison of the Minnesota Statutes and the Uniform Code. A direct comparison of the actual texts of each act will provide valuable insights into the strengths and weaknesses of each act. Those provisions that are comprehensive, and those that are lacking will become evident. Although comments are made throughout the comparison, the actual text comparison alone will serve as a tool to all legislators in deciding upon and formulating data privacy legislation.

1.2 SCOPE OF RESEARCH

This research is limited to a comprehensive, comparative study and analysis of the books, articles, and legal documents that have been published on data privacy and privacy in general. The Minnesota Statutes and the Uniform Information Practices Code are the two documents central to this study. It must be emphasized that both works are at the state (and not federal) level of government. Surveys or extensive interviews were not undertaken because these methods would not be as effective or helpful to legislators in achieving the objectives of this research as would an actual text comparison.

1.3 DEFINITIONS, CLARIFICATION OF TERMS USED THROUGHOUT THIS RESEARCH

1. The "acts" is the term used when referring to both the Minnesota Government Data Practices Act and the Uniform Information Practices Code simultaneously.

2. The "Minnesota Government Data Practices Act" refers to M.S. 15.1611 through 15.1698, hereinafter referred to as "the Minnesota Act." Amendments to the Statutes made in May, 1981 will alter the Statute numbers, but the Act in its entirely amended form is currently unavailable. (For the amendments see S.F. No. 470, Chapter No. 311.)

3. The "Uniform Information Practices Code" is hereinafter referred to as "the Uniform Code."

1.4 REPORT FORMAT

Background information on each act, such as history, current status, and major provisions will serve the purpose of re-acquainting one with each act. This will be followed by the main body of this research, Chapter 4, which is the direct provision-by-provision comparison of the texts of each act. Each major section of Chapter 4 contains a summary of the particular section. Afterward, a summary of the strengths and weaknesses of each act will ensue in order that recommendations and conclusions can be made.

CHAPTER 2

BACKGROUND OF THE MINNESOTA ACT

Minnesota's early involvement in state privacy legislation can be traced back to 1973 when representative John Lindstrom introduced the first data privacy bill to the Minnesota House of Representatives. The bill was passed by the House at that time; and it was afterwards submitted to the Senate. During the interim period from 1973-74, the Data Security and Privacy Subcommittee of the intergovernmental information systems advisory council reworked the bill. Meanwhile, Senator Robert J. Tennessen held a series of privacy hearings in the fall of 1973 which, along with the reknown HEW Report,[2] formed the basis for 3 different bills introduced in the 1974 legislative session. Lindstrom's reworked bill and Tennessen's bills were combined--resulting in Minnesota's becoming the first state to enact privacy legislation.[3]

Various subcommittees and commissions have contributed to the privacy effort. The Data Security and Privacy Subcommittees (mentioned above) became defunct in 1975 when an amendment to the Minnesota Privacy Statutes created a Legislative Privacy

Sutdy Commission. This group was authorized to examine issues involving data privacy and submit reports containing recommendations to improve privacy legislation to the Minnesota legislature. It carried out these duties until January 15, 1977.

Moreover, the Data Privacy Division (originally called the "Data Privacy Unit") of the Minnesota Department of Administration presently carries out the functions expressly authorized the Commissioner of the Department of Administration in the Minnesota Statutes. This includes rulemaking and approvals, although it also functions in an advisory capacity to inquiring citizens and agencies.

The Minnesota Government Data Practices Act has been amended every year since its inception in 1974. Amendments approved for 1981 primarily focus on the addition of specific categories of information for various agencies or changes to currently existing definitions.

2.1 OVERVIEW OF THE MAJOR PROVISIONS OF THE MINNESOTA ACT

The Minnesota Act applies to all state agencies, political subdivisions, or statewide systems in the state of Minnesota in their practices of handling government data. (See sections 4.2.3 and 4.3.1) On a conceptual level, the Act consists of two major sections: (1) the omnibus portion of the legislation which has general applicability to all agencies of the state; and (2) the various categories of information, which declare classifications of data other than public data, along with the agencies and persons affected, and the circumstances under which they are affected.

Contained in the omnibus portion of the Act are the following major provisions:

1. General Classifications of Government Data.
2. Access to Government Data.
3. Duties of Responsible Authorities.
4. Rights of Subjects of Data.
5. Legal Remedies.

All government data is classified as either data on individuals or data not on individuals. Data on individuals means "all government data in which any individual is or can be identified..."[4] It is further subdivided into public, private, and confidential data. If the data is not data on individuals, then it is called data not on

individuals, and its 3 subdivisions are public, nonpublic, and protected nonpublic data. (See Figure 1.)

Each classification of data has rules regarding who can access the data, but not completely. For instance, if the data is private, it is not public; and although it can be accessed by the individual to whom the data pertains, it is not clear as to the other individuals or persons who can also access the data. The thrust of this classification scheme is to limit accessibility to data as its classification becomes more personal. Confidential data, for instance, is inaccessible to the individual subject of that data. Again, though, the definition does not say to whom the data is accessible even though it is inaccessible to the individual data subject. By limiting the accessibility to data, it is believed that abuses to personal privacy can be reduced.

The second provision declares that all government data is public data, whether it be public data on individuals or public data not on individuals. Of course, it would be to the individual's best interest to classify all data as private; but this would not be fair to the public interest in accessing the data. Because public access to all government data is desired, the second provision provides for this. Hence, if any other classification of data is desired, an application to change it must be submitted by the responsible authority to the commissioner.

Who is the responsible authority? He or she is an actual person in each governmental agency that is responsible for implementing and administering the provisions of each Act. For example, he is responsible for reporting to the

individuals, and its 3 subdivisions are public, nonpublic, and protected nonpublic data. (See Figure 1.)

Each classification of data has rules regarding who can access the data. For instance, if the data is private, it is not public; and it can only be accessed by the individual to whom the data pertains. The thrust of this classification scheme is to limit accessibility to data as its classification becomes more personal. Confidential data, for instance, is inaccessible to the individual subject of that data. By limiting the accessibility to data, it is believed that abuses to personal privacy can be alleviated.

The second provision declares that all government data is public data, whether it be public data on individuals or public data not on individuals. Of course, it would be to the individual's best interest to classify all data as private; but this would not be fair to the public interest in accessing the data. Because public access to all government data is desired, the second provision provides for this. Hence, if any other classification of data is desired, an application to change it must be submitted by the responsible authority.

Who is the responsible authority? The responsible authority is an actual person in each governmental agency that is responsible for implementing and administering the provisions of the Act. For example, he is responsible for reporting to the

commissioner, overseeing the collection, storage, security, and dissemination of data, establishing procedures, applying for changes to the classification of data, and more. This person is the agency's focal point with regard to the Act.

The fourth provision, Rights of the Subjects of Data, accords rights to individuals who provide information to the agency. An individual must be assured of rights when data is collected from him. For instance, the individual must be informed of the intended purpose and use of the requested data, the consequences arising from his supplying the data, and so forth. Rights are granted to the individual to find out what data an agency maintains on the individual. Also, the accuracy or completeness of the public or private data on the individual may be contested.

Lastly, civil remedies are stated in the final major provision of the omnibus portion of the Act. An aggrieved individual may contest an agency's compliance with the Act, or the agency's practice of disclosure or nondisclosure of information.

The other portion of the Act is a listing of the various categories of information which describe the exceptions to the rule, which classifies all data as public. These categories have been established via the responsible authority submitting an application for temporary classification to the commissioner. If approved, these categories describe the data being classified as either private, confidential, nonpublic, or protected nonpublic. Other sections of the Minnesota Statutes also classify specific types of data.

CHAPTER 3

BACKGROUND OF THE UNIFORM CODE

The Uniform Information Practices Code has been refined through much effort on the part of the National Conference of Commissioners on Uniform State Laws (the "Conference") and many others. In 1977 a Special Committee on Uniform Privacy Act was created to determine whether there was a need for the Conference to begin drafting a Uniform Privacy Act. Their findings indeed revealed inconsistent and non-comprehensive state law, so it was decided to proceed with the drafting of the Act. At its 1980 annual conference, the Uniform Information Practices Code was approved and recommended for enactment in all the states.

In comparing the Minnesota Act with the Uniform Code, one must keep the time lapse differential in mind. In other words, it must be emphasized that the Minnesota Government Data Practices Act was enacted in 1974, and Minnesota was the first state ever to adopt such legislation. Conversely, work on the Uniform Code can be traced

back to 1977. By that time, other states had already introduced or adopted their own data privacy legislation. Thus, the drafters of the Code were advantageously able to build a foundation for privacy legislation utilizing knowledge of the weaknesses and strengths of other states' legislation. One can tell just from reading the two documents that quite a few of the provisions appear to be unusually similar in terms of content and wording.

The Uniform Code is lengthier than the Minnesota Act, but part of this can be attributed to comments which are freely interspersed throughout the Code. These comments reveal the drafters' intent with regard to the stated provisions. They contain cites to other cases or documents to justify their intentions, or they further serve to clarify or provide examples for the provisions.

The Uniform Information Practices Code was submitted to the House of Delegates of the American Bar Association in February, 1981 to be considered for endorsement. However, there was insufficient time to discuss it, and it is not known if it will be resubmitted.[5] In some cases the American Bar Association's approval might increase the Code's chances for passage by the states, but the true test of acceptance is in the state legislatures.

3.1 OVERVIEW OF MAJOR PROVISIONS OF THE UNIFORM CODE

Unlike the Minnesota Statutes, the Uniform Code was drafted with the intention of enacting it in all 50 states. It is applicable to all state agencies of the executive branch of government; and it excludes the legislative and judicial branches of government. The term, "government record," is used in lieu of the Minnesota term, government data, to refer to the data relevant to the Code. (See sections 4.2.3 and 4.3.1.)

Four underlying principles of the Code are expressly stated as follows:

"(1) to enhance governmental accountability through a general policy of access to government records;

(2) to make government accountable to individuals in the collection, use, and dissemination of information relating to them;

(3) to protect individual privacy and related interests whenever the public interest in disclosure does not outweigh those interests; and

(4) to make uniform the law with respect to the subject matter of this Code among states enacting it."[6]

These principles are embodied throughout the 5 major provisions of the Code by means of a delicate system of checks and balances.

Thus far, Minnesota has been the only state to introduce the Uniform Code to the legislature, but it has been met with fierce opposition from certain sectors. The two major criticisms of the Uniform Code are that: (1) too much discretionary power is given to a government agency; and (2) data used for law enforcement purposes is treated too favorably. Hence, no action has been taken to enact the Uniform Code in Minnesota. Rather, many amendments to the Minnesota Act have been made by the state legislature in 1981.

The Code's first article states the purposes of the Code, and defines all terms used throughout. Information which refers to individuals is referred to as "personal records," and it is a general term that is used whenever any agency maintains information about individuals.

If a personal record reveals, or can readily be associated with the identity of the individuals, then it is an individually identifiable record. This type of record becomes the focus of Article 3, which deals specifically with individually identifiable records. Personal records may also be described in terms of their accessibility, which is pertinent to the provisions relating to record retrievability. However, not all personal records are individually identifiable records or accessible records.

Article 2 declares that all government records are available for public inspection in an overall policy of freedom of information. In the Minnesota Act, all information that is classified as public is accessible, but the Code does not have this sort of classification system. Instead, the agency head may refuse to disclose records to the public if it is felt that the reasons for nondisclosure outweigh the public benefit derived from accessing the records. This authority to make a discretionary judgment is held in check by a provision which says that the head of the agency must be ready to justify why a particular record has been withheld from public access.

In like manner, the third article declares that the head of the agency has the authority to disclose an individually identifiable record to a person other than the individual to whom the record refers if the benefit derived from disclosing the information outweighs the individual's privacy interests. Moreover, an individually identifiable record can be withheld from the individual to whom it refers, but the responsible authority is once more responsible for his decision.

The fourth article establishes an Office of Information Practices; and it appoints a director of the Office of Information Practices to carry out specific, designated tasks. In effect, this Office is an entity which oversees the carrying out of the provisions of the Code. It is a built-in control mechanism because it has the power to recommend the taking of disciplinary action; or the taking of steps to instigate criminal prosecution procedures against the affected agencies. Also, it provides a second resource for individuals, which would result in improved quality of public access to information and protection of individual privacy rights.

Finally, the last major provision allows certain agencies to be exempted from some of the provisions of the Code. Either the Governor or the Office of Information Practices is granted the authority to decide whether an agency qualifies for exemption.

4.1 RULES FOR READING CHAPTER 4

1. A summary precedes the text of each major section except for section 4.13.
2. Provisions and comments for the Minnesota Statutes are always on the left half of each page; provisions and comments for the Uniform Code are always on the right half of the page.
3. Section numbers are assigned to the Minnesota Statutes (e.g., 15.162, 15.1621). However, official section numbers have not been assigned to the 1981 amendments yet. In these cases, the word, "Section," is spelled out.
4. Comments: A personal comment is enclosed in asterisks and brackets (i.e., [*comment*]). A comment directly after (beneath) a clause on the same half of the page refers to that particular clause.

   The comments taken directly from the Uniform Code are enclosed in asterisks and brackets, and always begin with, "COMMENT..."
5. REPEATed provisions are indicated, and a cite is given to refer to another section where it can be found.

4.2 PURPOSE, SCOPE

From the onset it must be realized that the comparison of the Minnesota Statutes with the Uniform Information Practices Code is not equally balanced. In the drafting stages, the Statutes were intended to formulate privacy legislation only for the state of Minnesota. The intent of the Uniform Code was to draft legislation to be adopted by all 50 states. Thus, it might be expected that the Uniform Code would be more comprehensive--particularly with regard to inter-state data handling practices.

However, both the Minnesota Act and the Uniform Code must in some way formulate underlying principles to regulate agency handling of data. The Minnesota Statutes should explicitly state the purpose(s) of the Act. A stated purpose(s) would serve as a guideline in evaluating present and future data privacy legislation. It would also provide cohesiveness to the Act, which is currently lacking.

The scope of the entities regulated by the Minnesota Act is quite comprehensive. As one can see, the definitions of state agency, political subdivision, and statewide system embody all entities of state government. On the other hand, the current provisions of the Uniform Code exempt the judicial and legislative branches of government from all provisions of the Code. In a way, this defeats the purpose of the Uniform Code because the exemption of these 2 branches of government would illustrate

CHAPTER 4

PROVISION-BY-PROVISION COMPARISON OF THE MINNESOTA ACT AND THE UNIFORM CODE

Unquestionably the lengthiest but most substantive chapter; the reader is urged to read the actual text comparisons in order to compare the distinct differences and the very subtle differences between the two acts. The sections have been organized to assist in comprehending similar and different provisions of the acts.

CONTENTS OF CHAPTER 4 - continued

CONTENTS OF CHAPTER 4 - continued

CONTENTS OF CHAPTER 4 - continued

CONTENTS OF CHAPTER 4 - continued

Section

Page

4.15 continued

that there is a double standard with regard to protecting individual privacy interests. All branches of government must be accountable for their data handling practices because abuses can occur in any branch of government that handles personal records. Also, the Uniform Code can be applied to the private sector.

Both the Minnesota Act and the Uniform Code naturally define an individual and a person in order to formulate policy with regard to agency interaction with the individual or person. Inter-agency and inter-state provisions permit the agency to disclose information, with restrictions. Intra-agency disclosures are mentioned within the categories of information listed in the Minnesota Act. The Uniform Code permits intra-agency disclosures, although it is not dealt with in any provision of the Code.

Lastly, the Minnesota Act does not provide for foreign disclosures of data. It only prohibits the dissemination of data to Interpol. The Uniform Code has one clause concerning foreign disclosures.

15.1611 GOVERNMENT DATA.
Subd. 2.
Sections 15.1611 to 15.1699 may be cited as the "Minnesota government data practices act."

Subdivision 1.
All state agencies, political subdivisions and statewide systems shall be governed by sections 15.1611 to 15.1699.

UNIFORM INFORMATION PRACTICES CODE

Article 1

General Provisions and Definitions

SECTION 1-101 (Short Title.)

This Act may be cited as the Uniform Information Practices Code.

[* All agencies of the executive branch of government are governed by the provisions of the Uniform Code. *]

4.2.2 Uniform Code: Purposes; Rules of Construction
4.2.2.1 Purposes; rules of construction

[* It is imperative that a purpose for the Government Data Practices Act be explicitly stated so that current and future amendments will be related to the purpose(s). *]

SECTION 1-102 (Purposes; Rules of Construction.)

This Code shall be applied and construed to promote its underlying purposes and policies, which are:

(1) to enhance governmental accountability through a general policy of access to governmental records;

(2) to make government accountable to individuals in the collection, use, and dissemination of information relating to them;

(3) to protect individual privacy and related interests whenever the public interest in disclosure does not outweigh those interests; and

(4) to make uniform the law with respect to the subject matter of this Code among states enacting it.

[* This has already occurred in the Minnesota Statutes through amendments. *]

SECTION 1-103 (Severability.)

If any provision of this Code or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of the Code which can be given effect without the invalid provision or application, and to this end the provisions of this Code are severable.

4.2.3 Scope
4.2.3.1 The data applicable to the act or the code

15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.
Subd. 11.
"Government data" means all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use.

[* See section 4.3.1.1. *]

[* In Ambrose Kottschade v. Gerald Lundberg, a Minnesota Attorney General determined that:
" The work sheets, commonly referred to as 'field cards,' on which an assessor in the field records his comments or observations with respect to each piece of property which he assesses, are not 'public records' within the meaning of Minn. St. 15.17, subd. 4, which requires that public records be made available for inspection by any member of the public... Any casual jotting, any tear-sheet observation, which discloses the promptings of official action, is to some extent 'necessary to a full and accurate knowledge of * * * official activities.' But it appears to us that the legislature did not intend anything that sweeping. Such a broad definition of public records would fill official archives to overflowing..." 7 *]

(3) "Government record" means information maintained by an agency in written, aural, visual, electronic or other physical form.

[* See section 4.3.1.1. *]

[* COMMENT in Uniform Code following section 1-105, page 5.
It includes all information maintained by an "agency" as long as the information exists in some physical form. For example, the personal recollection of an agency employee would not be a "government record" but his handwritten notes summarizing an event or conversation would. This definition triggers the general public right of access to information established in sections 2-101 and 2-102. *]

4.2.2.3 Construction against implied repeal

SECTION 1-104 (Construction Against Implied Repeal.)

This Code is a general act intended as a unified coverage of its subject matter and no provision of it is impliedly repealed by subsequent legislation if that construction can reasonably be avoided.

15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.

Subd. 7.

"State agency" means the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state.

Subd. 5.

"Political subdivision" means any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision. It includes any nonprofit corporation which is a community action agency organized pursuant to the economic opportunity act of 1964 (P.L. 88-452) as amended, to qualify for public funds, or any nonprofit social service agency which performs services under contract to any political subdivision, statewide system or state agency, to the extent that the nonprofit social service agency or nonprofit corporation collects, stored, disseminates, and uses data on individuals because of a contractual relationship with state agencies, political subdivisions or statewide systems.

Subd. 8.

"Statewide system" includes any recordkeeping system in which government data is collected, stored, disseminated and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

SECTION 1-105 (General Definitions.)

(2) "Agency" means a unit of government in this State, any political subdivision or combination of subdivisions, a department, institution, board, commission, district, council, bureau, office, officer, official, governing authority or other instrumentality of state or local government, or a corporation or other establishment owned, operated, or managed by or on behalf of this State or any political subdivision, but does not include the (name of legislative body) or the courts of this State.

[* COMMENT following SECTION 1-105, p. 5.

Not included within the definition of "agency" are the legislature and the courts of a state. Although not found persuasive in some jurisdictions, see, e.g., Conn. Gen. Stat. Ann. § 1-18a; Tex. Pub. Off. Code Ann. tit. 110A, § 6252-17a, the rationale for these exceptions is threefold: (1) the executive branch is by far the major recordkeeper in state government and has been chiefly responsible for excessive governmental secrecy and abuses in the collection, use and dissemination of personal records; (2) potential separation of powers issues would arise if the requirement of this Code were extended to the the judiciary and to records held or controlled by legislators; and (3) the legislative and judicial branches are held to a high level of public accountability through other means such as the electoral process and appellate review. *]

4.2.3.2 The bodies or entities regulated by the act or the code

15.1611 GOVERNMENT DATA.
Subd. 2.
Sections 15.1611 to 15.1699 may be cited as the "Minnesota government data practices act."
Subd. 1.
All state agencies, political subdivisions and statewide systems shall be governed by sections 15.1611 to 15.1699.

[* REPEAT. See section 4.2.1. *]

[* In Minneapolis Star and Tribune Company v. State and Others, a Minnesota Attorney General determined that the: "Board of Medical Examiners are not 'officers' of the state, and the Board is not an 'agency of the state.' Therefore, minutes of their meetings are not subject to indiscriminate public inspection in the absence of some special interest which confers standing." 8 *]

[* It is stated on page i. of Prefatory Note that, "The Code related to recorded information which is collected and maintained by state or local government," but is not explicitly stated in the text of the Code. *]

[* Also on page iii. of Prefatory Note: "...Records maintained by the private sector (e.g., insurance, credit, banking) could also be included." *]

[* Thus, since the private sector can be included, the scope of the entities regulated can be broader. Also will apply to all agencies of states that adopt the Code. *]

[* "Agency" in the Code is intended to be all-inclusive. The big difference is that the legislative and judicial branches are exempted from the Code. One of the purposes of the Code is to protect individual privacy interests when they are not outweighed by the public interest in disclosure. To the extent that the legislative and judicial branches also maintain personal records, abuses to an individual's privacy can still occur. Thus, these 2 branches must also be liable for their handling of data under this Code. *]

15.162 continued

[* Very comprehensive definitions. Emphasizes the exclusion of no agency or branch of government. Also see section 4.3. *]

SECTION 1-105 continued

[* Disagree with the above. All record keeping systems which keep records on individuals must be held accountable for their actions. *]

4.2.3.4 The entities which access the data and to which disclosures are made

INDIVIDUALS, PERSONS

15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.
Subd. 4.

"Individual" means a natural person. In the case of a minor, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian, except that the responsible authority shall withhold data from parents or guardians, or individuals acting as parents or guardians in the absence of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor.

Subd. 12.

"Person" means any individual, partnership, corporation, association, business trust, or a legal representative of an organization.

SECTION 1-105 (General Definitions.)
(4) "Individual" means a natural person.

[* Provisions are made for minors in SECTION 3-106(b). See section 4.4.4. *]

(7) "Person" means individual, corporation, government or governmental subdivision or agency, business trust, estate, trust, partnership, association, or any other legal entity.

4.2.3.3 The geographical area where the act or code is to be enacted

[* Only pertains to the state of Minnesota. *]

SECTION 1-102 (Purposes; Rules of Construction.)
(4) to make uniform the law with respect to the subject matter of this Code among states enacting it.

[* REPEAT. See section 4.2.2.1. *]

[* A major purpose of the National Conference of Commissioners on Uniform State Laws is to draft acts to be enacted in all 50 states. *]

FOREIGN GOVERNMENTS

15.1643 INTERNATIONAL DISSEMINATION PROHIBITED.

No state agency or political subdivision shall transfer or disseminate any private or confidential data on individuals to the private international organization known as Interpol.

[* The above is the only clause relating to international disclosures. It is a prohibition and does not really deal with disclosures to other foreign governments. Therefore, it is assumed that the scope of this Act does not cover disclosures to foreign governments. *]

SECTION 3-103 (Disclosure to Agencies or Government.)

(5) a foreign government pursuant to executive agreement, compact, treaty, or statute;

[* COMMENT following section 3-103.

Finally, subsection (a)(5) generally authorizes disclosure of individually identifiable records to foreign governments pursuant to executive agreement, compact, treaty or statute. Informal exchanges of information between agencies and foreign governments are forbidden under this subsection. *]

STATE GOVERNMENTS, AGENCIES

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 9. Intergovernmental access of data.
A responsible authority shall allow another responsible authority access to data classified as not public only when the access is authorized or required by statute or federal law. An agency that supplies government data under this subdivision may require the requesting agency to pay the actual cost of supplying the data...

[* See section 4.5.4 for more thorough coverage of these provisions. Also, these definitions above can be found in section 4.3.1. *]

[* Although not expressly provided for in the Act, specific mention is made of intra-agency disclosures within specific categories of information. For example, in section 4.15.8.1, WELFARE DATA, it is stated that private data on individuals shall not be disclosed except to an agent of the welfare system, or to personnel of the welfare system. *]

[* COMMENT following SECTION 3-103.
Section 3-103 deals with inter-agency disclosure of individually identifiable records. Intra-agency use and disclosure of those records are not regulated in this section or elsewhere in this Article. The policy of this Act is that individually identifiable records can be freely used within an agency. The additional layer of controls necessary to limit intra-agency use and disclosure would be costly and administratively burdensome and add marginally at best to the already extensive duties of the agency to protect the privacy of individually identifiable records. *]

[* SECTION 3-103 covers interstate, foreign disclosures of data. See section 4.5.4. *]

Secondly, in order to define the scope of the agencies to be regulated, the term,"agency," is defined. See section 4.2 for a related discussion.

Three specific positions are defined only in the Minnesota Statutes--namely, "commissioner," "responsible authority," and "designee." This is a good concept because it assigns responsibilities to specific persons as opposed to having agencies carry out the various functions. In the broadest sense, agencies perform functions; but the designation of people to perform specific duties, and to be held accountable for these duties, makes the law more specific and concrete.

In the Uniform Code a director of the Office of Information Practices is assigned responsibility for the Office of Information Practices. A definition for the head of the agency, not unlike the responsible authority, is needed in this section of definitions.

The definitions of research records and research purpose in the Code denotes the purpose for which an individually identifiable record will be used. A research record is, in actuality, an individually identifiable record; whereas "summary data" in the Statutes refers to the output or results of the compilation of individually identifiable records. Thus, the definition of summary data is not linked with a purpose, for summary data may be generated for purposes other than research purposes.

4.3 DEFINITIONS

The most critical definitions in this section are those that relate to the definition of a personal record or data on individuals. This is because an individual's personal privacy can be abused when an agency handles personal records and discloses them to others. Moreover, these 2 definitions underly the structure of the acts with regard to the manner in which policy is formulated for disclosures of information. Two unique approaches in defining personal records have been taken in the two acts.

In the Minnesota Statutes, all government data must be assigned to 1 of 6 specific classifications of data. Although this framework is very clear cut, the implications of this scheme will become apparent in section 4.14 and 4.15. Each classification of data is also defined in terms of who can access the data.

Conversely, the Uniform Code defines a personal record, but it is more vague in the sense that it does not attempt to further classify all types of personal records into specific categories. Neither does it classify all government records that are not personal records. This results in less structured provisions because all data does not have to be classified,and the rules for accessing the data are not embedded in the definitions.

15.162 continued

Subd. 8.
"Statewide system" includes any record-keeping system in which government data is collected, stored, disseminated and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

Subd. 7.
"State agency" means the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state.

Subd. 5.
"Political subdivision" means any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision. It includes any nonprofit corporation which is a community action agency organized pursuant to the economic opportunity act of 1964 (P.L. 88-452) as amended, to qualify for public funds, or any nonprofit social service agency which performs services under contract to any political subdivision, statewide system or state agency, to the extent that the nonprofit social service agency or nonprofit corporation collects, stores, disseminates, and uses data on individuals because of a contractual relationship with state agencies, political subdivisions or statewide systems.

[* All above repeated. See section 4.2.3.2. *]

SECTION 1-105 continued

(2) "Agency"means a unit of government in this State, any political subdivision or combination of subdivisions, a department, institution, board, commission, district, council, bureau, office, officer, official, governing authority or other instrumentality of state or local government, or a corporation or other establishment owned, operated, or managed by or on behalf of this State or any political subdivision, but does not include the (name of legislative body) or the courts of this State.

[* See section 4.2.3.2 for notes to this definition. *]

4.3.1 Definitions--Up Front
4.3.1.1 Government data applicable

15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.
Subd. 1.
As used in sections 15.1611 to 15.1699, the terms defined in this section have the meanings given them.

REPEAT
Subd. 11.
"Government data" means all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use.

[* See section 4.2.3.1 for a discussion of these definitions. *]

SECTION 1-105 (General Definitions.)

Subject to additional definitions in subsequent Articles which are applicable to specific Articles, and unless the context otherwise requires in this Code:

REPEAT
(3) "Government record" means information maintained by an agency in written, aural, visual, electronic or other physical form.

[* See section 4.2.3.1. *]

(6) "Maintain" means hold, possess, preserve, retain, store, or administratively control.

15.162 continued

Subd. 5b. "Public data on individuals" means data which is accessible to the public in accordance with the provisions of section 15.1621.

Subd. 5a. "Private data on individuals" means data which is made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of that data.

[* Although the above definition states that the data is accessible to the data subject, it does not specify who else can access the data. *]

Subd. 2a. "Confidential data on individuals" means data which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data.

SECTION 1-105 continued

COMMENT continued

to extrinsic facts known or reasonably available to the requester? If neither part of the test is met, an agency may deal with the record free of the access and disclosure restrictions previously noted. *]

[* The Code has no concept of the Minnesota Act's classification system. It merely distinguishes the personal record from the rest of the government records rather than attempting to classify all personal records and all government records that are not personal records. *]

15.162 continued

Subd. 3.
"Data on individuals" means all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual.

[* See section 2.2 for explanation of this classification scheme. This is the crucial definition in understanding the Statutes, for anything that is not data on individuals is data not on individuals. *]

SECTION 1-105 continued

(8) "Personal record" means any item or collection of information in a government record which refers, in fact, to a particular individual, whether or not the information is maintained in individually identifiable form.

[* COMMENT from the Code following SECTION 1-105, page 5.
Section 1-105 (8) provides that a "personal record" is an item of information in a government record that refers in fact to a particular individual. The distinctive function of this term is to trigger certain general agency recordkeeping duties. *]

(5) "Individually identifiable record" means a personal record that identifies or can readily be associated with the identity of an individual to whom it pertains.

[* COMMENT from the Code following SECTION 1-105, page 6.
As used in this Code, this term limits public access to information in government records about individuals, e.g., sections 2-103(12), 3-101 and 3-102, and disclosure of such information between agencies, section 3-103. The test is objective:
(1) does the record on its face identify the individual to whom it pertains; or
(2) can the record be associated with the individual to whom it pertains by reference

15.162 continued

Subd. 3a. "Data not on individuals" means all government data which is not data on individuals.

Subd. 5b. "Public data not on individuals" means data which is accessible to the public pursuant to section 15.1621.

Subd. 5c. "Nonpublic data" means data not on individuals which is made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the subject, if any, of the data.

[* By definition, nonpublic data should not have a data subject. If one could be identified, it would be data on individuals. *]

SECTION 1-105 continued

(l) "Accessible record" means a personal record, except a research record, that is:

(i) maintained according to an established retrieval scheme or indexing structure on the basis of the identity of, or so as to identify, individuals; or

(ii) otherwise retrievable because an agency is able to locate the record through the use of information provided by a requester without an unreasonable expenditure of time, effort, money, or other resources.

[* An accessible record is defined to clearly state policy with regard to an agency's ability to retrieve the record when an individual requests to see his own personal record. See sections 4.4.3 and 4.4.4. *]

[* Individually identifiable records and accessible records are 2 types of personal records, but these 2 subsets are not meant to encompass all personal records. *]

15.162 continued

[* Public, private, and confidential data on individuals classify all data on individuals.*]

[* Again, the Minnesota Act is silent with regard to the other individuals or persons who can access the data, even though it is inaccessible to the individual data subject. These definitions will allow much room for other disclosures to be made which may be clearly unwarranted invasions of personal privacy. *]

SECTION 1-105 continued

15.162 continued

Subd. 5d. "Protected non-public data" means data not on individuals which is made by statute or federal law applicable to the data (a) , not public and (b) not accessible to the subject of the data.

[* The word, "non-public," in Subd. 5d. must be amended to "nonpublic." *]

[* Again, this definition does not make sense. If it is not data on individuals, it should not have a data subject and access provisions are irrelevant. *]

15.162 continued

Subd. 4.
"Individual" means a natural person. In the case of a minor, "individual" includes a parent or guardian or an individual acting as a parent or guardian, except that the responsible authority shall withhold data from parents or guardians, or individuals acting as parents or guardians in the absence of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor.

[* REPEAT See section 4.2.3.4. *]

[* Use of the definition of "minor" appears in section 4.15.10. It might be a good idea to separate the clause regarding the withholding of a minor's personal record by the responsible authority, from the definition of an individual. This situation might pertain to future categories of data under different circumstances. *]

Subd. 12. "Person" means any individual, partnership, corporation, association, business trust, or a legal representative of an organization.

SECTION 1-105 continued

(4) "Individual" means a natural person.

(7) "Person" means individual, corporation, government or governmental subdivision or agency, business trust, estate, trust, partnership, association, or any other legal entity.

15.162 continued

Subd. 9. "Summary data" means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

* Summary data is the aggregate information prepared from data on individuals. The research record is data on individuals, but its ultimate use is for research purposes. From this definition, summary data can be used for purposes other than research purposes. *]

SECTION 1-105 continued

(10) "Research record" means an individually identifiable record collected solely for a research purpose and not intended to be used in individually identifiable form to make any decision or to take any action directly affecting the individual to whom the record pertains.

(9) "Research purpose" means an objective to develop, study, or report aggregate or anonymous information not intended to be used in any way in which the identity of an individual is material to the results.

[* There is a definite emphasis on purpose which becomes apparent in the legislation concerning research records in section 4.10. The definition of a research record is clearly linked with research purpose. *]

15.162 continued

Subd. 2. "Commissioner" means the commissioner of the department of administration.

Subd. 6. "Responsible authority" in a state agency or a statewide system means the state official designated by law or by the commissioner as the individual responsible for the collection, use and dissemination of any set of data on individuals, government data, or summary data. "Responsible authority" in any political subdivision means the individual designated by the governing body of that political subdivision as the individual responsible for the collection, use, and dissemination of any set of data on individuals, government data, or summary data, unless otherwise provided by state law.

Subd. 10. "Designee" means any person designated by a responsible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data.

* Because these 3 positions are defined, the roles for each position must be specified in the Act. *]

[* The Code does not provide for any definitions in the definition section. Because the director of the Office of Information Practices is appointed later, it would be a good idea to define that position in this section. *]

[* The Code employs the all-encompassing term, "agency," to delegate responsibilities. Specific positions are not defined for specific persons. *]

4.4 PUBLIC AND INDIVIDUAL ACCESS TO INFORMATION

Section 4.4 introduces some very interesting developments. An agency's government data is declared to be accessible to the public in an expressly stated freedom of information policy. The Uniform Code states that government records are available to the public for inspection during business hours. The Minnesota Statutes declares all government data to be classified as public (either public data on individuals or public data not on individuals) unless otherwise classified by statute, federal law, or temporary classification. Doing so infers that all exceptions must be declared by law. Hence, all of these exceptions are listed in section 4.15. This is the primary disadvantage of the Minnesota Statutes' scheme of defining all government data to fit a particular data classification.

Interestingly, the terminology used in each act impacts the forcefulness of each act in a subtle manner. The Minnesota Act refers to the freedom of information policy as "Access to Government Data." This terminology views access to an agency's information from the standpoint of the general public. The Uniform Code calls it, "Duties of Agency," which specifically focuses and assigns responsibilities to the agency.

Individual access to one's own personal records, and the limitations placed on this access, are also covered. The procedures for access in the Uniform Code

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 8. Publication of access procedures.
The responsible authority shall prepare a public document setting forth in writing the rights of the data subject pursuant to section 15.165 and the specific procedures in effect in the state agency, statewide system or political subdivision for access by the data subject to public or private data on individuals.

Article 2

Freedom of Information

SECTION 2-101 (Affirmative Agency Disclosure Responsibilities.)

Each agency shall make available for public inspection:

(1) rules of procedure, substantive rules of general applicability, statements of general policy, and interpretations of general applicability, adopted by the agency; and

(2) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases.

are the same as those for public access, with the exception that the individual's identity must be confirmed and that the agency should provide an audit trail of disclosures made, if requested. The Statutes contain a provision whereby the agency is not required to disclose the individual's record for 6 months after a request has been made. If would be a good idea to include a provision similar to this in the Code because continual requests by the same requester could jeopardize the agency's operations.

The Minnesota Statutes specify time limits for acting upon an individual's request to inspect his own record, but such time limits are not mentioned in public access to information. Both types of requesters should be treated equally.

Finally, it must be noted that there are contingent situations in which the responsible authority (in the Statutes) is allowed to use discretion in deciding whether to release an individual's record to the individual or to the public. These situations are declared by Statute and involve examination and law enforcement data, and disclosure of a minor's personal records. The provisions for these contingent situations resemble the construction of provisions for disclosure in the Code.

15.1621 continued

Subd. 2. Procedures.
The responsible authority in every state agency, political subdivision, and statewide system shall establish procedures, consistent with sections 15.1611 to 15.1698, to ensure that requests for government data are received and complied with in an appropriate and prompt manner...

Subd. 3. Request for data.
...If the responsible authority or designee is not able to provide copies at the time a request is made he shall supply copies as soon as reasonably possible...

Subd. 3. Request for data.
Upon request to a responsible authority or designee, a person shall be permitted to inspect and copy government data at reasonable times and places, and if the person requests, he shall be informed of the data's meaning.

* The Act need more definite time and cost policies. Without any definite time limits, it could be months before an agency might respond to the request. *]

SECTION 2-102 continued

(d) Promptly, but no later than 7 days after receiving a written request for access which reasonably identifies or describes a government record, the agency shall:

[* Notice that both acts emphasize promptness, but the Code sets a time limit for acting on the request to ensure that it replies promptly. *]

(1) make the record available to the requester, including, if necessary, an explanation of any machine readable code or any other code or abbreviation;

(2) inform the requester that the record is in use or that unusual circumstances have delayed or impaired the handling of the request and specify in writing the earliest time and date, not later than 21 days after receipt of the request, when the record will be available;

(3) inform the requester that the agency does not maintain the requested record, and provide, if known, the name and location of the agency maintaining the record; or

(4) deny the request.

* Compare the two section titles. The Act is from the viewpoint of the public; the Code makes it a duty of the agency. *]

15.1621 ACCESS TO GOVERNMENT.
Subd. 1. Public data.
All government data collected, created, received, maintained or disseminated by a state agency, political subdivision, or statewide system shall be public unless classified by statute, or temporary classification pursuant to section 15.1642, or federal law, as not public, or with respect to data on individuals, as private or confidential. The responsible authority in every state agency, political subdivision and statewide system shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use. Photographic, photostatic, microphotographic, or microfilmed records shall be considered as accessible for convenient use regardless of the size of such records.

* Declaring all government data to be public unless classified otherwise makes it necessary to name all other exceptions. This becomes cumbersome if there are many exceptions. It also ignores use. *]

SECTION 2-102 (Duties of Agency.)
(a) Except as provided in section 2-103, each agency upon request by any person shall make government records available for inspection and copying during regular business hours.

[* By defining an accessible record, the Code does not require agencies to conform to this order. In manual systems this might be costly for the agency to do. *]

15.1621 continued

15.1621 ACCESS TO GOVERNMENT DATA
Subd. 2. Procedures.
...Full convenience and comprehensive accessibility shall be allowed to researchers including historians, genealogists and other scholars to carry out extensive research and complete copying of all records containing government data except as otherwise expressly provided by law.

* This provision should be in the Minnesota Statutes because it limits the amount of information the agency is required to access. What is meant by "comprehensive accessibility" above? What explicit rules are there for covering the cost to the agency versus the public right to access records? *]

SECTION 2-102 continued

(b) Unless the information is readily retrievable by the agency in the form in which it is requested, an agency is not required to prepare a compilation or summary of its records.

(c) Each agency shall assure reasonable access to facilities for duplicating records and for making memoranda or abstracts from them. If a government record is not immediately available or a request for access is denied, the agency shall inform the requester of the right to make a written request for access under subsection (d).

[* COMMENT following SECTION 2-102 of the Code.

"While this does not require each agency to have its own duplicating equipment, it does impose an oblication to establish agency procedures for having copies of records made when requested." *]

15.1621 continued

Subd. 3. Request for data.
...The responsible authority or designee shall provide copies of government data upon request. The responsible authority may require the requesting person to pay the actual costs of making, certifying and compiling the copies.

* There is much leeway here as to what the agency may charge. *]

SECTION 2-102 continued

(e) Unless otherwise provided by law, whenever an agency provides a copy of a government record, it may charge the currently prevailing commercial rate for copying. An agency may not charge for the services of government personnel in searching for a record, reviewing its contents, and segregating disclosable from non-disclosable information or for expenses incurred in establishing or maintaining the record. The agency shall establish a schedule of its charges and make it available to the public.

[* COMMENT following SECTION 2-102 of the Code.

The policy underlying subsection (e) reflects an accommodation between promoting public access to government records and fairly allocating the costs of agency compliance on a case-by-case basis. If the cost of exercising rights under this Article is too high, the Article will not achieve its broad purposes. The public as a whole benefits from the policy of access to governmental information. For that reason, subsection (e) requires each agency to absorb all costs of compliance except the cost of copying. But when a person receives a copy of a government record, the character of the benefit conferred on the person is direct and immediate. This justifies shifting the cost of duplication to the record requester. *]

* It is a good idea to verify the individual's identity to prevent fradulent access. Section 15.166 seems to emphasize agency violations, and does not consider fradulent access. *]

* Minnesota Statutes does not contain this provision because an audit trail is not required. *]

SECTION 3-105 (Access to Records by Record Subject.)

Except as provided in section 3-106, an individual or his duly authorized representative may examine or copy, during the regular business hours of the agency, any accessible record that pertains to him. In implementing the rights under this section, the agency shall follow the procedures established in section 2-102, subject to the following additional requirements:

(1) upon receipt of a written request to examine or copy an accessible record, the agency shall verify the identity of the requester; and

(2) the agency, if specifically requested, shall inform the requester of all disclosures of the record outside the agency as required in subsection 3-108 (a)(2).

[* See section 4.6.2 for audit trail discussion. *]

15.1621 continued

Subd. 3. Request for data.
...If the responsible authority or designee determines that the requested data is classified so as to deny the requesting person access, the responsible authority or designee shall so inform the requesting person orally at the time of the request, and in writing as soon thereafter as possible, and shall cite the statute, temporary classification, or federal law on which the determination is based.

[* Again, specific time limits for dealing with this situation are absent. *]

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 5. Data protection.
The responsible authority shall (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; and (2) establish appropriate security safeguards for all records containing data on individuals.

* A discussion of this clause is in section 4.6. It is more relevant to the collection and maintenance of records. *]

SECTION 2-102 continued

(f) If a request for access to a government record is denied, in whole or in part, the agency in writing shall notify the requester of the specific reasons for its denial, and identify by name and position or title the individual responsible for its denial. In addition, the agency shall inform the requester that review of a denial of access may be sought from the head of the agency and that a request for review must be filed within 90 days after notification of the denial. The head of the agency, within 10 days after a request for review is filed, shall decide whether the denial of access will be upheld. If the decision is to disclose, the agency shall immediately notify the requester and make the record available. If the denial of access is upheld, in whole or in part, the head of the agency is writing shall notify the requester of the decision, the specific reasons for the decision and the right to bring a judicial action under this Code.

(g) Each agency may adopt reasonable rules to protect its records from theft, loss, defacement, alteration, or deterioration and to prevent undue interference with the discharge of its functions.

[* See section 4.6. *]

15.165 continued

* Why is there a time restriction here and not for public access to data? A priority should not be given to the individual's accessing his own records. Public and individual access are equally important. *]

15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 3.

Upon request to a responsible authority, an individual shall be informed whether he is the subject of stored data on individuals, and whether it is classified as public, private, or confidential. Upon his further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge to him and, if he desires, shall be informed of the content and meaning of that data. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to him for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected or created. The responsible authority shall provide copies of the private or public data upon request by the individual subject of the data. The responsible authority may require the requesting person to pay the actual costs of making, certifying, and compiling the copies.

The responsible authority shall comply immediately, if possible, with any request made pursuant to this subdivision, or within five days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. If he cannot comply with the request within that time, he shall so inform the individual, and may have an additional five days within which to comply with the request, excluding Saturdays, Sundays and legal holidays.

SECTION 3-105 continued

[* See section 4.4.4 for comment. *]

[* See 4.3.1.5 definition of individual. There are restrictions on parents gaining access to a minor's personal records in the definition. *]

REPEAT
15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 3.

...After an individual has been shown the private or public data and informed of its meaning, the data need not be disclosed to him for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected or created...

SECTION 3-106 continued

(b) This section does not abridge any statute that authorizes an agency to withhold information from the parent or legal guardian of a child.

(c) If an individual requests an accessible record containing information the agency is not required to disclose under subsections (a) and (b), the agency shall provide any reasonably segregable portion of the record to the requester after deleting the undisclosable material.

[* In effect, this clause imposes a check on the agency to make sure that too much information is not withheld when parts of a record can be disclosed. *]

[* This is a necessary limitation which is missing in the Code. An individual can request to examine his personal record(s) as many times as desired. Abuse on the part of requesting individuals must also be checked. *]

* Because the data is classified and access depends on the designated classification, the responsible authority generally does not have to delicately balance or be held responsible for deciding which situations override an individual's gaining access to his own record. There are exceptions, though, where subjective judgment is used. See sections 4.3.1.5, 4.15.5.1, 4.15.5.4, and 4.15.13. *]

SECTION 3-106 (Limitations on Individual Access.)

(a) An agency is not required by section section 3-105 to disclose;

(1) information that may be withheld pursuant to section 2-103 (a)(1) and (3) through (11) except to the extent that the information sought was submitted by the requester, but under appropriate safeguards designed to protect the integrity of the examination process, an individual may examine, but not copy, his own test questions and answers in any examination used for licensing or employment;

(2) information collected and used solely to evaluate the character and fitness of persons, but only to the extent that disclosure would identify the source of the information; or

(3) information that does not relate directly to the requester, and which if disclosed, would constitute a clearly unwarranted invasion of another individual's personal privacy.

the authority to disclose or not disclose information. However, the power gained from this authority is kept in check by the fact that the responsible authority is held liable for any decision made. For example, if the responsible authority decides not to disclose information to the public, the responsible authority must justify why this decision was made, if there is opposition to it.

Taken from this perspective, section 4.5 presents sets of guidelines for disclosure and nondisclosure. The wording in sections 4.5.1 - 4.5.5 is created to intentionally place the burden of decision upon the responsible authority.

Section 4.5.1 lists 12 categories of information which are exceptions to disclosure. The responsible authority does not have to disclose information which would be used for 12 different purposes if the interest in nondisclosure outweighs the public interest in disclosure.

Sections 4.5.1, 4.5.3, and 4.5.4 relate specifically to individually identifiable records and issues surrounding personal privacy. Personal and individually identifiable records were defined in section 4.3 because unauthorized disclosure of personal records could lead to a personal privacy abuse.

Section 4.5.2 prohibits an agency from disclosing an individually identifiable record to any person other than the individual to whom the record pertains. However,

4.5 DISCLOSURE AND PURPOSE

Tension exists in data privacy legislation when attempting to balance the principles of public access to information with personal privacy of an individual. Section 4.4 discussed public and individual access to government data. The Minnesota Statutes strike a compromise between public access and personal privacy by declaring all government data as being public unless otherwise classified. If data is otherwise classified, the public cannot access it; and the individual's or data subject's privacy is maintained. In this way, a balance is reached between public access and personal privacy.

The problem with this system is that an application to change the classification of data applies to <u>all</u> records within a certain category of information. This "all or none" type of system disregards the uses for which the data will be put. For example, in some cases, the public benefit in accessing a record classified as private might outweigh the individual's desire to keep the record private. Therefore, a mechanism does not exist which would weigh public access against personal privacy.

Rather than employing the above-mentioned system, the Uniform Code utilizes a completely different approach. The responsible authority of an agency is given

unless they pertain to any of the 8 categories listed.

Certainly these lists are not meant to be all-inclusive. That would be an impossible feat to perform. Instead, the most important exceptions or conditions are conveyed, and the decision to disclose or not disclose rests upon the responsible authority.

Some categories listed could possibly be covered under two different sections. For instance, information compiled as part of an investigation might not be disclosed in conjunction with section 4.5.1. It also might not be disclosed due to section 4.5.2 because it would be an unwarranted invasion of privacy.

10 types of information or conditions under which it would be permissible to disclose an individually identifiable record are identified. These 10 exceptions are short and are not very explicit; and the tenth category ("in any other case, not a clearly unwarranted invasion of personal privacy") leaves much room for interpretation and subjective judgment on the part of the responsible authority.

What constitutes a clearly unwarranted invasion of personal privacy? The next section does not define all the conditions which satisfy a clearly unwarranted invasion of personal privacy. Rather, the reverse is explained. That is, if the public interest in disclosure outweighs the privacy interest of the individual, then disclosure of an individually identifiable record does not constitute a clearly unwarranted invasion of personal privacy. Therefore, the responsible authority must himself eliminate those cases that he believes not to be a clearly unwarranted invasion of privacy. Also, 9 examples of information where the individual would be very interested in protecting his privacy interests are listed; but it is not explicitly stated that these 9 examples are clearly unwarranted invasions of personal privacy.

Afterwards, section 4.5.4 conveys policy on disclosures of individually identifiable records to other agencies and other governments. Disclosures are prohibited

* The Statutes declare examination data to be nonpublic. This declaration is followed by exceptions for disclosure to the public, or nondisclosure to the individual who took the exam. The resulting accessibility of examination data is similar to the Code, except that its classification is nonpublic. *]

SECTION 2-103 continued

[* See section 4.5.4 (a)(3). Subsection (a)(1) and (a)(2) above exempt certain inter- and intra-agency communications from disclosure for law enforcement purposes. This overlaps with the provision (a)(3) of section 4.5.4, which covers interstate, inter-agency, foreign disclosures. The main difference is that section 2-103 is for government records, and section 3-103 specifically relates to individually identifiable records. *]

(2) inter-agency or intra-agency advisory, consultative, or deliberative material (other than factual information) if:

(i) communicated for the purpose of decision-making, and

(ii) disclosure would substantially inhibit the flow of ideas within an agency or impair the agency's decision-making processes;

(3) material prepared in anticipation of litigation which would not be available to a party in litigation with the agency under the rules of pretrial discovery for actions in the (designate appropriate court) of this State;

(4) materials used to administer a licensing, employment, or academic examination if disclosure would compromise the fairness or objectivity of the examination process;

4.5.1 Cases Where Information is Not Subject to the Duty of Disclosure

SECTION 2-103 (Information Not Subject to Duty of Disclosure.)

(a) This Article does not require disclosure of:

[* The following 12 categories of information are not meant to be entire record systems. These 12 exemptions give the agency the authority not to disclose information if it is not in the public interest to do so. *]

(1) information compiled for law enforcement purposes if disclosure would:

(i) materially impair the effectiveness of an ongoing investigation, criminal intelligence operation, or law enforcement proceeding,

(ii) identify a confidential informant,

(iii) reveal confidential investigative techniques or procedures, including criminal intelligence activity, or

(iv) endanger the life of an individual;

SECTION 2-103 continued

(11) information that is expressly made nondisclosable under federal or state law or protected by the rules of evidence; or

| * This section (a)(1) through (a)(11) is confusing in the sense that individually identifiable records may be included in 1 through 11 above. However, individually identifiable records are also treated separately in Article 3, so it might be better to reword subsection (a) as: "(a) This Article pertains to all government records, including individually identifiable records. It does not require ..." *|

(12) an individually identifiable record not disclosable under Article 3.

(b) If an agency pursuant to section 2-102 (a) decides to grant a request to inspect or copy a government record to which subsections (a)(8), (10) or (12) may apply, the agency shall make reasonable efforts to notify the person to whom the record relates and provide him an opportunity to object to disclosure of the record.

(c) If a person submits information claimed to be subject to subsection (a)(9), the agency shall upon such person's request make reasonable efforts to notify the person making the claim and provide him an opportunity to object prior to disclosure of the record.

* See section 4.15.4. *]

* See section 4.15.11. *]

* See section 4.15.3. *]

* See section 4.15.3. *]

* See section 4.15.3. *]

* See section 4.15.14. *]

SECTION 2-103 continued

(5) information which, if disclosed, would frustrate government procurement or give an advantage to any person proposing to enter into a contract or agreement with an agency;

(6) information identifying real property under consideration for public acquisition before acquisition of rights to the property; or information not otherwise available under the law of this State pertaining to real property under consideration for public acquisition before making a purchase agreement;

(7) administrative or technical information, including software, operating protocols, employee manuals or other information, the disclosure of which would jeopardize the security of a record keeping system;

(8) proprietary information, including computer programs and software and other types of information manufactured or marketed by persons under exclusive legal right, owned by the agency or entrusted to it;

(9) trade secrets or confidential commercial and financial information obtained, upon request, from a person;

(10) library, archival, or museum material contributed by private persons to the extent of any lawful limitation imposed on the material;

4.5.2 Cases Where Personal Records May Be Disclosed to the Public

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 4: Collection and use of data; general rule.
Private or confidential data on an individual shall not be collected, stored, used or disseminated by political subdivisions, statewide systems or state agencies for any purposes other than those stated to the individual at the time of collection in accordance with section 15.165, except as provided in this subdivision.

(a) Data collected prior to August 1, 1975, and which have not been treated as public data, may be used, stored, and disseminated for the purposes for which the data was originally collected or for purposes which are specifically approved by the commissioner as necessary to public health, safety, or welfare.

[* This section attempts to integrate public access to information with personal privacy. It limits the amount of information that can be disclosed to the public with regard to individually identifiable records. The following is a list of exceptions--disclosures of individually identifiable records which can be made. *]

SECTION 3-101 (Limitations on Disclosure to Public.)

An agency may not disclose or authorize the disclosure of an individualy identifiable record to any person other than the individual to whom the record pertains unless the disclosure is:

SECTION 2-103 continued

(d) If over objection, the agency decides to grant the request for access, it shall inform each objector of the agency's decision and the right to seek review from the head of the agency.

(e) If the head of the agency decides to grant the request, he shall give reasonable notice to each objector of his decision to release information. If the head of an agency denies a request for access because information is within subsections (a)(8), (9), (10) or (12) and the agency is subsequently sued as a result of that denial, it shall make reasonable efforts to inform each objector of the suit.

(f) The agency shall provide any reasonably segregable portion of the record to the person requesting it after deleting the undisclosable material.

15.163 (4)(d) continued

(6) Specific as to the purpose or purposes for which the information may be used by any of the parties named in clause (5), both at the time of the disclosure and at any time in the future.

(7) Specific as to its expiration date which should be within a reasonable period of time, not to exceed one year except in the case of authorizations given in connection with applications for life insurance or noncancelable or guaranteed renewable health insurance and identified as such, two years after the date of the policy.

SECTION 3-101 continued

(3) of information collected and maintained for the purpose of making information available to the general public;

(4) of information contained in or compiled from a transcript, minutes, report, or summary of a proceeding open to the public;

15.163 continued

Subd. 4. Collection and use of data; general rule.

...(d) Private data may be used by and disseminated to any person or agency if the individual subject or subjects of the data have given their informed consent. Whether a data subject has given informed consent shall be determined by rules of the commissioner. Informed consent shall not be deemed to have been given by an individual subject of the data by the signing of any statement authorizing any person or agency to disclose information about him or her to an insurer or its authorized representative, unless the statement is:

(1) In plain language;
(2) Dated;
(3) Specific in designating the particular persons or agencies the data subject is authorizing to disclose information about him or her;
(4) Specific as to the nature of the information he or she is authorizing to be disclosed;
(5) Specific as to the persons or agencies to whom he or she is authorizing information to be disclosed;

SECTION 3-101 continued

(1) the name, compensation, job title, business address, business telephone number, job description, education and training background, previous work experience, or dates of first and last employment of present or former officers or employees of the agency;

(2) pursuant to the prior written consent of the individual to whom the record refers;

[* This is much less comprehensive than the Statutes. *]

SECTION 3-101 continued

(7) pursuant to an order of a court in which case the agency shall notify the individual to whom the record refers by mailing a copy of the order to his last known address;

(8) pursuant to a subpoena from (either House of) the (name of legislative body) or any committee or subcommittee, in which case the agency shall notify the individual to whom the record refers by mailing a copy of the subpoena to his last known address;

(9) for a research purpose as provided in section 3-109 and 3-110; or

(10) in any other case, not a clearly unwarranted invasion of personal privacy.

4.5.2 continued

15.163 continued

Subd. 4. Collection and use of data; general rule.

(b) Private or confidential data may be used and disseminated to individuals or agencies specifically authorized access to that data by state, local, or federal law subsequent to the collection of the data.

(c) Private or confidential data may be used and disseminated to individuals or agencies subsequent to the collection of the data when the responsible authority maintaining the data has requested approval for a new or different use or dissemination of the data and that request has been specifically approved by the commissioner as necessary to carry out a function assigned by law.

[* (c) above contradicts the principle stated in section 4.6.1 that an individual has a right to know the purpose for which the data is being collected. If the data will be put to a new use, the individual must be notified or the data must be re-collected. *]

SECTION 3-101 continued

(5) pursuant to federal law or a statute of this State that expressly authorizes disclosure;

(6) pursuant to a showing of compelling circumstances affecting the health or safety of any individual, in which case the agency shall make reasonable efforts to notify the individual to whom the record refers;

SECTION 3-102 continued

(b) The following are examples of information in which the individual has a significant privacy interest:

(1) information relating to medical, psychiatric, or psychological history, diagnosis, condition, treatment, or evaluation, other than directory information concerning an individual's presence at any facility;

(2) information compiled and identifiable as part of an investigation into a possible violation or criminal law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation.

(3) information relating to eligibility for social services or welfare benefits or to the determination of benefit levels;

(4) information in an agency's personnel file, or applications, nominations, recommendations or proposals for public employment or appointment to a governmental position; except information relating to the status of any formal charges against the employee and disciplinary action taken;

(5) information relating to an individual's nongovernmental employment history;

4.5.3 Cases Where the Individual Has a Significant Privacy Interest

[* The Minnesota Statutes declare that all information is public unless classified otherwise. Prevention of data privacy abuses using the Statutes' methodology takes the benefit of the majority into account. If the majority are protected, the exceptional cases are not considered. Data privacy abuses are very personal in nature. The circumstances surrounding each situation are unique. Thus, the Statutes really do not focus upon intent of usage. *]

[* This is one of the most interesting sections in the Code. Titled, "Clearly Unwarranted Invasion of Personal Privacy," I expected a list of situations which would be an unwarranted invasion of personal privacy. Instead, it is worded in a way such that 9 situations in which the individual has a significant privacy interest are presented. *]

SECTION 3-102 (Clearly Unwarranted Invasion of Personal Privacy.)

(a) Disclosure of an individually identifiable record does not constitute a clearly unwarranted invasion of personal privacy if the public interest in disclosure outweighs the privacy interest of the individual.

[* Subsection (a) is conditional. This makes it possible to judge each disclosure on a case-by-case basis. *]

4.5.4 Interstate, Inter-Agency, Foreign Disclosures

[* Section 4.5.1 covers disclosure of individually identifiable records to the public. This section covers the disclosure of individually identifiable records to other agencies, other states, or foreign governments. *]

[* See section 4.2.3.4, Scope, for reasons why intra-agency disclosures are not covered. *]

SECTION 3-103 (Disclosures to Agencies of Government.)

(a) In addition to disclosures permitted under section 3-101, an agency may disclose or authorize the disclosure of an individually identifiable record if made to:

(1) another agency if disclosure is:

(i) certified by the requesting agency as being necessary to the performance of its duties and functions, and

(ii) compatible with the purpose for which the information in the record was originally collected or obtained;

SECTION 3-102 continued

(6) information in an income or other tax return measured by items of income or gathered by an agency for the purpose of administering the tax;

(7) information describing an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or credit worthiness;

(8) information compiled as part of an inquiry into an individual's fitness to be granted or to retain a license, except the record of any proceeding resulting in revocation or suspension of a license and the grounds for revocation or suspension; and

(9) information comprising a personal recommendation or evaluation.

15.163 continued

[* This conflicts with the notion (section 4.6.2) that an individual shall be informed of the purpose for which the data is being used. In the above case, the individual must be notified of this change in usage. *]

Subd. 9. Intergovernmental access of data.

A responsible authority shall allow another responsible authority access to data classified as not public only when the access is authorized or required by statute or federal law. An agency that supplies government data under this subdivision may require the requesting agency to pay the actual cost of supplying the data.

REPEAT

15.1643 INTERNATIONAL DISSEMINATION PROHIBITED.

No state agency or political subdivision shall transfer or disseminate any private or confidential data on individuals to the private international organization known as Interpol.

[* Only prohibits--does not formulate policy on disclosures to foreign governments. *]

[* See section 4.2.3.4. *]

SECTION 3-103 continued

(iii) pursuant to agreement or written request;

(4) an agency for transmission to courts of this State, another state or the United States for pre-sentence or probationary purposes;

(5) A foreign government pursuant to executive agreement, compact, treaty, or statute;

REPEAT

15.163 DUTIES OF RESPONSIBLE AUTHORITY

Subd. 4. Collection and use of data; general rules.

...(b) Private or confidential data may be used and disseminated to individuals or agencies specifically authorized access to that data by state or federal law subsequent to the collection of the data.

(c) Private or confidential data may be used and disseminated to individuals or agencies subsequent to the collection of the data when the responsible authority maintaining the data has requested approval for a new or different use or dissemination of the data and that request has been specifically approved by the commissioner as necessary to carry out a function assigned by law.

SECTION 3-103 continued

[* Both conditions above must hold or else the agency should collect the information directly from the individual. *]

(2) the State Archives for purposes of historical preservation, administrative maintenance, (or destruction);

(3) another agency, another state, or the federal government if disclosure is:

(i) for the purpose of a civil or criminal law enforcement investigation,

(ii) specifically authorized by statute or compact, and

4.5.5 Uniform Code: Overriding Prohibition on Disclosure.

SECTION 3-104 (Prohibitions on Disclosures Not affected.)

Nothing in sections 3-101 through 3-103 authorizes the disclosure of an individually identifiable record if disclosure is otherwise prohibited by law.

15.163 DUTIES OF RESPONSIBLE AUTHORITY:
Subd. 9. Intergovernmental access of data.
...Data shall have the same classification in the hands of the agency receiving it as it had in the agency providing it.

SECTION 3-103 continued

(6) a criminal law enforcement agency of this State, another state, or the federal government if the information requested is limited to an individual's name and other identifying particulars, including present and past addresses and present and past places of employment;

(7) authorized officials of the federal government or of an agency of this State for audit or review purposes if:

(i) the audit or review is expressly authorized by law, and

(ii) disclosure is certified by the requesting agency as being necessary to the performance of audits or reviews; or

(8) the United States Bureau of the Census for the purpose of planning or carrying out a census, survey or related activity under Title 13 of the U.S. Code.

[* Thus, inter-agency disclosures of individually identifiable records are prohibited unless one of the above exceptions applies. *]

(b) An agency receiving information pursuant to subsection (a) is subject to the same restrictions on disclosure of the information as the originating agency.

4.6 DUTIES OF THE HOLDERS OF INFORMATION

Because a transaction is being conducted between the individual and the agency, several necessary practices are required of an agency when collecting and maintaining information. First, unnecessary information must not be gathered. While collecting the information, the individual must be informed of the intended uses of the data being supplied. Also, the agency must clarify to the individual: the consequences of not supplying the information; the persons authorized to access the data; and whether the identity of the individual and the information supplied by that individual will be revealed to the subject of the data in the case of, for instance, a personal recommendation. This last provision is absent in the Minnesota Statutes.

The agency is also expected to maintain accurate records, establish security safeguards, and keep an audit trail of disclosures. An audit trail provision is not included in the Act. Only the existence of data on an individual and the classification of that data (if any) are provided to the requesting individual. Personal privacy abuses occur when the information is not used for its intended purpose. If the person is unable to see what disclosures were made via an audit trail, personal privacy abuses could occur which would never be known to the individual.

One more agency duty to the individual is to provide procedures whereby an individual may contest the accuracy of the data. In the case of a denial to amend

a record, the Statutes do not relay enough information to the individual with regard to why the request was denied, along with the resources or alternatives available to the individual after a denial.

Annual reports must be submitted to either the commissioner (for the Statutes), or the Office of Information Practices or Secretary of State (for the Code) when requested. These reports are meant to monitor the types of information being maintained by the agency, request information, and agency compliance with the provisions. Although this report might initially be time consuming to agencies unfamiliar with the requirements, the commissioner or Office of Information Practices could provide assistance to these agencies.

REPEAT
15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 5. Data protection.
The responsible authority shall (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected;

...and (2) establish appropriate security safeguards for all records containing data on individuals.

[* See section 4.4.2. *]

SECTION 3-108 continued

(5) collect and maintain all records used by the agency with the accuracy, completeness, timeliness, and relevance reasonably necessary to assure fairness in agency action affecting the individual to whom they pertain; and

(6) establish reasonable safeguards to assure the integrity, confidentiality, and security of individually identifiable records.

REPEAT
SECTION 2-102 (Duties of Agency.)
(g) Each agency may adopt reasonable rules to protect its records from theft, loss, defacement, alteration, or deterioration and to prevent undue interference with the discharge of its functions.

[* See section 4.4.2. *]

SECTION 3-108 (Collection and Maintenance of Information.)
(b) The requirements of subsection (a)(5) do not apply to an agency or component thereof whose principal function is criminal law enforcement if the agency clearly identifies potentially inaccurate, untimely, incomplete, or irrelevant information to the users and recipients of information.

15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 1.
The rights of individuals on whom the data is stored or to be stored shall be as set forth in this section.

Subd. 2.
An individual asked to supply private or confidential data concerning himself shall be informed of: (a) the purpose and intended use of the requested data within the collecting state agency, political subdivision or statewide system; (b) whether he may refuse or is legally required to supply the requested data; (c) any known consequence arising from his supplying or refusing to supply private or confidential data; and (d) the identity of other persons or entities authorized by state or federal law to receive the data.

SECTION 3-108 continued

(4) inform each individual from whom information is requested:

(i) of the principal purposes for which the agency intends to use the information;

(ii) of the consequences to the individual of not providing the information; and

(iii) whether the information collected and the identity of the person providing it will be accessible to the individual to whom the information pertains;

[* This phrase (iii above) is unclear. I had to read the COMMENT section to understand it. The reason for this difficulty is that the individual being referred to in (4) changes to the identity of the person providing it. Perhaps, "whether the individual's identity and the information supplied the agency will be accessible to the individual to whom the information pertains in the case where an individual provides information about another person to the agency." *]

Section 36 LAW ENFORCEMENT DATA.
Subd. 10. Data retention.
Nothing in this section shall require law enforcement agencies to create, collect or maintain data which is not required to be created, collected or maintained by any other applicable rule or statute.

[* The above requirement, although not part of the omnibus portion of the Act, is inserted to show that the provision in section 36 is redundant. *]

SECTION 3-108 continued

(2) maintain a record of all disclosures of individually identifiable records to recipients outside the agency during the preceding 3 years, including the identity of each recipient and the date of each disclosure, but an agency is not required to maintain an accounting of disclosures made pursuant to sections 3-101 (1) through (4) and sections 3-103 (a)(2), (5) and (7);

[* See section 4.6.2 for notes. *]

(3) collect information, whenever practicable, directly from the individual to whom the information pertains;

[* Also see section 4.5.4(a)(1) for disclosures to agencies. The COMMENT section emphasizes that if the use is not compatible with purpose for which it was originally intended, the agency should collect the data directly from the individual. *]

15.163 DUTIES OF RESPONSIBLE AUTHORITY

Subd. 3. Standards for collection and storage.

Collection and storage of public, private or confidential data on individuals and use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature, local governing body or mandated by the federal government.

REPEAT

Subd. 4. Collection and use of data; general rule.

Private or confidential data on an individual shall not be collected, stored, used or disseminated by political subdivisions, statewide systems or state agencies for any purposes other than those stated to the individual at the time of collection in accordance with section 15.165, except as provided in this subdivision.

(a) Data collected prior to August 1, 1975, and which have not been treated as public data, may be used, stored, and disseminated for the purposes which are specifically approved by the commissioner as necessary to public health, safety, or welfare.

[* See section 4.5.2. *]

SECTION 3-108 (Collection and Maintenance of Information.)

(a) Each agency that collects, receives or maintains personal records shall:

(1) collect or maintain only information about individuals necessary to accomplish its purposes as authorized by federal law or executive order, state statute or executive order, or local ordinance or resolution:

4.6.2 Audit Trail

[* An audit trail is vital to the individual to ensure that unauthorized disclosures have not been made. With the current provisions, an individual can only find out whether the agency maintains any information on the individual, and which classification of data it belongs to (if any). Instead, it is much more important to know who accessed the individual's data and what it was used for. *]

REPEAT
SECTION 3-108 (Collection and Maintenance of Information.)

(a) Each agency that collects, receives, or maintains personal records shall:

(2) maintain a record of all disclosures of individually identifiable records to recipients outside the agency during the preceding 3 years, including the identity of each recipient and the date of each disclosure, but an agency is not required to maintain an accounting of disclosures made pursuant to sections 3-101(1) through (4) and sections 3-103 (a)(2), (5) and (7);

REPEAT
SECTION 3-105 (Access to Records by Record Subject.)
(2) the agency, if specifically requested, shall inform the requester of all disclosures of the record outside the agency as required in subsection 3-108 (a)(2).

[* Also in section 4.4.3. *]

REPEAT
15.1621 ACCESS TO GOVERNMENT DATA.
Subd. 1. Public data.
...The responsible authority in every state agency, political subdivision and statewide system shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use...

Subd. 2. A responsible authority may designate one or more designees.

SECTION 3-108 continued

[* The Code does not make this requirement. This might pose an undue burden on the agency. *]

4.7 ENFORCEMENT, REMEDIES, PENALTIES

An aggrieved individual may take action against an agency in court, primarily for the following reasons: (1) if it is felt that there has been an invasion of privacy; (2) if the agency failed to comply with the provisions of the Act or the Code; or (3) if the agency did not disclose information which the individual feels should have been disclosed. The provisions for court procedures are similar for both acts, with the exception that the Uniform Code separates violations to public access and disclosure, from violations to individual access and disclosure. The Minnesota Act includes both in one section.

The major differences between the Code and the Act are that:

1. In the Code, the burden is upon the agency to prove why a personal record or government record cannot be disclosed to the public, or why an individual cannot gain access to his own personal record.
2. In the Code, the agency can be held liable for not complying with the time limit.
3. The Code includes provisions to indemnify itself from an employee or officer of the agency who commits data privacy violations.
4. The Code states 2 conditions under which criminal penalties will be charged. The Minnesota Act authorizes criminal penalties for willful violations of any provision of the Act.

[* These steps are absolutely necessary in promulgating agency compliance, but are not stated in the Act. They are most likely implied. *]

SECTION 3-115 (Agency Implementation.)

Each agency shall:

(1) issue instructions and guidelines necessary to effectuate this Article, and

(2) take steps to assure that all its employees and officers responsible for the collection, maintenance, use, and dissemination of personal records are informed of the requirements of this Article and the requirements and procedures adopted by the agency pursuant to this Article.

15.163 continued

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 1. Annual inventory of records.
...The document shall be available from the responsible authority to the public in accordance with the provisions of sections 15.1621 and 15.17.

SECTION 3-116 continued

(b) The agency shall make the reports available for public inspection.

15.163 continued

[* The reporting requirements for the Minnesota Statutes is similar to the Code but much less comprehensive. The 1974 Minnesota Statutes was very comprehensive with regard to reports to the legislature. However, much of this information was amended out because the reporting requirements was felt to be too burdensome. There are about 3500 jurisdictions in Minnesota, so the paperwork generated would be overwhelming. *]

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 1. Annual inventory of records.
...containing his name, title and address...

SECTION 3-116 continued

(7) the agencies and categories of persons outside of the agency who routinely use the records;

(8) the individually identifiable records routinely used by the agency which are maintained by:

(i) another agency, or

(ii) a person other than an agency;

(9) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the information maintained in records;

(10) the title, business address, and business telephone number of the agency officer responsible for the records;

(11) the agency procedures whereby an individual can request access to personal records; and

(12) after the first year of operation under this Article, the number of written requests for access within the preceding year, the number denied, the number of lawsuits initiated against the agency under the Article, and the number of suits in which access was granted.

4.6.4 Annual Report of Records

15.163 DUTIES OF RESPONSIBLE AUTHORITY.

Subd. 1. Annual inventory of records.
The responsible authority shall prepare a public document...

Subd. 2. Copies to commissioner.
The commissioner may require responsible authorities to submit copies of the public document required in subdivision 1, and may request additional information relevant to data collection practices, policies and procedures.

Subd. 1. Annual inventory of records.
...and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by his state agency, statewide system, or political subdivision...

SECTION 3-116 (Report of Recordkeeping Policies and Practices.)

(a) Each agency shall compile a report each year describing the personal records it maintains. The report must be made available to the (Office of Information Practices) (Secretary of State) upon request. The report must include:

(1) the name and location of each set of records;

(2) the authority under which the records are maintained;

(3) the categories of individuals concerning whom records are maintained;

(4) the categories of information or data maintained in the records;

(5) the categories of sources of information in the records;

(6) the categories of uses and disclosures made of the records;

15.165 continued

15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 4.

...The determination of the responsible authority may be appealed pursuant to the provisions of the administrative procedure act relating to contested cases.

[* The Administrative Procedure Act is Chapter 15 of the Minnesota Statutes. The Minnesota Government Data Practices Act is part of the Administrative Procedures Act. See section 4.11.1. *]

SECTION 3-107 continued

(e) continued

(2) furnish a copy of the individual's statement; and

(3) furnish a concise statement of the agency's current position with respect to the request for correction or amendment and transmit a copy of this statement to the last known address of the individual whose record is disclosed.

(f) Each agency maintaining personal records shall take reasonable steps to provide statements of disagreement and corrections or amendments to all persons and agencies that have provided or received information concerning the disputed portions of the record within the preceding 3 years.

4.6.3 Correction and Amendment of Records

15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 4.
An individual may contest the accuracy or completeness of public or private data concerning himself...

Subd. 4.
...To exercise this right, an individual shall notify in writing the responsible authority describing the nature of the disagreement. The responsible authority shall within 30 days either:

(a) correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or

(b) notify the individual that he believes the data to be correct...

[* But why does he think it is correct? What can the individual do to contest the decision? The wording of this sentence is one-sided and in favor of the agency. *]

SECTION 3-107 (Correction and Amendment of Records; Propagation.)

(a) An individual may request an agency to correct or amend any incomplete or inaccurate information pertaining to him if it is contained in an accessible record and the record is available under section 3-105.

(b) Not later than 7 days after receiving a request from an individual in writing to correct or amend an accessible record pertaining to him, an agency shall:

(1) make the requested correction or amendment and inform the requester of the action;

(3) inform the requester in writing of its refusal to correct or amend the record as requested, the reason for the refusal, the agency procedures for review of the refusal by the head of the agency, and the name and position or title of the individual responsible for the refusal.

15.165 continued

15.165 RIGHTS OF SUBJECTS OF DATA.
Subd. 4.
...Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data...

SECTION 3-107 continued

(2) inform the requester that the agency does not maintain the record and, if it knows, provide the name and location of the agency maintaining it; or

(c) Not later than 30 days after an individual requests review of an agency's refusal to correct or amend his record, the agency shall make a final determination.

(d) If, after the review provided for by subsection (c) the agency refuses to correct or amend the record in accordance with the request, the agency shall:

(1) permit the requester to file with the record a concise statement of his reasons for the requested correction or amendment and for his reasons for disagreement with the agency's refusal; and

(2) notify the requester of his right to bring an action pursuant to section 3-112.

(e) Whenever an agency discloses information to a third party about which an individual has filed a statement pursuant to subsection (d), the agency shall:

(1) clearly identify the disputed portion of the information;

4.7.1 continued

15.166 continued

Subd. 4.
...In an action involving a request for government data under section 15.1621 or 15.165, the court may inspect in camera the government data in dispute, but shall conduct its hearing in public and in a manner that protects the security of data classified as not public.

Subd. 4.
In addition to the remedies provided in subdivisions 1 to 3 or any other law, any aggrieved person may bring an action in district court to compel compliance with sections 15.1611 to 15.1698 and may recover costs and disbursement, including reasonable attorney's fees, as determined by the court. If the court determines that an action brought under this subdivision is frivolous and without merit and a basis in fact, it may award reasonable costs and attorney fees to the responsible authority. The matter shall be heard as soon as possible.

[* Who can afford to bring a frivolous matter to court? The intentions of protecting the agency are understood, but perhaps unnecessary. *]

SECTION 3-112 continued

(c) In any action brought under this section alleging an agency's refusal to comply, in whole or in part, with a request for access under section 3-105, the court shall hear the matter de novo, may order the agency to disclose the records or account for the uses and disclosures thereof, and may order the production of any agency records or other information withheld from the requester. The court may examine the contents of any agency records in camera to determine whether the records or any portion therof may be withheld under section 3-106. The burden of proof is on the agency to establish the nondisclosability of a record.

(d) In any action brought under this section in which the court determines that the agency has violated any provision of sections 3-101 through 3-111, the claimant is entitled to recover from the agency damages sustained as a result of the violation; but he may not recover more than ($10,000) exclusive of any pecuniary loss. An officer or employee of an agency is not personally liable to the claimant for damages sustained as a result of a violation of this Article.

15.166 CIVIL PENALTIES.

Subd. 1.

Notwithstanding section 466.03, a political subdivision, responsible authority or state agency which violates any provision of sections 15.1611 to 15.1698 is liable to a person who suffers any damage as a result of the violation, and the person damaged may bring an action against the political subdivision, responsible authority, statewide system or state agency to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the political subdivision, statewide system or state agency shall, in addition, be liable to exemplary damages of not less than $100, nor more than $10,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under sections 15.1611 to 15.1698.

Subd. 2. A political subdivision, responsible authority, statewide system or state agency which violates or proposes to violate sections 15.1611 to 15.1698 may be enjoined by the district court. The court may make any order or judgment as may be necessary to prevent the use or employment by any person of any practices which violate sections 15.1611 to 15.1698.

SECTION 3-112 (Civil Remedies.)

(a) Any individual aggrieved by a violation of sections 3-101 through 3-111 with respect to his personal records may bring an action for relief as provided in this section.

(b) In an action brought under this section, the court shall hear the matter de novo, may order the agency to comply with this Article and to cease the unlawful practice or procedure, and may provide any other appropriate relief.

4.7.2 Judicial Enforcement

REPEAT
15.166 CIVIL PENALTIES.
Subd. 4.
...In an action involving a request for government data under section 15.1621 or 15.165, the court may inspect in camera the government data in dispute, but shall conduct its hearing in public and in a manner that protects the security of data classified as not public.

[* See section 4.7.1. *]

SECTION 2-104 (Judicial Enforcement.)

(a) A person aggrieved by a violation of section 2-101 or 2-102 may bring an action against the agency to compel disclosure. In an action to compel the agency to disclose a government record, the court shall hear the matter de novo. The court may examine the record at issue in camera to determine whether it or any part of it may be withheld. The agency has the burden of proof to establish the justification for non-disclosure, unless the record is non-disclosable under Article 3.

(b) If the complainant substantially prevails in an action brought under this section, the court may assess against the agency reasonable attorney's fees and all other expenses reasonably incurred in the litigation.

((c) The court in the (district) (judicial circuit) in which the requested record is maintained or the agency's headquarters are located has jurisdiction over an action brought under this section.)

15.166 continued

[* This sort of agency protection is not provided for in the Statutes. It is an issue which would arise frequently and should therefore be provided for in the Act. *]

Subd. 3.

An action filed pursuant to this section may be commenced in the county in which the individual alleging damage or seeking relief resides, or in the county wherein the political subdivision exists, or, in the case of the state, any county.

SECTION 3-112 continued

(e) An agency is entitled to indemnification from an employee or officer of the agency who:

(1) willfully discloses or provides a copy of an individually identifiable record to any person or agency not entitled to receive it; and

(2) has knowledge that disclosure is prohibited.

(f) If an individual substantially prevails in any action brought under this section, the court may assess against the agency reasonable attorney's fees and all other expenses reasonably incurred in the litigation.

(g) If an agency fails to comply with the time limits of sections 3-105 and 3-107, the requester may bring an action pursuant to this section.

15.167 PENALTIES.
...Willful violation of sections 15.162 to 15.1671 by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

15.167 PENALTIES.
Any person who willfully violates the provisions of sections 15.162 to 15.1671 or any lawful rules and regulations promulgated thereunder is guilty of a misdemeanor.

SECTION 2-105 (Disciplinary Action.)

An agency shall take disciplinary action, which may include suspension or discharge, against any officer or employee of the agency who knowingly and willingly violates any provision of this Article. Any other violation of this Article is cause for disciplinary action.

SECTION 3-113 (Disciplinary Action.)

(Exactly the same as SECTION 2-105 above except applies to Article 3)

SECTION 3-114 (Criminal Penalties.)

(a) An officer or employee of an agency or authorized recipient of records under section 3-109 (a) who willfully discloses or provides a copy of an individually identifiable record to any person or agency, with knowledge that disclosure is prohibited, is guilty of a (_____).

(b) A person who, by false pretenses, bribery or theft, gains access to or obtains a copy of an individually identifiable record whose disclosure is prohibited to him is guilty of a (_____).

SECTION 2-104 continued

[* Subsection (c) is optional. *]

(d) If the agency fails to comply with the time limits of section 2-102, the requester may bring an action under this section.

15.167 continued

SECTION 3-114 continued

[* COMMENT following SECTION 3-114 of the Code, pages 51-52.

Criminal provisions are contained occasionally in legislation similar to this Code. Some criminal provisions authorize sanctions for willful or purposeful violations of any provision of the Act. Minn. Stat. § 15.167 (1977); Ohio Rev. Code Ann. § 1347.99 (1980); Utah Code Ann. § 63-50-9 (1953). Others limit criminal penalties to knowing and willful violations of provisions that may be regarded as central to the privacy protection mechanism of the statute. Such statutes, almost without exception, single out disclosure of personal records to unauthorized persons and obtaining records by false pretenses or other unlawful means as the kinds of violations which warrant the extreme response of criminal prosecution...This section adopts the latter approach.

...This section does not establish a grade for these offenses. But among the existing statutes protecting the privacy of individual records, those which include criminal penalties treat such violations as misdemeanors not felonies. *]

4.8 CHANGE OF STATUS--TEMPORARY CLASSIFICATION

Since all government data is declared to be public unless otherwise stated, the mechanism used to classify data into 1 of the other 4 categories (i.e., private, confidential, nonpublic, or protected nonpublic) is the temporary classification procedure. This mechanism is absent in the Uniform Code because it is unnecessary for the agency to assign various classifications to all government records in order that certain types of persons can access the data. Rather, the burden of proof rests upon the agency head to justify why a particular record was or was not granted access.

The temporary classification process is efficient in the sense that all records of a particular category are immediately granted a change of status upon the commissioner's approval. However, this blanket coverage disregards situations where the disclosure of information is a very fine line between public and some other data classification. In other words, the responsible authority does not have to be very concerned about disclosing information on a case-by-case basis. It is these cases where individual invasions of personal privacy can occur, or where information is not disclosed when it would be in the public interest to disclose it.

Moreover, this process is time consuming. It might possibly take 90 days before the classification is determined. By that time, the information might not be needed.

4.8.1 Minnesota Statutes: Temporary Classification

15.1642 TEMPORARY CLASSIFICATION.

Subd. 1. Application.

Notwithstanding the provisions of section 15.1621, the responsible authority of a state agency, political subdivison or statewide system may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, or data not on individuals as non-public or protected non-public, for its own use and for the use of other similar agencies, political subdivisons until a proposed statute can be acted upon by the legislature. The application for temporary classification is public.

Upon the filing of an application for temporary classification, the data which is the subject of the application shall be deemed to be classified as set forth in the application for a period of 45 days, or until the application is disapproved or granted by the commissioner, whichever is earlier.

Subd. 2. Contents of application for private or confidential data.

An application for temporary classification of data on individuals shall include and the applicant shall have the burden of clearly establishing that no statute currently

[* This type of provision is unnecessary in the Code because a classification system does not exist. *]

It has also been noticed (particularly in the 1981 amendments) that it might be difficult to apply for a change in classification to one particular classification category. For example, in the categories of information which contain both data on individuals and data not on individuals, it is not clear in the Statutes how the responsible authority applies for a change of status for two classifications of data in one separate application.

4.10 RESEARCH RECORDS

The primary purpose in including provisions for research records in both acts is to safeguard individual privacy interests. Personal records which very frequently contain confidential information are oftentimes used and abused by researchers.

In interpreting the provisions, it is cautioned that the reader understand the definitions accorded the terms, "summary data," "research record," and "research purpose." In the Uniform Code, a research record is an individually identifiable record collected solely for a research purpose. It is not intended to be used in individually identifiable form, though, to reveal the identity of the individual. The Statutes do not have a definition comparable to research record. Summary data is not data on individuals. Although it is derived from the individually identifiable record, summary data is the tabulated results or records in a form which does not reveal the identity of the individual.

Thus, in the case of the Minnesota Statutes, all summary data is public. Even confidential or private data on individuals, which might not be revealed to the individual himself, can be disclosed to the requestor if these are put in the form of summary data. However, the provision allowing private or confidential data to be used for research purposes is, (1) either unclear; or it is (2) a personal abuse to

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 6. Contracts.
Except as provided in section 15.1691, subdivision 5, in any contract between a governmental unit subject to section 15.1611 to 15.1698 and any person, when the contract requires that data on individuals be made available to the contracting parties by the governmental unit, that data shall be administered consistent with sections 15.1611 to 15.1698. A contracting party shall maintain the data on individuals which it received according to the statutory provisions applicable to the data.

[* Provision (b) in the Code is not in the Statutes. The question arises as to who will enforce compliance. *]

[* See section 4.15.8.1. Concerns private health care providers under contract with an agency and exemption from revealing a requester's personal records from that requester. *]

SECTION 3-111 (Government Contractors and Grant Recipients.)

(a) Any contractor, grant recipient, or subcontractor of either, who performs any function of an agency that requires the contractor or grant recipient to maintain individually identifiable records is subject to sections 3-101 and 3-102 with respect to those records.

(b) The agency with which the contract or grant is established is responsible for assuring compliance with the provisions of this Article.

(c) For purposes of the civil remedies of section 3-112, a contractor or grant recipient is a separate agency and in that capacity is subject to injunctive or other relief, and is liable for damages, attorney's fees, and all other expenses reasonably incurred in the litigation.

(d) An official or employee of an agency may not obligate the agency to indemnify a contractor, grant recipient, or subcontractor of either, for losses suffered as a result of its liabilities under section 3-112.

4.9 GOVERNMENT CONTRACTORS

Contractors or grant recipients who contract with an agency are subject to the same provisions of the Act or the Code with regard to the handling of personal records. In effect, the contracting party becomes a separate agency instead of an appendage of the government agency. The major difference between the Code and the Act is that the agency has the responsibility in seeing that the contracting party complies with the provisions of the Code. As this is not stated in the Act, compliance is not ensured until an aggrieved individual contests the contracting party's practices in court.

When a private health care provider contracts with an agency of the welfare system in the Act, the provider does not have to disclose to the requester his own personal record. This restriction impinges upon an individual's right to gain access to his own medical record for welfare purposes.

[* Perhaps this may never be desired, but what are the procedures for declassifying data (e.g., change from private to public classification)? *]

15.1642 continued

Subd. 5. - continued

classifications. All temporary classifications granted under this section prior to the effective date of this act and still in effect, and all temporary classifications thereafter applied for and granted pursuant to this section shall expire on July 31, 1981 or 18 months after the classification is granted, whichever occurs later.

Subd. 5a. Legislative consideration and expiration of temporary classifications.
On or before January 15 of each year, the commissioner shall submit all temporary classifications in effect on January 1 in bill form to the legislature.

15.1621 ACCESS TO GOVERNMENT DATA.
Subd. 4.
The classification of data in the possession of an agency shall change if it is required to do so to comply with either judicial or administrative rules pertaining to the conduct of legal actions or with a specific statute applicable to the data in the possession of the disseminating or receiving agency.

Section 38. EXTENSION OF CERTAIN TEMPORARY CLASSIFICATIONS.
~~C~~ourt services data, criminal history data, and corrections and detention data classified by temporary classifications granted prior to January 1, 1981, pursuant to Minnesota Statutes, Section 15.1642, shall retain their temporary classification until July 1, 1982.

15.1642 continued

Subd. 2b. - continued

application within 20 days after it is filed. Five working days after the date of the commissioner's disapproval of the amended application, the data which is the subject of the application shall become public data. No more than one amended application may be submitted for any single file or system.

If the commissioner grants an application for temporary classification, it shall become effective immediately, and the complete record relating to the application shall be submitted to the attorney general, who shall review the classification as to form and legality. Within 25 days, the attorney general shall approve the classification, disapprove a classification as confidential but approve a classification as private, or disapprove the classification. If the attorney general disapproves a classification, the data which is the subject of the classification shall become public data five working days after the date of the attorney general's disapproval.

(M.S. 15.1642, Subd. 4, has been repealed.)

Subd. 5. Expiration of temporary classification.

Emergency classifications granted before July 1, 1979 are redesignated as temporary

15.1642 continued

Subd. 2b. - continued

is disapproved or granted by the commissioner, whichever is earlier. Proceedings after the grant or disapproval shall be governed by the provisions of subdivision 3.

Subd. 3. Determination.

The commissioner shall either grant or disapprove the application for temporary classification within 45 days after it is filed. If the commissioner disapproves the application, he shall set forth in detail his reasons for the disapproval, and shall include a statement of what classification he believes is appropriate for the data which is the subject of the application. Twenty days after the date of the commissioner's disapproval of an application, the data which is the subject of the application shall become public data, unless the responsible authority submits an amended application for temporary classification which requests the classification deemed appropriate by the commissioner in his statement of disapproval or which sets forth additional information relating to the original proposed classification. Upon the filing of an amended application, the data which is the subject of the amended application shall be deemed to be classified as set forth in the amended application for a period of 20 days or until the amended application is granted or disapproved by the commissioner, whichever is earlier. The commissioner shall either grant or disapprove the amended

15.1642 continued

Subd. 2b. - continued

intention by publication in the state register and by notification to the intergovernmental information systems advisory council, within ten days of receiving the application. Within 30 days after publication in the state register and notification to the council, an affected agency, political subdivision, the public, or statewide system may submit comments on the commissioner's proposal. The commissioner shall consider any comments received when granting or denying a classification for data of the kind which is the subject of the application, for the use of all agencies, political subdivisions, or statewide systems similar to the applicant. Within 45 days after the close of the period for submitting comment, the commissioner shall grant or disapprove the application. Applications processed under this subdivision shall be either approved or disapproved by the commissioner within 90 days of the receipt of the application. For purposes of subdivision 1, the data which is the subject of the classification shall be deemed to be classified as set forth in the application for a period of 90 days, or until the application is disapproved or granted by the commissioner, whichever is earlier. If requested in the application, or determined to be necessary by the commissioner, the data in the application shall be so classified for all agencies, political subdivisions, or statewide systems similar to the applicant until the application

15.1642 continued

Subd. 2a. continued

(b) Public access to the data would render unworkable a program authorized by law; or

(c) That a compelling need exists for immediate temporary classification, which if not granted could adversely affect the health, safety or welfare of the public.

[* It is not explained what the procedures are when the responsible authority holds information that is both data on individuals and data not on individuals. Two separate classifications are desired for 1 category of data. For instance, a number of statutes declare, "classified as private in the case of data on individuals and nonpublic in the case of data not on individuals." *]

Subd. 2b.

If the commissioner determines that an application for temporary classification involves data which would reasonably be classified in the same manner by all agencies, political subdivisions, or statewide systems similar to the one which made the application, the commissioner may approve or disapprove the classification for data of the kind which is the subject of the application for the use of all agencies, political subdivisions, or statewide systems similar to the applicant. If the commissioner deems this approach advisable, he shall provide notice of his

15.1642 continued

Subd. 2 - continued

exists which either allows or forbids classification as private or confidential; and either

(a) That data similar to that for which the temporary classification is sought has been treated as either private or confidential by other state agencies or political subdivisions, and by the public; or

(b) That a compelling need exists for immediate temporary classification, which if not granted could adversely affect the public interest or the health, safety, well being or reputation of the data subject.

Subd. 2a. Contents of application for nonpublic data.

An application for temporary classification of government data not on individuals shall include and the applicant shall have the burden of clearly establishing that no statute currently exists which either allows or forbids classification as nonpublic or protected nonpublic; and either

(a) That data similar to that for which the temporary classification is sought has been treated as nonpublic or protected nonpublic by other state agencies or political subdivisions, and by the public; or

15.163 DUTIES OF RESPONSIBLE AUTHORITY.
Subd. 7. Preparation of summary data.
The use of summary data derived from private or confidential data on individuals under the jurisdiction of one or more responsible authorities shall be permitted. Unless classified pursuant to section 15.1642, summary data is public. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person...

[* See also definition of summary data in section 4.3.1.4 and 4.3 summary. *]

[* Subsection (2) is an absolute must for researchers given the permission to compile the summary data themselves. The personal records must be destroyed after the research has been completed. *]

SECTION 3-109 (Disclosure of Individually Identifiable Records for Research Purposes; Limitations on Redisclosure.)

(a) An agency may disclose or authorize disclosure of an individually identifiable record for research purposes only if the agency:

(1) determines that the research purpose cannot reasonably be accomplished without use or disclosure of the information in individually identifiable form and the additional risk to individual privacy as a result of the disclosure will be minimal;

(2) receives adequate assurances that the recipient will establish the safeguards required by section 3-108(a)(6) and will remove or destroy the individual identifiers associated with the records as soon as the purpose of the research project has been accomplished;

privacy if the intended research purpose was never revealed to the individual when the data was first collected from the individual. The intended purpose for research must be included in the definition of summary data as it is included in the Uniform Code's definition.

Also, the researcher in M.S. 15.163, subd. 7, rather than the responsible authority, is allowed to compile the summary data himself. Merely obtaining the written purpose of research, along with the agreement not to disclose the data on individuals is inadequate.

The Uniform Code contains more safeguards for handling research records because, by definition, the research records are the individually identifiable records. They are not statistical records or reports. It is commendable that the Code establishes a provision for protecting the research subjects by not allowing the research records to be obtained for investigative purposes or as evidence to be used in a proceeding. Of course, this limitation on access can still be penetrated under the discovery process of a lawsuit.

SECTION 3-109 continued

(i) the audit or evaluation is expressly authorized by law, and

(ii) no subsequent use or disclosure of the record in individually identifiable form will be made by the auditor evaluator except as provided by this section; or

(3) the record is furnished in compliance with a search warrant or subpoena as provided in section 3-110(a).

15.163 continued

Subd. 7. Preparation of summary data. ...provided that the request is in writing and the cost of preparing the summary data is borne by the requesting person...

...The responsible authority may delegate the power to prepare summary data (1) to the administrative officer responsible for any central repository of summary data; or (2) to a person outside of its agency if the person, in writing, sets forth his purpose and agrees not to disclose, and the agency reasonably determines that the access will not compromise private or confidential data on individuals.

* The second provision (2) above should not be allowed unless more adequate measures are established relating to what is done with the personal records after the research is completed. Rules for subsequent use must also be promulgated. *

SECTION 3-109 continued

(3) secures from the recipient of the records a written statement of his understanding of and agreement to the conditions of this subsection; and

(4) prohibits any subsequent use or disclosure of the record in individually identifiable form without express authorization of the agency or the individual to whom the record pertains.

(b) A person or agency may use or disclose a research record only if:

(1) the person or agency reasonably believes that use or disclosure will prevent or minimize physical injury to an individual and the disclosure is limited to information necessary to protect the individual who has been or may be injured;

(2) the record is disclosed in individually identifiable form for the purpose of auditing or evaluating a research program and:

SECTION 3-110 (Research Records: Amenability to Compulsory Process; Researcher Privilege.)

(a) A court may issue a search warrant or subpoena concerning a research record only if the purpose of the warrant or subpoena is to assist inquiry into an alleged violation of law by a person using the record for a research purpose or by a person or agency maintaining the record.

[* The purpose of subsection (a) is to protect the confidentiality of research subjects. Search warrants and subpoenas may only be issued to investigate an alleged violation of the law by the researcher or the agency maintaining the record. Thus, research records may not be used to discover unlawful violations, etc. revealed by the research subjects for the research. *]

(b) Any research record obtained pursuant to subsection (a), as well as any information directly or indirectly derived from the record, may not be used as evidence in an administrative, judicial, or legislative proceeding except in a proceeding against the person using the record for a research purpose or a person or agency maintaining the record.

4.11 BODY TO OVERSEE THE CARRYING OUT OF THE STATUTES

Although the Minnesota Statutes does not establish an Office of Information Practices, Minnesota does have a Data Privacy Division to carry out the powers delegated to the commissioner of the department of administration. The major duties of the commissioner are to promulgate rules in conjunction with the intergovernmental information services advisory council; inform all agencies affected by the Data Practices Act about the Act; ensure that responsible authorities submit annual reports; grant or disapprove applications for temporary classification; and submit the temporary classifications to the legislature. The Data Privacy Division exists to carry out these functions.

In comparison, the director of the Office of Information Practices is delegated more powers. It can, for example, examine the records of an agency; conduct inquiries and investigations into possible violations of the Code; recommend disciplinary action or criminal prosecution to the officers of an agency; and bring action against another agency to compel compliance.

The authority to compel compliance is important. Otherwise, as in the Minnesota Statutes, the aggrieved citizen must alone compel compliance. This is a rather naive solution to the problem, for it pits person against agency. If granted the authority, the body to oversee the carrying out of the Statutes would be much more effective in seeing that the provisions of the Act are acted upon by all agencies.

4.11.2 Office of Information Practices
4.11.2.1 Appointment of director

(Article 4

Office of Information Practices

SECTION 4-101 (Organization; Appointment of Director.)

(a) The Office of Information Practices is created.

(b) The Governor shall appoint with the advice and consent of the (name of legislative body) a director of the Office of Information Practices who is its chief executive officer.

(c) All powers and duties of the Office of Information Practices are vested in the director.

(d) The director may delegate any of his powers and duties to any other officer or employee of the office.

[* REPEAT. (see section 4.8.1, Temporary Classification, subd. 1, subd. 2b., subd. 3, subd. 5a. for other references to commissioner's duties. *]

[* The intergovernmental information services advisory council was established by statute to advise the Commissioner in matters relating to the coordination of information systems. The general thrust of the council is to act in an advisory capacity. (Don Gemberling, Director, Data Privacy Division) *]

[* The administrative procedures act is Chapter 15 of the Minnesota Statutes. The Minnesota Government Data Practices Act is part of the Administrative Procedures Act. See section 4.6.3 for reference to this. *]

[* The Privacy Study Commission, whose purpose it was to examine data privacy issues and report to the legislature, became defunct on January 15, 1977. (Don Gemberling, Director, Data Privacy Division) *]

[* Why won't section 15.165 be affected and section 15.1621 (ACCESS TO GOVERNMENT DATA--public access), subd. 3, be affected? *]

REPEAT

15.163 DUTIES OF RESPONSIBLE AUTHORITY.

Subd. 2. Copies to commissioner.

The commissioner may require responsible authorities to submit copies of the public document required in subdivision 1, and may request additional information relevant to data collection practices, policies and procedures.

[* See section 4.6.4. *]

REPEAT
15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.
Subd. 2.
"Commissioner" means the commissioner of the department of administration.

[* See section 4.3.1.5. *]

15.1671 DUTIES OF THE COMMISSIONER.
The commissioner shall with the advice of the intergovernmental information services advisory council promulgate rules, in accordance with the rule-making procedures in the administrative procedures act which shall apply to state agencies, statewide systems and political subdivisions to implement the enforcement and administration of sections 15.162 to 15.169. The rules shall not affect section 15.165, relating to rights of subject of data, and section 15.169, relating to the powers and duties of the privacy study commission. Prior to the adoption of rules authorized by this section the commissioner shall give notice to all state agencies and political subdivisions in the same manner and in addition to other parties as required by section 15.0412, subdivision 3, of the date and place of hearing, enclosing a copy of the rules and regulations to be adopted.

SECTION 4-102 (Powers and Duties of the Office of Information Practices.)

(a) With respect to Article 2, (Freedom of Information), the Office of Information Practices:

(1) upon request by an agency, shall provide advisory guidelines, opinions, or other information concerning that agency's functions and responsibilities;

(2) upon request by any person, may provide advisory opinions or other information regarding that person's rights and the functions and responsibilities of agencies;

(3) may conduct inquiries regarding compliance by an agency and investigate possible violations by any officer or employee of any agency;

(4) may examine the records of any agency for the purpose of paragraph (3) and seek to enforce that power in the courts of this State;

(5) may recommend disciplinary action to appropriate officers of an agency;

(6) shall report annually to the Governor and the (name of legislative body) on the activities and findingsof the office, including recommendations for legislative changes; and

SECTION 4-102 continued

(7) shall receive complaints from and actively solicit the comments of the public regarding the implementation of the Article.

(b) With respect to Article 3, (Disclosure of Personal Records), the Office of Information Practices:

(1) shall review the official acts, records, policies and procedures of the officer designated for each agency pursuant to section 3-116(10);

(2) shall assist agencies in complying;

(3) upon request by an agency, shall provide (an) (a binding) interpretative ruling concerning any question arising under the Article;

(4) upon request by any person, may provide advisory opinions or other information regarding that person's rights and the functions and responsibilities of agencies;

(5) may conduct inquiries regarding agency compliance by an agency and investigate possible violations by any officer, employee, contractor, grant recipient, subcontractor or agent of any agency;

SECTION 4-102 continued

(iii) the right to know the purposes for which records pertaining to him are kept;

(iv) the right to be informed of the uses and disclosures of records pertaining to him;

(v) the right to correct or amend records pertaining to him; and

(vi) the right to place a statement in a record pertaining to him.

(c) The officer may bring an action against another agency, other than for damages, to enforce the provisions of this Code.)

SECTION 4-102 continued

(6) may examine the records of any agency for the purposes of paragraph (5) and seek to enforce that power in the courts of this State;

(7) may recommend disciplinary action or criminal prosecution to the appropriate officers of an agency;

(8) shall receive complaints from and actively solicit the comments of the public regarding the effectuation of the Article;

(9) report annually to the Governor and the (name of legislative body) summarizing the expressed complaints, comments and concerns;

(10) may conduct any other investigations and prepare and publish any other reports and recommendations necessary or desirable to protect an individual's right of privacy; and

(11) shall inform the public of the following rights of an individual and the procedures for exercising them:

(i) the right of access to records pertaining to him;

(ii) the right to obtain a copy of records pertaining to him;

4.12.1 Grant of Exemption

[* There exists no provision in the Act which would exempt any statewide system, agency, or political subdivision from the provisions of the Act. *]

Article 5

Exemptions

SECTION 5-101 (Grant of Exemption.)

(a) Pursuant to the administrative rule-making procedures of this State, the (Office of Information Practices) (Governor) may adopt rules under which it may exempt an agency from compliance with this Code.

(b) An (annual) exemption may be granted to an agency only if the (Office of Information Practices)(Governor) determines that the benefit to the agency from the exemption outweighs the public interest in full compliance with this Code.

(c) In determining whether to grant an exemption, the (Office of Information Practices) (Governor) shall consider, among other relevant factors:

(1) the number and type of government records that would be affected by the exemption;

(2) the probable number of requests for disclosure of government records to be received in a year by the agency requesting exemption; and

4.12 EXEMPTIONS

There exists no provision in the Minnesota Statutes which would exempt any statewide system, agency, or political subdivision from all or some of the provisions of the Act. Currently, the Uniform Code exempts two branches of government from the entire Code--the legislative and judicial branches of government. The provisions from which an agency can be exempted do not appear to impose a great burden upon the agency.. For instance, it was discussed in section 4.4.2 that an interpretation of section 2-102(c) is that the agency does not have to purchase duplicating facilities. Rather, the agency must establish procedures for dealing with the requester and for making copies of the requested information. The requirements of sections 2-102(f), and 3-116 also do not appear to pose a burden upon the agency to the extent that it should be exempted from the above requirements.

4.12.1 continued

SECTION 5-101 continued

(g) This section shall be strictly construed and an exemption may be granted only in a situation in which it is found impractical to require compliance.

[* COMMENT following SECTION 5-101 of the Code. "The benefit to the agency from the exemption must outweigh the public interest in full compliance with the sections for which an exemption is sought." *]

SECTION 5-101 continued

(3) the likelihood of an abuse of freedom of information or privacy interests that may result from the grant of the exemption.

(d) A grant of an exemption will relieve an agency from the duty to comply with:

(1) Section 2-102(c) to the extent that it requires the agency to provide access to facilities for duplication;

(2) Section 2-102(f) but the agency shall notify the requester in writing the reasons for its determination; and

(3) Sections 3-115 and 3-116.

[* Section 3-115 is with regard to agency implementation; section 3-116 concerns annual reports. *]

(e) Exemptions granted under this section must be general. Each exempt classification must be established on reasonable terms and must reasonably identify the agencies entitled to exemption. All agencies falling within a classification established for exemption are entitled to the exemption.

(f) An exemption must set forth the grounds upon which it is based.

Section 39. REVISOR'S INSTRUCTIONS.
The revisor of statutes shall codify the provisions of sections 1 to 44 and recodify the provisions of Minnesota Statutes 1980, Sections 15.1611 to 15.1699 in an appropriate place in the next edition of Minnesota Statutes. He shall also correct all statutory cross references to provisions of sections 15.1611 to 15.1699.

SECTION 4.13

REVISOR'S INSTRUCTIONS; REPEALER; EFFECTIVE DATE

Section 32. HOUSING AGENCY DATA.

Subd. 1. Definition.

For purposes of this section "housing agency" means the public housing agency or housing and redevelopment authority of a political subdivision.

Section 36. LAW ENFORCEMENT DATA.

Subd. 1. Application.

This section shall apply to agencies which carry on a law enforcement function, including but not limited to municipal police departments, county sheriff departments, fire departments, the bureau of criminal apprehension, the Minnesota state patrol and the securities and real estate division of the department of commerce.

Section 24. MEDICAL EXAMINER DATA.
Subd. 1. Definition.
As used in this section, "medical examiner data" means data relating to deceased individuals and the manner and circumstances of their death which is created, collected, used or maintained by a county coroner or medical examiner in the fulfillment of his official duties pursuant to chapter 390, or any other general or local law on county coroners or medical examiners.

Section 27. LICENSING DATA.
Subd. 1. Definition.
As used in this section "licensing agency" means any board, department or agency of this state which is given the statutory authority to issue professional or other types of licenses.

Section 29. BENEFIT DATA.
Subd. 1. Definition.
As used in this section, "benefit data" means data on individuals collected or created because an individual seeks information about becoming, is, or was an applicant for or a recipient of benefits or services provided under various housing, home ownership, and rehabilitation and community action agency programs administered by state agencies, political subdivisions, or statewide systems. Benefit data does not include welfare data which shall be administered in accordance with section 15.1691.

15.1695 CRIME REPORTS.
Subd. 1.
When collected, created, or maintained by law enforcement agencies including municipal police departments, county sheriff departments, fire departments, the bureau of criminal apprehension, the Minnesota state patrol or the peace officers standards and training board.

15.1698 MEDICAL DATA.
Subd. 1. Definition.
As used in this section:

(a) "Directory information" means name of the patient, date admitted, general condition, and date released.

(b) "Medical data" means data collected because an individual was or is a patient or client of a hospital, nursing home, medical center, clinic, health or nursing agency operated by a state agency or political subdivision including business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual.

Section 22. INVESTIGATIVE DATA.
Subd. 1. Definitions.
A "pending civil legal action" includes but is not limited to judicial, administrative or arbitration proceedings. Whether a civil legal action is pending shall be determined by the chief attorney acting for the state agency, political subdivision or statewide system.

15.1693 (1) continued

(b) "Student" includes a person currently or formerly enrolled or registered, and applicants for enrollment or registration at a public educational agency or institution.

(c) "Substitute teacher" means an individual who performs on a temporary basis the duties of the individual who made the record, but does not include an individual who permanently succeeds the maker of the record in his position.

15.1691 (1) continued

(c) "Welfare system" includes the department of public welfare, county welfare boards, human services boards, community mental health boards, state hospitals, state nursing homes, and persons, agencies, institutions, organizations and other entities under contract to any of the above agencies to the extent specified in the contract.

15.1692 PERSONNEL DATA.
Subd. 1.
As used in this section, "personnel data" means data on individuals collected because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with a state agency, statewide system or political subdivision or is a member of an advisory board or commission.

15.1693 EDUCATIONAL DATA.
Subd. 1.
As used in this section:

(a) "Educational data" means data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student.

15.1673 (1) continued

(c) "Labor relations information" means management positions on economic and non-economic items that have not been presented during the collective bargaining process or interest arbitration, including information specifically collected or created to prepare the management position.

15.1680 INVESTIGATIVE DETENTION DATA.
Subd. 1. Definition.
As used in this section, "investigative detention data" means government data created, collected, used or maintained by the state reformatories, prisons and correctional facilities, municipal or county jails, lockups, work houses, work farms and other correctional and detention facilities which: (a) if revealed, would disclose the identity of an informant who provided information about suspected illegal activities, and (b) if revealed, is likely to subject the informant to physical reprisals by others.

15.1691 WELFARE DATA.
Subd. 1. Definitions.
As used in this section:

(a) "Individual" means an individual pursuant to section 15.162, subdivision 4, but does not include a vendor of services.

(b) "Program" includes all programs for which authority is vested in a component of the welfare system pursuant to statute or federal law.

15.1673 GENERAL NONPUBLIC DATA.
Subd. 1.
As used in this section, the following terms have the meanings given them.

(a) "Security information" means government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.

(b) "Trade secret information" means government data, including a formula, pattern, compilation, program, device, method, technique or process (1) that was supplied by the affected individual or organization, (2) that is the subject of efforts by the individual or organization that are reasonable under the circumstances to maintain its secrecy, and (3) that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use.

4.14 DEFINITIONS PERTAINING TO SPECIFIC CATEGORIES OF DATA

Those definitions not stated up front in section 4.3 are listed in this section for easier access while reading section 4.15. The most striking feature of these definitions is that they are applicable only to a specific category of information. Also, they define the scope of that particular category of information. The scope of applicability, in terms of the situations or agencies to which the definition will apply, is very clear cut. It has to be. This is because each category of data that is defined in section 4.15 is an exception to the general rule. These exceptions are classified as either private, confidential, nonpublic or public. Thus, the scope of the agencies which are covered by these definitions must be well defined.

4.13.3 Minnesota Statutes: Effective Date

Section 41 EFFECTIVE DATE.
Sections 1 to 40 are effective the day following final enactment.

[* Sections 1 to 40 passed the Senate May 16, 1981. They passed the House of Representatives May 15, 1981. They were approved by Governor Albert H. Quie May 29, 1981. *]

4.13.2 Minnesota Statutes: Repealer

Section 40 REPEALER.

Minnesota Statutes 1980, Section 15.162, Subdivision 1a is repealed.

[* Section 15.162, subdivision 1a is as follows:

" 'Arrest information' shall include (a) the name, age, and address of an arrested individual; (b) the nature of the charge against the arrested individual; (c) the time and place of the arrest; (d) the identity of the arresting agency; (3) information as to whether an individual has been incarcerated and the place of incarceration. 'Arrest information' does not include data specifically made private, confidential or nonpublic pursuant to section 260.161 or any other statute. " *]

15.1694 ATTORNEYS

Notwithstanding the provisions of sections 15.162 to 15.17, the use, collection, storage, and dissemination of data by an attorney acting in his professional capacity for the state, a state agency or a political subdivision shall be governed by statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility; provided that this section shall not be construed to affect the applicability of any statute, other than sections 15.162 to 15.17, which specifically requires or prohibits disclosure of specific information by the attorney, nor shall this section be construed to relieve any responsible authority, other than the attorney, from his duties and responsibilities pursuant to sections 15.1611 to 15.17.

[* This statement is similar to section 4.5.5 whereby the Uniform Code states that other statutes will not be voided by the Code. Perhaps the Statutes should state this principle in lieu of always stating, "except pursuant to federal or state law..." *]

Section 35 continued

Subd. 2. Confidential data.
The following data created, collected and maintained by the office of the attorney general are classified as confidential, pursuant to section 15.162, subdivision 2a: data acquired through communications made in official confidence to members of the attorney general's staff where the public interest would suffer by disclosure of the data.

Subd. 3. Public data.
Data describing the final disposition of disciplinary proceedings held by any state agency, board or commission are classified as public, pursuant to section 15.162, subdivision 5b.

[* It is quite apparent that much of the above information could apply to all agencies--and not just the Attorney General's office. *]

[* See section 4.5.2 (SECTION 3-101, (4)). An individually identifiable record may be disclosed to the public if it is information contained in or compiled from a transcript, minutes, report, or summary of a proceeding open to the public. *]

Section 35 ATTORNEY GENERAL DATA.

Subd. 1. Private data.

The following data created, collected and maintained by the office of the attorney general are classified as private, pursuant to section 15.162, subdivision 5a:

(a) The record, including but not limited to, the transcript and exhibits of all disciplinary proceedings held by a state agency, board or commission, except in those instances where there is a public hearing;

[* See section 4.5.1. whereby information does not have to be disclosed if it is (1) communicated for the purpose of decision-making; or (2) would substantially inhibit the flow of ideas within an agency or impair the agency's decision-making processes. *]

(b) Communications and non-investigative files regarding administrative or policy matters which do not evidence final public actions;

(c) Consumer complaint data, other than that data classified as confidential, including consumers' complaints against businesses and follow-up investigative materials; and

(d) Investigative data, obtained in anticipation of, or in connection with litigation or an administrative proceeding where the investigation is not currently active.

[* See section 4.5.1. An exception to disclosure of information is that which is prepared in anticipation of litigation. *]

4.15 CATEGORIES OF INFORMATION

Specific categories of information, ranging from medical examiner data to library data, are listed in section 4.15. The purpose of these categories is to specify those types of information which are not public; and in turn, the new classification would limit access to a particular category of information in order to prevent disclosure of information to the public. Limited access would also protect the individual from personal privacy abuses.

The information classified as private, confidential, nonpublic, or protected nonpublic is quite detailed when compared with the guidelines or examples given in the Code. Each classification of data that a particular category of information is placed in must be very specific when describing what information will be included in the classification. Because it is an exception, the boundaries between public and one of the other classification groups must be well-defined.

What is the cause of the categories of information? These result from an agency's applying for a change of classification for that particular agency's data. Thus, the categories are delineated by agency or information type.

15.1673 GENERAL NONPUBLIC DATA.
Subd. 2. Classification.
The following government data is classified as nonpublic data with regard to data not on individuals, pursuant to section 15.162, subdivision 5c, and as private data with regard to data on individuals, pursuant to section 15.162, subdivision 5a: Security information, trade secret information, sealed absentee ballots prior to opening by an election judge, sealed bids prior to the opening of the bid, and labor relations information. Provided that specific labor relations information which relates to a specific labor organization is classified as protected nonpublic data pursuant to section 15.162, subdivision 5d.

[* Although this section is titled "General Nonpublic Data," it does not include all nonpublic data. See sections 4.15.7.4, 4.15.4, 4.15.7.3, 4.15.13, 4.15.17, 4.15.11, 4.15.7.2, 4.15.5.2 (c) for other nonpublic categories. Many are new amendments. *]

[* See section 4.5.1. Information jeopardizing the security of a record keeping system; proprietary information; or trade secret information does not have to be disclosed. *]

4.15.4 Federal Contracts Data

.15.1677 FEDERAL CONTRACTS DATA.
To the extent that a federal agency requires it as a condition for contracting with a state agency or political subdivision, all government data collected and maintained by the state agency or political subdivision because that agency contracts with the federal agency are classified as either private or nonpublic depending on whether the data are data on individuals or data not on individuals.

[* See section 4.5.1. It states that contract information is not required to be disclosed. *]

4.15.5 Law Enforcement Related Data
4.15.5.1 Section 15.1695 law enforcement data

15.1695 LAW ENFORCEMENT DATA.

Subd. 1. Crime reports.

(a) Data contained on incident complaint reports, variously called logs or dockets, comprising a chronological record of events, shall be public; provided that data on individuals which could reasonably be used to determine the identity of an undercover agent, informant, or victim of criminal sexual conduct shall be private data on individuals; provided further that any other data classified by law as private or confidential contained in incident complaint reports shall remain private or confidential data.

(b) Data in arrest warrant indices are classified as confidential pursuant to section 15.162, subdivision 2a, until the defendant has been taken into custody, served with a warrant, or appears before the court except when the law enforcement agency determines that the public purpose is served by making the information public.

(c) Data which uniquely describes stolen, lost, confiscated or recovered property or property described in pawn shop transaction records are classified as either private or nonpublic depending on the content of the specific data.

[* Section 4.5.1 does not require disclosure of this information (which would identify a confidential informant). Notice how all the exceptions must be stated in the Statutes; whereas the Code just provides a rough guideline. *]

15.1695 continued

(d) To the extent that the release of program data would reveal the identity of an informant or adversely affect the integrity of the fund, financial records of a program which pays rewards to informants shall be protected nonpublic data in the case of data not on individuals or confidential data in the case of data on individuals.

Subd. 2.

Nothing in this chapter shall prohibit the exchange of information by law enforcement agencies provided the exchanged information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation.

[* The Statutes allow inter-agency transfers of private or confidential data if it is stated by law. This Statute gives law enforcement agencies freedom in exchanging information. *]

Subd. 3.

Information reflecting deliberative processes or investigative techniques of law enforcement agencies is confidential; provided that information, reports, or memoranda which have been adopted as the final opinion or justification for decision of a law enforcement agency are public.

[* See section 4.5.4 (SECTION 3-103 (3)(i)) for inter-agency disclosures for law enforcement purposes. *]

[* See section 4.5.2 (1) for information which does not have to be disclosed. There is some overlap with sections 4.5.4 and 4.5.1. *]

[* See section 4.5.1 which does not require the disclosure of information which would reveal confidential investigative techniques. The agency decides whether to disclose the information. The Statutes definitely prohibit disclosure. *]

15.1695 continued

Subd. 4.

Nothing in this section shall be held to expand or limit the scope of discovery available at law to any party in a civil, criminal, or administrative proceeding.

Section 36 LAW ENFORCEMENT DATA.
Subd. 2. Arrest data.
The following data created or collected by law enforcement agencies which documents any actions taken by them to cite, arrest, incarcerate or otherwise substantially deprive an adult individual of his liberty shall be public at all times in the originating agency:

(a) Time, date and place of the action;
(b) Any resistance encountered by the agency;
(c) Any pursuit engaged in by the agency;
(d) Whether any weapons were used by the agency or other individual;
(e) The charge, arrest or search warrants, or other legal basis for the action;
(f) The identities of the agencies, units within the agencies and individual persons taking the action;
(g) Whether and where the individual is being held in custody or is being incarcerated by the agency;
(h) The date, time and legal basis for any transfer of custody and the identity of the agency or person who received custody;
(i) The date, time and legal basis for any release from custody or incarceration;
(j) The name, age, sex and last known address of an adult person or the age and sex of any juvenile person cited, arrested, incarcerated or otherwise substantially deprived of his liberty;

Section 36 (2) continued

(k) Whether the agency employed wiretaps or other eavesdropping techniques, unless the release of this specific data would jeopardize an ongoing investigation;

(l) The manner in which the agencies received the information that led to the arrest and the names of individuals who supplied the information unless the identities of those individuals qualify for protection under subdivision 9; and

(m) Response or incident report number.

Subd. 3. Request for service data.

The following data created or collected by law enforcement agencies which documents requests by the public for law enforcement services shall be public government data:

(a) The nature of the request or the activity complained of;

(b) The name and address of the individual making the request unless the identity of the individual qualifies for protection under subdivision 9;

(c) The time and date of the request or complaint; and

(d) The response initiated and the response or incident report number.

Subd. 4. Response or incident data.

The following data created or collected by law enforcement agencies which documents the agency's response to a request for service or which describes actions taken by the

Section 36 (4) continued

agency on its own initiative shall be public government data:

(a) Date, time and place of the action;
(b) Agencies, units of agencies and individual agency personnel participating in the action unless the identities of agency personnel qualify for protection under subdivision 9;
(c) Any resistance encountered by the agency;
(d) Any pursuit engaged in by the agency;
(e) Whether any weapons were used by the agency or other individuals;
(f) A brief factual reconstruction of events associated with the action;
(g) Names and addresses of witnesses to the agency action or the incident unless the identity of any witness qualifies for protection under subdivision 9;
(h) Names and addresses of any victims or casualties unless the identities of those individuals qualify for protection under subdivision 9;
(i) The name and location of the health care facility to which victims or casualties were taken; and
(j) Response or incident report number.

Subd. 5. Data collection.
Except for the data defined in subdivisions 2,3, and 4, investigative data

Section 36 (5) continued

collected or created by a law enforcement agency in order to prepare a case against a person, whether known or unknown, for the commission of a crime or civil wrong is confidential while the investigation is active. Inactive investigative data is public unless the release of the data would jeopardize another ongoing investigation or would reveal the identity of individuals protected under subdivision 9. Photographs which are part of inactive investigative files and which are clearly offensive to common sensibilities are classified as private data, provided that the existence of the photographs shall be disclosed to any person requesting access to the inactive investigative file. An investigation becomes inactive upon the occurrence of any of the following events:

(a) A decision by the agency or appropriate prosecutorial authority not to pursue the case;

(b) Expiration of the time to bring a charge or file a complaint under the applicable statute of limitations; or

(c) Exhaustion of or expiration of all rights of appeal by an individual convicted on the basis of the investigative data.

Any investigative data presented as evidence in court shall be public. Data determined to be inactive under clause (a) of this subdivision may become active if the agency or appropriate prosecutorial authority decides to renew the investigation.

[* See section 4.5.3 where information compiled as part of an investigation is an example of information being of significant privacy interest to the individual. *]

Section 36 (5) continued

During the time when an investigation is active, any person may bring an action in the district court located in the county where the data is being maintained to authorize disclosure of investigative data. The court may order that all or part of the data relating to a particular investigation be released to the public or to the person bringing the action. In making the determination as to whether investigative data shall be disclosed, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the agency or to any person identified in the data. The data in dispute shall be examined by the court in camera.

Subd. 6. Withholding public data.
A law enforcement agency may temporarily withhold response or incident data from public access if the agency reasonably believes that public access would be likely to endanger the physical safety of an individual or cause the perpetrator to flee, evade detection or destroy evidence. In such instances, the agency shall, upon the request of any person, provide a statement which explains the necessity for its action. Any person may apply to a district court for an order requiring the agency to release the data being withheld. If the court determines that the agency's action is not reasonable, it shall order the release of the data and may award costs and attorney's fees to the person who sought the order. The data in dispute shall be examined by the court in camera.

[* See section 4.5.2. An exception to disclosure of information is when it would endanger the life of an individual. *]

Section 36 continued

Subd. 7. Public benefit data.
Any law enforcement agency may make any data classified as confidential pursuant to subdivision 5 accessible to any person, agency or the public if the agency determines that the access will aid the law enforcement process, promote public safety or dispel widespread rumor or unrest.

Subd. 8. Public access.
When data is classified as public under this section, a law enforcement agency shall not be required to make the actual physical data available to the public if it is not administratively feasible to segregate the public data from the confidential. However, the agency must make the information described as public data available to the public in a reasonable manner. When investigative data becomes inactive, as described in subdivision 5, the actual physical data associated with that investigation, including the public data, shall be available for public access.

[* This is an interesting provision. This is the first mention of ability to access data, but it only applies to the law enforcement category of data. Why isn't this expressed in the general public access section, 4.4.2? *]

[* Defining an accessible record similar to that in the Uniform Code would apply to this situation. *]

Section 36 continued

Subd. 9. Protection of identities. A law enforcement agency may withhold public access to data on individuals to protect the identity of individuals in the following circumstances:

[* This subdivision is constructed very similarly to section 4.5.1 because the law enforcement agency is able to decide if information should be withheld. *]

(a) When access to the data would reveal the identity of an undercover law enforcement officer;

(b) When access to the data would reveal the identity of a victim of criminal sexual conduct;

(c) When access to the data would reveal the identity of a paid or unpaid informant being used by the agency if the agency reasonably determines that revealing the identity of the informant would threaten the personal safety of the informant; or

(d) When access to the data would reveal the identity of a victim of or witness to a crime if the victim or witness specifically requests that his identity not be revealed, and the agency reasonably determines that revealing the identity of the victim or witness would threaten the personal safety or property of the individual.

[* See section 4.5.1 whereby the agency does not have to disclose information which would identify a confidential informant. *]

[* See section 4.5.1--exceptions to disclosure. *]

Section 36 continued

Subd. 10. Data retention.
Nothing in this section shall require law enforcement agencies to create, collect or maintain data which is not required to be created, collected or maintained by any other applicable rule or statute.

[* This is repetitious of section 4.6.1 concerning the general collection of data, with the exception that it applies solely to the category of law enforcement data. *]

Section 22 INVESTIGATIVE DATA.
Subd. 2. Civil actions.
Data collected by state agencies, political subdivisions or statewide systems as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action, or which are retained in anticipation of a pending civil legal action, are classified as protected nonpublic data pursuant to section 15.162, subdivision 5d in the case of data not on individuals and confidential pursuant to section 15.162, subdivision 2a in the case of data on individuals.

[* See section 4.5.1. An exception to information disclosed is that which is prepared in anticipation of litigation.*]

4.15.5.4 Data access for crime victims

15.1696 DATA ACCESS FOR CRIME VICTIMS. The prosecuting authority shall release investigative data collected by a law enforcement agency to the victim of a criminal act or his legal representative upon written request unless the prosecuting authority reasonably believes:

(a) That the release of that data will interfere with the investigation; or

(b) That the request is prompted by a desire on the part of the requester to engage in unlawful activities.

[* This enables the authority to make subjective judgment similar to the Uniform Code. *]

[* Section 4.5.2 (SECTION 2-103) does not require disclosure of information that would impair the effectiveness of an ongoing investigation. *]

4.15.5.5 Investigative detention data

15.1680 INVESTIGATIVE DETENTION DATA.
Subd. 2. General.
Investigative detention data is confidential and shall not be disclosed except:

(a) Pursuant to section 15.163 or any other statute;

(b) Pursuant to a valid court order; or

(c) To a party named in a civil or criminal proceeding, whether administrative or judicial, to the extent required by the relevant rules of civil or criminal procedure.

Section 33 CORRECTIONS OMBUDSMAN DATA.

Subd. 1. Private data.

The following data maintained by the ombudsman for corrections are classified as private, pursuant to section 15.162, subdivision 5a:

(a) All data on individuals pertaining to contacts made by clients seeking the assistance of the ombudsman, except as specified in subdivisions 2 and 3;

(b) Data recorded from personal and phone conversations and in correspondence between the ombudsman's staff and persons interviewed during the course of an investigation;

(c) Client index cards;

(d) Case assignment data; and

(e) Monthly closeout data.

Subd. 2. Confidential data.

The following data maintained by the ombudsman are classified as confidential, pursuant to section 15.162, subdivision 2a: the written summary of the investigation to the extent it identifies individuals.

[* See section 4.5.3 where information compiled as part of an investigation is an example of information that is of significant privacy to the individual. *]

Section 33 continued

Subd. 3. Public data.
The following data maintained by the ombudsman are classified as public, pursuant to section 15.162, subdivision 5b: client name, client location; and the inmate identification number assigned by the department of corrections.

4.15.5.7 Domestic abuse data

Section 23 DOMESTIC ABUSE DATA.

All government data on individuals which is collected, created, received or maintained by police departments, sheriffs' offices or clerks of court pursuant to the domestic abuse act, section 518B.01, are classified as confidential data, pursuant to section 15.162, subdivision 2a, until a temporary court order made pursuant to subdivisions 5 or 7 of section 518B.01 is executed or served upon the data subject who is the respondent to the action.

[* See section 4.5.3 concerning instances which may be of significant privacy interest to the individual. *]

Section 20 FIREARMS DATA.

All data pertaining to the purchase or transfer of firearms and applications for permits to carry firearms which are collected by state agencies, political subdivisions or statewide systems pursuant to sections 624.712 to 624.718 are classified as private, pursuant to section 15.162, subdivision 5a.

15.1678 PROPERTY COMPLAINT DATA.

The names of individuals who register complaints with state agencies or political subdivisions concerning violations of state laws or local ordinances concerning the use of property are classified as confidential, pursuant to section 15.162, subdivision 2a.

Section 24 MEDICAL EXAMINER DATA.
Subd. 2. Public data.
Unless specifically classified otherwise by state statute or federal law, the following data created or collected by a medical examiner or coroner on a deceased individual is public: name of the deceased; date of birth; date of death; address; sex; race; citizenship; height; weight; hair color; eye color; build; complexion; age, if known, or approximate age; identifying marks, scars and amputations; a description of the decedent's clothing; marital status; location of death including name of hospital where applicable; name of spouse; whether or not the decedent ever served in the armed forces of the United States; social security number; occupation; business; father's name; mother's maiden name; birthplace; birthplace of parents; cause of death; causes of cause of death; whether an autopsy was performed and if so, whether it was conclusive; date and place of injury, if applicable, including work place; how injury occurred; whether death was caused by accident, suicide, homicide, or was of undetermined cause; certification of attendance by physician; physician's name and address; certification by coroner or medical examiner; name and signature of coroner or medical examiner;

Section 24 (2) continued

type of disposition of body; burial place name and location, if applicable; date of burial, cremation or removal; funeral home name and address; and name of local register or funeral director.

Section 24 continued

Subd. 3. Unidentified individual: public data.
Whenever a county coroner or medical examiner is unable to identify a deceased individual subject to his investigation, he may release to the public any relevant data which would assist in ascertaining identity.

Subd. 4. Confidential data.
Data created or collected by a county coroner or medical examiner which is part of an active investigation mandated by Minnesota Statutes, Chapter 390, or any other general or local law relating to coroners or medical examiners is confidential data on individuals pursuant to Minnesota Statutes, Section 15.162, Subdivision 2a, until the completion of the coroner's or medical examiner's final summary of his findings at which point the data collected in the investigation and the final summary thereof shall become private data on individuals, except that nothing in this subdivision shall be construed to make private or confidential the data elements identified in subdivision 2 at any point in the investigation or thereafter.

Subd. 5. Private data.
All other medical examiner data on deceased individuals is private pursuant to Minnesota Statutes, Section 15.162, Subdivision 5a, and shall not be disclosed except pursuant to the provisions of Minnesota Statutes, Chapter 390, or any other general or local law on county coroners or medical examiners, or pursuant to a valid court order.

Section 24 continued

Subd. 6. Other data.
Unless a statute specifically provides a different classification, all other data created or collected by a county coroner or medical examiner that is not data on deceased individuals or the manner and circumstances of their death is public pursuant to Minnesota Statutes, Section 15.1621.

Subd. 7. Court review.
Any person may petition the district court located in the county where medical examiner data is being maintained to authorize disclosure of private or confidential medical examiner data. The petitioner shall notify the medical examiner or coroner. The court may notify other interested persons and require their presence at a hearing. A hearing may be held immediately if the parties agree, and in any event shall be held as soon as practicable. After examining the data in camera, the court may order disclosure of the data if it determines that disclosure would be in the public interest.

Subd. 8. Access to private data.
The data made private by this section shall be accessible to the legal representative of the decedent's estate or to the decedent's surviving spouse or next of kin or their legal representative.

[* See section 4.5.2 (SECTION 3-101 (7)). Although an individually identifiable record may not be disclosed to any other person other than the individual to whom the record pertains, an exception is pursuant to a court order. However, the agency shall notify the individual to whom the record refers. *]

Section 24 continued

[* In Minneapolis Star and Tribune Company v. State and Others, a Minnesota Attorney General determined that: "...any member of the public is entitled to inspect whatever records the Board (of Medical Examiners) maintains regarding disciplinary action taken against a member of the medical profession and the reasons stated therefor, provided the inspection is limited to documents which do not contain privileged or confidential information." 9 *]

4.15.7 Personnel Related Data
4.15.7.1 Personnel data

15.1692 PERSONNEL DATA.
Subd. 2.

Except for employees described in subdivision 6, the following personnel data on current and former employees, volunteers and independent contractors of a state agency, statewide system or political subdivision and members of advisory boards or commissions is public: name; actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary; job title; job description; education and training background; previous work experience; date of first and last employment; the status of any complaints or charges against the employee, whether or not the complaint or charge resulted in a disciplinary action; and the final disposition of any disciplinary action and supporting documentation; work location; a work telephone number; badge number; and, city and county of residence.

[* See section 4.5.2 (SECTION 3-101 (1)). An exception where individually identifiable records may be disclosed to the public is the name, compensation, job title, business address, business telephone number, job description, education and training background, previous work experience or dates of first and last employment of present or former officers or employees of the agency. This is much less comprehensive than the personal data which can be disclosed in the Statutes. Notice the levels of detail for the Code and the Statutes. *]

15.1692 continued

Subd. 3. Public employment.
Except for applicants described in subdivision 6, the following personnel data on current and former applicants for employment by a state agency, statewide system or political subdivision is public: veteran status; relevant test scores; rank on eligible list; job history; education and training; and work availability. Names of applicants shall be private data except when certified as eligible for appointment to a vacancy or when applicants are considered by the appointing authority to be finalists for a position in public employment. For purposes of this subdivision, "finalist" means an individual who is selected to be interviewed by the appointing authority prior to selection.

Subd. 5.
All other personnel data is private data on individuals, except pursuant to a valid court order.

Subd. 6
All personnel data maintained by any state agency, statewide system or political subdivision relating to an individual employed as or an applicant for employment as an undercover law enforcement officer is private data on individuals.

[* See section 4.5.1--unwarranted invasion of privacy. *]

15.1692 continued

Subd. 7. Access by labor organizations. Personnel data may be disseminated to labor organizations to the extent that the responsible authority determines that the dissemination is necessary to conduct elections, notify employees of fair share fee assessments, and implement the provisions of chapter 179. Personnel data shall be disseminated to labor organizations and to the bureau of mediation services to the extent the dissemination is ordered or authorized by the director of the bureau of mediation services.

Section 34. EMPLOYEE RELATIONS DATA. The following data collected, created or maintained by the department of employee relations are classified as nonpublic pursuant to section 15.162, subdivision 5c:

(a) The commissioner's plan prepared by the department, pursuant to section 3.855, which governs the compensation and terms and conditions of employment for employees not covered by collective bargaining agreements until the plan is submitted to the legislative commission on employee relations;

(b) Data pertaining to grievance or interest arbitration that has not been presented to the arbitrator or other party during the arbitration process; and

(c) Notes and preliminary drafts of reports prepared during personnel investigations and personnel management reviews of state departments and agencies.

Section 25 WORKERS' COMPENSATION SELF-INSURANCE DATA.

Financial data relating to nonpublic companies which are submitted to the commissioner of insurance for the purpose of obtaining approval to self-insure workers' compensation liability as a group are classified as nonpublic data, pursuant to section 15.162, subdivision 5c.

Section 19 SALARY BENEFIT SURVEY DATA. Salary and personnel benefit survey data purchased from consulting firms, nonprofit corporations or associations or obtained from employers with the written understanding that the data shall not be made public which is maintained by state agencies, political subdivisions or statewide systems are classified as nonpublic pursuant to section 15.162, subdivision 5c.

4.15.8 Welfare and Social Program Related Data
4.15.8.1 Welfare data

15.1691 WELFARE DATA.

Subd. 2. General.

Unless the data is summary data or a statute specifically provides a different classification, data on individuals collected, maintained, used or disseminated by the welfare system is private data on individuals, and shall not be disclosed except:

(a) Pursuant to section 15.163;

(b) Pursuant to a valid court order;

(c) Pursuant to a statute specifically authorizing access to the private data;

(d) To an agent of the welfare system, including appropriate law enforcement personnel, who are acting in the investigation, prosecution, criminal or civil proceeding relating to the administration of a program;

(e) To personnel of the welfare system who require the data to determine eligibility, amount of assistance, and the need to provide services of additional programs to the individual;

(f) To administer federal funds or programs; or

(g) Between personnel of the welfare system working in the same program.

[* See section 4.5.3 for cases which are of significant privacy interest to the individual. *]

[* See section 4.5.3 where information relating to an individual's eligibility for social services is an example of information of significant privacy interest to the individual. *]

15.1691 continued.

Subd. 3. Investigative data.
Data on persons including data on vendors of services, which is collected, maintained, used or disseminated by the welfare system in an investigation, authorized by statute and relating to the enforcement of rules or law, is confidential pursuant to section 15.162, subdivision 2a, and shall not be disclosed except:

(a) Pursuant to section 15.163:

(b) Pursuant to statute or valid court order;

(c) To a party named in a civil or criminal proceeding, administrative or judicial, for preparation of defense.

The data referred to in this subdivision shall be classified as public data upon its submission to a hearing examiner or court in an administrative or judicial proceeding.

Subd. 4. Licensing data.
All data pertaining to persons licensed or registered under the authority of the commissioner of public welfare, except for personal and personal financial data submitted by applicants and licensees under the home day care program and the family foster care program, is public data. Personal and personal financial data on home day care program and family foster care program applicants and licensees is private data pursuant to section 15.162, subdivision 5a.

[* See section 4.5.3 for individual privacy interest situations. *]

15.1691 continued

Subd. 5. Medical data; contracts.
Data relating to the medical, psychiatric or mental health of any person, including diagnosis, progress charts, treatment received, case histories, and opinions of health care providers, which is collected, maintained, used or disseminated by a private health care provider under contract to any agency of the welfare system is private data on individuals, and is subject to the provisions of sections 15.162 to 15.1671, and this section, except that the provisions of section 15.165, subdivision 3, shall not apply. Access to medical data referred to in this subdivision by the individual who is the subject of the data is subject to the provisions of section 144.335.

Subd. 6. Other data.
Data collected, used, maintained or disseminated by the welfare system that is not data on individuals is public pursuant to sections 15.1621 and 15.17.

[* See section 4.5.3, which gives an example of medical data of significant privacy interest to the individual. *]

Section 21 SOCIAL RECREATIONAL DATA. The following data collected and maintained by political subdivisions for the purpose of enrolling individuals in recreational and other social programs are classified as private, pursuant to section 15.162, subdivision 5a: data which describes the health or medical condition of the individual, family relationships and living arrangements of an individual or which are opinions as to the emotional makeup or behavior of an individual.

[* See section 4.5.3. It lists medical data as being of significant privacy interest to the individual. *]

15.1699 EMPLOYEE ASSISTANCE DATA.

All data created, collected or maintained by any state agency or political subdivision to administer employee assistance programs similar to the one authorized by section 16.02, subdivision 28, are classified as private, pursuant to section 15.162, subdivision 5a.

Section 28 FOSTER CARE DATA.

The following data collected, created and maintained by a community action agency in a study of the impact of foster care policies on families are classified as confidential data, pursuant to section 15.162, subdivision 2a: names of persons interviewed; foster care placement plans obtained from other public and private agencies; and all information gathered during interviews with study participants.

Section 29 BENEFIT DATA.

Subd. 2. Public data.

The names and addresses of applicants for and recipients of benefits characterized as the urban homesteading, home ownership, and new housing programs operated by a housing and redevelopment authority in a city of the first class are classified as public data on individuals.

Subd. 3. Private data.

Unless otherwise provided by law, all other benefit data is private data on individuals, except pursuant to a valid court order.

[* See section 4.5.3 which gives examples of information of significant privacy interest to the individual. *]

4.15.9 Medical and Health Related Data
4.15.9.1 Medical data

15.1698 MEDICAL DATA.
Subd. 3. Public hospitals; directory information.
If a person is a patient in a hospital operated by a state agency or political subdivision pursuant to legal commitment, directory information is public data. If a person is a patient other than pursuant to a commitment in a hospital controlled by a state agency or political subdivision, directory information is public data unless the patient requests otherwise, in which case it is private data on individuals.

Directory information about an emergency patient who is unable to communicate which is public under this subdivision shall not be released until a reasonable effort is made to notify the next of kin. Although an individual has requested that directory information be private, the hospital may release directory information to a law enforcement agency pursuant to a lawful investigation pertaining to that individual.

[* See section 4.5.4. Medical data, with the exception of directory information, holds a significant privacy interest to the individual. *]

15.1698 continued

Subd. 4. Classification of medical data. Unless the data is summary data or a statute specifically provides a different classification, medical data are private but are available only to the subject of the data as provided in section 144.335, and shall not be disclosed to others except:

(a) Pursuant to section 15.163;

(b) Pursuant to a valid court order;

(c) To administer federal funds or programs;

(d) To the surviving spouse or next of kin of a deceased patient or client;

(e) To communicate a patient's or client's condition to a family member or other appropriate person in accordance with acceptable medical practice, unless the patient or client directs otherwise; or

(f) As otherwise required by law.

Section 31 HEALTH DATA.

Subd. 1. Private data.

The following data created, collected and maintained by the department of health, political subdivisions, or statewide systems are classified as private, pursuant to section 15.162, subdivision 5a: data on individual patients pertaining to the investigation and study of non-sexually transmitted diseases, except that the data may be made public to diminish a threat to the public health.

Subd. 2. Confidential data.

The following data created, collected and maintained by a department of health operated by the state or a political subdivision are classified as confidential, pursuant to section 15.162, subdivision 2a: investigative files on individuals maintained by the department in connection with the epidemiologic investigation of sexually transmitted diseases, provided that information may be released to the individual's personal physician and to a health officer, as defined in Minnesota Statutes, Section 145.01, for the purposes of treatment, continued medical evaluation and control of the disease.

[* See section 4.5.3 Medical data is an example given of a possible invasion of an individual's personal privacy. *]

Section 18 PUBLIC SAFETY DATA.

The following data collected and maintained by the state department of public safety are classified as private, pursuant to section 15.162, subdivision 5a: medical data on driving instructors, licensed drivers, and applicants for parking certificates and special license plates issued to physically handicapped persons. The following data collected and maintained by the state department of public safety are classified as confidential, pursuant to section 15.162, subdivison 2a: data concerning an individual's driving ability when that data is received from a member of the individual's family.

15.1693 EDUCATIONAL DATA.
Subd. 1.
As used in this section:

...Records of instructional personnel which are in the sole possession of the maker thereof and are not accessible or revealed to any other individual except a substitute teacher, and are destroyed at the end of the school year, shall not be deemed to be government data.

Records of a law enforcement unit of a public educational agency or institution which are maintained apart from education data and are maintained solely for law enforcement purposes, and are not disclosed to individuals other than law enforcement officials of the jurisdiction are confidential; provided, that education records maintained by the educational agency or institution are not disclosed to the personnel of the law enforcement unit.

Records relating to a student who is employed by a public educational agency or institution which are made and maintained in the normal course of business, relate exclusively to the individual in that individual's capacity as an employee, and are not available for use for any other purpose are classified pursuant to section 15.1692.

15.1693 continued

Subd. 1a. Student health data.
Health data concerning students, including but not limited to, data concerning immunizations, notations of special physical or mental problems and records of school nurses; and pupil census data, including but not limited to, emergency information, family information and data concerning parents shall be considered educational data. Access by parents to student health data shall be pursuant to section 15.162, subdivision 4.

Subd. 2.
Except as provided in subdivision 4, educational data is private data on individuals and shall not be disclosed except as follows:

(a) Pursuant to section 15.163;
(b) Pursuant to a valid court order;
(c) Pursuant to a statute specifically authorizing access to the private data;
(d) To disclose information in health and safety emergencies pursuant to the provisions of 20 U.S.C., Section 1232g(b)(1)(I) and 45 C.F.R., Section 99.36 which are in effect on July 1, 1979; or
(e) Pursuant to the provisions of 20 U.S.C., Sections 1232g(b)(I), (b)(4)(A), (b)(4)(B), (b)(1)(B), (b)(3) and 45 C.F.R., Sections 99.31, 99.32, 99.33, 99.34 and 99.35 which are in effect on July 1, 1979; or
(f) To appropriate health authorities but only to the extent necessary to administer immunization programs.

[* See section 4.5.3, which lists medical data as being of significant privacy interest to the individual. *]

15.1693 continued

Subd. 3.
A student shall not have the right of access to private data provided in section 15.165, subdivision 3, as to financial records and statements of his parents or any information contained therein.

Subd. 4. Information designated as public.
Information designated as directory information pursuant to the provisions of 20 U.S.C., Section 1232g and regulations adopted pursuant thereto which are in effect on July 1, 1979 is public data on individuals.

[* See section 4.5.3 where information describing an individual's finances is of significant privacy interest. *]

Section 32 HOUSING AGENCY DATA.

Subd. 2. Confidential data.

The following data on individuals maintained by the housing agency are classified as confidential data, pursuant to section 15.162, subdivision 2a: correspondence between the agency and the agency's attorney containing data collected as part of an active investigation undertaken for the purpose of the commencement or defense of potential or actual litigation, including but not limited to: referrals to the office of the inspector general or other prosecuting agencies for possible prosecution for fraud; initiation of lease terminations and unlawful detainer actions; admission denial hearings concerning prospective tenants; commencement of actions against independent contractors of the agency; and tenant grievance hearings.

Subd. 3. Protected nonpublic data.

The following data not on individuals maintained by the housing agency are classified as protected nonpublic data, pursuant to section 15.162, subdivision 5d: correspondence between the agency and the agency's attorney containing data collected as part of an active investigation undertaken for the purpose of the commencement or defense of potential or actual litigation, including but not limited

[* See section 4.5.1. An exception to disclosure of information is that material prepared in anticipation of litigation. *]

Section 32 (3) continued

to, referrals to the office of the inspector general or other prosecuting bodies or agencies for possible prosecution for fraud and commencement of actions against independent contractors of the agency.

Subd. 4. Nonpublic data.

The following data not on individuals maintained by the housing agency are classified as nonpublic data, pursuant to section 15.162, subdivision 5c: all data pertaining to negotiations with property owners regarding the purchase of property. With the exception of the housing agency's evaluation of properties not purchased, all other negotiation data shall be public at the time of the closing of the property sale.

[* See section 4.5.1. Exceptions to disclosure of property information are discussed. *]

Section 27 LICENSING DATA.

Subd. 2. Private data.

The following data collected, created or maintained by any licensing agency are classified as private, pursuant to section 15.162, subdivision 5a: data, other than their names and addresses, submitted by licensees and applicants for licenses; the identity of complainants who have made reports concerning licensees or applicants which appear in inactive complaint data unless the complainant consents to having his or her name disclosed; the nature or content of unsubstantiated complaints when the information is not maintained in anticipation of legal action; the identity of patients whose medical records are received by any health licensing agency for purposes of review or in anticipation of contested matter; inactive investigative data relating to violations of statutes or rules; and the record of any disciplinary proceeding except as limited by subdivision 4.

Subd. 3. Confidential data.

The following data collected, created or maintained by any licensing agency are classified as confidential, pursuant to section 15.162, subdivision 2a: active investigative

[* See section 4.5.3 for examples of information that is of significant privacy interest to the individual. *]

Section 27 (3) continued

data relating to the investigation of complaints against any licensee.

Subd. 4. Public data.

Licensing agency minutes, orders for hearing, finding of fact, conclusions of law and specification of the final disciplinary action contained in the record of the disciplinary action are classified as public, pursuant to section 15.162, subdivision 5b. The entire record concerning the disciplinary proceeding is public data pursuant to section 15.162, subdivision 5b, in those instances where there is a public hearing concerning the disciplinary action.

15.1672 EXAMINATION DATA.

Data consisting solely of testing or examination materials, or scoring keys used solely to determine individual qualifications for appointment or promotion in public service, or used to administer a licensing examination, or academic examination, the disclosure of which would compromise the objectivity or fairness of the testing or examination process are classified as nonpublic, except pursuant to court order. Completed versions of personnel, licensing, or academic examinations shall be accessible to the individual who completed the examination, unless the responsible authority determines that access would compromise the objectivity, fairness, or integrity of the examination process. Notwithstanding section 15.165, the responsible authority shall not be required to provide copies of completed examinations or answer keys to any individual who has completed an examination.

[* See section 4.5.1. An exception to information disclosed is materials used to administer examinations if disclosure would compromise the fairness or objectivity of the examination process. *]

[* See section 4.4.4. Under certain conditions, an individual may examine, but not copy, his own test taken. *]

[* The above 2 examples are a good illustration of the delicate balance the agency must reach in deciding whether to disclose information or not. *]

[* The Statutes provide for similar discretion to be taken. *]

15.1679 LIBRARY DATA.

Subd. 1.

All records collected, maintained, used or disseminated by a public library shall be administered in accordance with the provisions of sections 15.1611 to 15.17.

Subd. 2.

That portion of records maintained by a public library which links a library patron's name with materials requested or borrowed by the patron or which links a patron's name with a specific subject about which the patron has requested information or materials is classified as private, pursuant to section 15.162, subdivision 5a, and shall not be disclosed except pursuant to a valid court order.

[* See section 4.5.1, which discusses exceptions to disclosure of information relating to library, archival or museum material. *]

15.1675 REVENUE DATA.

The following data created, collected and maintained by the state department of revenue are classified as protected nonpublic pursuant to section 15.162, subdivision 5d: criteria used in the computer processing of income tax returns to determine which returns are selected for audit; department criteria used to determine which income tax returns are selected for an in-depth audit; and department criteria and procedures for determining which accounts receivable balances below a specified amount are cancelled or written-off.

[* See section 4.5.3 (6) for information posing a significant privacy interest to the individual. *]

Section 26 REVENUE DEPARTMENT INFORMANT DATA.

Names of informers, informer letters and other unsolicited data, in whatever form, furnished to the state department of revenue by a person, other than the data subject or revenue department employee, which inform that a specific taxpayer is not or may not be in compliance with the tax laws of this state are classified as confidential data pursuant to section 15.162, subdivision 2a.

15.1676 SURPLUS LINE INSURANCE DATA.
All data appearing on copies of surplus line insurance policies collected by the insurance division of the department of commerce pursuant to section 60A.20 are classified as private, pursuant to section 15.162, subdivision 5a.

Section 30 ASSESSOR'S DATA.

Subd. 1. Generally.

The following data collected, created and maintained by political subdivisions are classified as private, pursuant to section 15.162, subdivision 5a, or nonpublic depending on the content of the specific data:

Data contained on sales sheets received from private multiple listing service organizations where the contract with the organizations requires the political subdivision to refrain from making the data available to the public.

Subd. 2. Income property assessment data.

The following data collected by political subdivisions from business entities concerning income properties are classified as nonpublic data pursuant to section 15.162, subdivision 5c:

(a) Detailed income and expense figures for the current year plus the previous three years;

(b) Average vacancy factors for the previous three years;

(c) Verified net rentable areas or net usable areas, whichever is appropriate;

Section 30 (2) continued

(d) Anticipated income and expenses for the current year; and

(e) Projected vacancy factor for the current year.

15.1674 DEFERRED ASSESSMENT DATA.
Any data, collected by political subdivisions pursuant to section 435.193, which indicate the amount or location of cash or other valuables kept in the homes of applicants for deferred assessment, are private data pursuant to section 15.162, subdivision 5a.

[* See section 4.5.3 where information describing an individual's finances is of significant privacy to the individual. *]

4.15.19 Photographic Negatives

Section 37 PHOTOGRAPHIC NEGATIVES.
Photographic negatives obtained by the department of public safety in the process of issuing drivers licenses or Minnesota identification cards shall be private data on individuals pursuant to section 15.162, subdivision 5a.

4.15.20 Elected Officials Correspondence Data

15.1697 ELECTED OFFICIALS; CORRESPONDENCE; PRIVATE DATA.

Correspondence between individuals and elected officials is private data on individuals, but may be made public by either the sender or the recipient.

CHAPTER 5

AN OVERVIEW OF THE PROVISIONS COVERED IN THE CHAPTER 4 COMPARISON

Before discussing the strengths and weakness of the Minnesota Act and the Uniform Code, a quick general overview of the material covered will enable one to grasp the major provisions of each act. As one can see from Table 2, there are some gaps in both of the acts with regard to the manner in which the text was organized. For example, the Statutes contain no sections comparable to: the purposes of the Code; instances where the responsible authority does not have to disclose information to the public; examples of clearly unwarranted invasions of personal privacy; audit trail provisions; the establishment of the Office of Information Practices; or grants of exemption.

On the other hand, the Code contains no sections comparable to the Statutes' temporary classification method; duties of the commissioner; definitions pertaining to specific categories of information; or a list of the categories of information. Just because the Code or the Act does not contain comparable sections does not mean

TABLE 1: A COMPARISON OF THE PROVISIONS EXISTING IN BOTH ACTS ORDERED BY CHAPTER 4 INDEX

	DOES THE ACT/CODE PROVIDE FOR:	MINNESOTA STATUTES	UNIFORM CODE
	PURPOSE, SCOPE		
1.	Purposes; Rules of Construction?	No	Yes (SECTION 1-102, 1-103 1-104)
	DEFINITIONS		
2.	Up Front Definitions?	Yes (SECTION 15.162)	Yes (1-105
	PUBLIC AND INDIVIDUAL ACCESS TO INFORMATION		
3.	Public Access to Records?	Yes (15.1621, 15.163)	Yes (2-101, 2-102)
4.	Individual Access to Own Data?	Yes (15.165)	Yes (3-105)
5.	Limitations on Individual Access to Own Data?	Yes (15.165)	Yes (3-106)
	DISCLOSURE AND PURPOSE		
6.	Cases Where Information is Not Subject to the Duty of Disclosure?	No	Yes (2-103)
7.	Cases Where Personal Records May be Disclosed to the Public?	Yes (15.163)	Yes (3-101)
8.	Cases Where the Individual Has a Significant Privacy Interest?	No	Yes (3-102)
9.	Interstate, Inter-Agency, Foreign Disclosures?	Yes (15.163)	Yes (3-103)
10.	Overriding Prohibition on Disclosure?	No	Yes (3-104)
	DUTIES OF THE HOLDERS OF INFORMATION		
11.	Collection and Maintenance of Information?	Yes (15.163, 15.165, 15.1621)	Yes (3-108, 2-102)
12.	Audit Trail?	No	Yes (3-108, 3-105)

Table 1 - continued

	DOES THE ACT/CODE PROVIDE FOR:	MINNESOTA STATUTES	UNIFORM CODE
	DUTIES OF THE HOLDERS OF INFORMATION		
13.	Correction and Amendment of Records?	Yes (15.165)	Yes (3-107)
14.	Annual Report of Records?	Yes (15.163)	Yes (3-116)
15.	Agency Implementation?	No	Yes (3-115)
	ENFORCEMENT, REMEDIES, PENALTIES		
16.	Civil Remedies?	Yes (15.166)	Yes (3-112)
17.	Judicial Enforcement?	Yes (15.166)	Yes (2-104)
18.	Penalties?	Yes (15.167)	Yes (2-105, 3-113, 3-114)
	CHANGE OF STATUS--TEMPORARY CLASSIFICATION		
19.	Temporary Classification?	Yes (15.1642)	No
	GOVERNMENT CONTRACTORS		
20.	Government Contractors?	Yes (15.163)	Yes (3-111)
	RESEARCH RECORDS		
21.	Procedures, Limitations?	Yes (15.163)	Yes (3-109)
22.	Amenability of Research Records to Compulsory Process; Researcher Priviledge?	No	Yes (3-110)
	BODY TO OVERSEE THE CARRYING OUT OF THE STATUTES		
23.	Duties of the Commissioner?	Yes (15.1671)	No
24.	Appointment of Director of Office of Information Practices?	No	Yes (4-101)
25.	Powers and Duties of the Office of Information Practices?	No	Yes (4-102)

Table 1 - continued

	DOES THE ACT/CODE PROVIDE FOR:	MINNESOTA STATUTES	UNIFORM CODE
	EXEMPTIONS		
26.	Grant of Exemption?	No	Yes (5-101)
	DEFINITIONS PERTAINING TO SPECIFIC CATEGORIES OF DATA		
27.	Definitions (Other)?	Yes (Throughout Amendments)	No
	CATEGORIES OF INFORMATION		
28.	Categories of Information?	Yes (15.1672 through Section 37)	No

that they are deficient in those areas. Rather, although certain underlying principles might be similar, the framework for each act has been constructed quite differently.

CHAPTER 6

ANALYSIS OF THE MINNESOTA ACT

Four major strengths of the Minnesota Government Data Practices Act become quite apparent after the comparison with the Uniform Information Practices Code in Chapter 4. They are as follows:

1. Exclusion of No State Agency, Political Subdivision, Statewide System, Branch of Government

The scope of the state agencies, political subdivisions, and statewide systems regulated by the Minnesota Act is specific and comprehensive. No branches of government are exempted from the provisions of the Act.

Some of the lengthiest definitions in sections 4.2.3 (Scope) or 4.3.1 (Definitions--Up Front) are those defining state agencies, political subdivisions and statewide systems. These definitions are comprehensive to the point of being too detailed. Nonetheless, the intent is truly apparent. That is, all agencies of the

state must comply with the provisions of the Minnesota Act; and the terms, state agency, statewide system, and political subdivision are always stated together in each provision of the text where they apply.

Throughout the years, these definitions have been amended to be more comprehensive. In particular, the definition of political subdivision has become more explicit with regard to nonprofit agencies.

2. No Exemptions Granted

There are no provisions in the Minnesota Act from which any state agency, political subdivision or statewide system is exempted. All are subject to and held liable for all of the provisions of the Act. This is in line with point 1 above, which exempts no agency from the provisions of the Minnesota Act.

The only duty the responsible authority of an agency might not have to fulfill is that of submitting an annual report to the commissioner (see section 4.6.4). The Minnesota Statutes state that the commissioner may require responsible authorities to submit the annual report or additional information relevant to data collection practices and procedures. This is the only example of implied exemptions. Otherwise, all agencies are equally subject to all provisions of the Minnesota Act.

3. Commissioner, Responsible Authority, Designee Positions

The three positions of commissioner, responsible authority, and designee are created in the Minnesota Act. That is why, when reading section 4.3.1.6 (Minnesota Statutes: Commissioner, responsible authority, designee), one becomes aware of three definitions which do not exist in the Uniform Code--commissioner, responsible authority, and designee. Specific duties are assigned to them. Those persons filling the positions interface with each other and with individuals outside of the agency.

Although it is the agencies that are being regulated by the Minnesota Act, it is the people in specific positions who perform the necessary duties of each entity. It is much easier to understand the provisions of the Act when one can mentally picture certain persons carrying out assigned tasks.

Moreover, individuals who access the data are defined in the general definitions section (section 4.3.1.5). Individuals interface with the designees or responsible authority of an agency. The responsible authority interfaces with the commissioner in a designated, hierarchical chain of command. These personss also serve as key focal points to whom other individuals may go to for assistance or complaints. It is comendable that only one person is assigned to each of the positions of commissioner and responsible authority. Two or more persons in these decision-making positions may tend to confuse matters or produce non-uniform policies with regard to specific issues.

Although the responsible authority position was defined in the 1974 Minnesota Act, most duties to be performed were stated primarily in terms of the commissioner. For example, the 1974 Act did not specify that the responsible authorities were to prepare a report of an annual inventory of records. Instead, the commissioner was to prepare a report to the legislature containing a comprehensive listing of information about the state recordkeeping systems. In 1975, section 15.1641, Duties of responsible authority, was added to the Act, which delegated specific duties to the responsible authority. Thus, one can see that the duties of each position have been defined and refined via amendments to the Minnesota Act.

4. Comprehensive Work of Legislation

Compared with the Uniform Code, the Minnesota Act is short and not nearly as comprehensive. Nevertheless, it contains provisions for many different facets of data privacy legislation. It is also quite comprehensive when compared with other states' data privacy bills. Although each provision is not as detailed as the Uniform Code, the scope of the provisions covered is impressive. As mentioned in Chapter 3, the drafters of the Uniform Code had the advantage of being able to utilize the Minnesota Act.

The provisions that are more comprehensive than the Uniform Code are, for example, the definitions of statewide system, state agency, and political subdivision.

This was discussed in the first point of this chapter. The provision for obtaining written consent from the subject of a personal record before a disclosure is made (section 4.5.2) is noteworthy. Whereas the Uniform Code states that an agency may disclose an individually identifiable record pursuant to the prior written consent of the individual, the Minnesota Act contains seven specific conditions for written informed consent to be valid.

6.1 WEAKNESSES OF THE MINNESOTA ACT

Major weaknesses of the Minnesota Act are as follows:

1. Absence of Purpose

Noteably missing in the comparison is the fact that a purpose(s) for the legislation is nonexistent in the Minnesota Act. A purpose is essential in data privacy legislation because there is still much confusion as to what data privacy is, what entities it is supposed to protect, and what facets are the most crucial in data privacy legislation. Is the purpose of the Statutes to regulate the data handling practices of agencies of the state of Minnesota? Or is the purpose to state the rights of the public and individuals? Currently, there is a lack of purpose in the Minnesota Act.

Drafts of the 1974 Minnesota Act did include a provision stating three purposes of the Act: "(1) to encourage more secure systems of records on individuals; (2) to establish more effective structures and procedures for the protection of individual privacy; and (3) to assure periodic reporting to the legislature and the general public concerning record-keeping."[10] However, these provisions were dropped in the 1974 enactment.

Clearly, a purpose(s) would establish a firm foundation upon which the various provisions could be formulated and evaluated. It would provide a cohesiveness

to the Minnesota Act, remove unnecessary provisions, and provide legislators with guidelines for evaluating this Minnesota Act, as well as other data privacy acts.

2. Extensive Classification System

An extensive classification system exists which is based upon the eight definitions of data. This classification system results in:

- the inability to disclose or not disclose information using discretionary judgment on a case-by-case basis;
- redundancy of the information contained in the categories of information, the number of agencies which must file temporary classification applications;
- statutes which describe all the data classifications (including public data) for all of the information related to a specific agency;
- a time consuming temporary classification process;
- the omnibus portion of the Minnesota Act becoming overwhelmed by the statutes related to specific categories of information.

The definition of data on individuals and data not on individuals is currently crippling the Minnesota Act. For instance, the 1981 amendments introduced 20 new categories of information to the Statutes. These amendments are the by-products of the classification system, which classifies all government data into one of six categories. All data that is not public must be placed in one of the remaining four classifications of data, and these exceptions must be approved via the temporary classification procedure.

There are several unfortunate results with this method. First, classifying all records of a certain category of information into a specific classification of data inhibits the disclosure of information on a case-by-case basis. This is unfair to the public and to the individual, for access to the data is based only upon the classification within which it falls. The cases bordering on disclosure or nondisclosure cannot be deliberated upon individually because the rules for access have already been established.

Secondly, the cost of this specificity in classifying all data is redundancy. Each agency must apply for a change of status for the particular categories of information that are maintained by the agency. A great deal of overlap was discovered when matching certain situations with the situations listed in the Uniform Code. An example of this would be investigative data prepared in anticipation of a litigation. This situation can be found in attorney general data, law enforcement related data, housing agency data, and welfare data. However, four different amendments have been promulgated to cover this situation for each of these agencies. The result is redundancy and inefficiency.

Moreover, legislators, the commissioner, and responsible authorities could spend their time and efforts in a more effective manner if they did not have to constantly be burdened by the applications for temporary classification. Legislators must

approve each new category of information in order for it to become an amendment to the Minnesota Act. The commissioner must spend time reviewing these similar types of information. Therefore, legislators would be well-advised to move the redundant categories of information into the omnibus portion of the Minnesota Act.

When grouping all of the data according to which classification it belongs to, it was found that an abundance of public data was also described. The reason for this is that the scope of the exceptional categories of information must be described in-depth. At the same time, it becomes convenient and necessary to define what data shall be public in order to better understand what data is not public. This results in excessive verbiage.

3. Definitions of Private and Confidential Data on Individuals

Two serious loopholes exist in the definitions of private data on individuals and confidential data on individuals. Although private data on individuals can be accessed by the individual to whom the data pertains, it does not explicitly state what other persons or individuals can access the data. This means that others may also be able to access the data without the individual's knowledge of who else is accessing the data.

Confidential data on individuals also prohibits disclosure to the individual data subject; but at the same time, the definition leaves room for disclosures to be

made to others. It does not state to whom else the data is accessible, but it does not expressly prohibit disclosures to others. Also, with the absence of any audit trail provisions, many abuses to an individual's personal privacy may occur without the data subject knowing to whom the data was disclosed. Therefore, these two definitions must be revised.

4. Unnecessary Definitions--Nonpublic Data and Protected Nonpublic Data

By definition, both nonpublic data and protected nonpublic data are data not on individuals. This means that a data subject cannot be identified. However, the definitions of nonpublic and protected nonpublic data contain access provisions for the data subject, if one should exist. This does not make sense, for if a data subject could be identified, it would not be data not on individuals. It would be data on individuals.

There is no need to further classify data not on individuals because data privacy issues are not relevant when data not on individuals is disclosed to others. Abuses to an individual's privacy occur when data on individuals is disclosed to unauthorized persons for unauthorized purposes. Eliminating the nonpublic and protected nonpublic classifications would reduce the amount of time spent by legislators in approving or rejecting categories of information falling under either of these two classifications.

5. Summary Data Not Linked With Purpose

Summary data derived from private or confidential data on individuals is classified as public. Although summary data by definition does not identify the individuals, the personal records can be used for purposes that were not stated to the individual at the time that the data was collected.

Personal records can, by permission of the responsible authority, be disclosed to researchers and even non-researchers because the definition of summary data is not linked with research purpose. This is a dangerous situation--especially when the controls over the persons using the personal records are inadequate. For example, in order to protect the individuals who are the subjects of the personal records, the requester should be required to destroy the records after usage because they can intentionally or unintentionally be disclosed to others.

6. Lack of a Mechanism to Ensure Agency Compliance

The commissioner is delegated very little authority to compel agency compliance. The notion of having a commissioner to oversee the carrying out of the provisions of the Minnesota Act is good. However, a mechanism does not exist which will ensure that agencies carry through with the provisions of the Minnesota Act. The commissioner and the Data Privacy Division of the Department of Administration would be the ideal

candidates to monitor agency compliance, assist agencies and private citizens, recommend disciplinary actions for officers of an agency, or bring a court action against an agency.

Although an aggrieved individual may bring an action to court to make an agency comply with the provisions of the Minnesota Act, the Act does not state how compliance will be carried out. Therefore, the commissioner should be assigned statutory powers to carry out the provisions. Otherwise, the Act would be ineffective if not enforced properly.

7. Lack of Audit Trail Provisions

As discussed in section 4.6.2, the lack of an audit trail means that the individual will have no knowledge of the disclosures made by the agency to other individuals, agencies, persons, states or foreign governments. Chances for abuses to personal privacy occurring can greatly increase. Currently the Minnesota Act only provides for the responsible authority informing the individual whether he is a subject of stored data at the agency; the classification; content and meaning of the data. If the personal record has been disclosed to unauthorized persons or individuals, the individual has no means of knowing this, and therefore cannot seek legal remedies against the agency.

CHAPTER 7

ANALYSIS OF THE UNIFORM CODE

Before making a hasty judgment with regard to either the Minnesota Act or the Uniform Code, it is also necessary to examine the strengths and weaknesses of the Code. The strengths of the Uniform Code are that:

1. Case-By-Case Decisions; the Importance of Purpose in Disclosure

The agency is given the freedom to examine disclosures of information to individuals, other agencies, other states on a case-by-case basis. This results in a higher degree of fairness to all parties concerned because it attempts to balance the public interest in disclosure versus the individual's right to privacy.

Perhaps the primary strength of the Uniform Code is the fact that the notion of purpose is adequately dealt with in regard to the uses and abuses of data. Because the data is not classified, the responsible authority has the freedom to disclose or not to disclose information. His decision is based upon the purpose that the data will be used for in a given situation. If purpose is ignored in data privacy legislation, all of the cases in which an individual's personal privacy may be invaded

cannot really be given adequate protection.

Thus, the Uniform Code approaches this delicate situation by only providing a list of guidelines for clearly unwarranted invasions of privacy, or information which may or may not be disclosed. These are only roughh guidelines; because the agency head must pass his own judgement upon the circumstances surrounding his decision to disclose or not disclose information.

This policy should lessen abuses to an individual's personal privacy because each case is dealt with separately. In the Minnesota Act, all records pertaining to a specific situation are granted special access privileges, so special consideration is not given to exceptional situations. Furthermore, as stated in section 6.1, the Minnesota Act is not clear as to which other individuals or persons can access private or confidential data on individuals, or what criteria are used in deciding who else can access the data.

Although the decision to disclose is initially the agency head's decision, the scope of disclosure will eventually be determined by the courts as court actions occur and are reviewed de novo on a case-by-case basis. This is preferred over the Minnesota Act, where the intended purpose of use is not given adequate consideration.

2. Explicit Procedures With Which the Agency Must Comply

The provisions relating to the duties of the agency have been thought out quite carefully because the procedures for the agency are very well-defined. For example, specific time limits are stated in the Code within which the agency must make available or respond to a request to access the data. The Minnesota Act is not as specific, and there is much leeway in interpreting the obligations of the agency, as well as the individual.

At the same time, the Uniform Code, while stating a policy of liberal access to information, balances the interests of both the agency and the requester with regard to making the records available to the public. Although public access to agency information is desirable, the agency's ability to retrieve and make the records available must also be considered. Both sides are dealt with fairly in the Uniform Code.

For instance, the agency is not required to create new records for the requester. It should only make existing records available to the requester. Another example of fair dealings with both the agency and the requester is the determination of the allocation of costs when making available records for public inspection. The agency absorbs the cost of retrieving the records, but the requester must pay for the costs of copying the records.

3. Well-Defined Purpose

The purposes of the Uniform Code stated in section 4.2.2.1 clearly serve to show what principles were essential in drafting this privacy legislation. A discussion of the importance of stated purposes in data privacy legislation can be found in Chapter 6.0.

4. Statutory Powers of the Office of Information Practices

The major difference between the Office of Information Practices and the commissioner's Data Privacy Division is that it has the authority, for example, to recommend disciplinary actions to an agency's officers, to assist agencies in complying with the Uniform Code's provisions, or to criminally prosecute the officers of an agency. The commissioner lacks these powers; and hence, this mechanism to ensure that the Statutes are complied with by the agencies, is quite ineffective (see Chapter 6).

5. Research Records Are Associated With Purpose

Research records are associated with purpose, and comprehensive safeguards are established to protect the subject of the research, as well as the researcher. (This is covered in section 4.10.)

7.1 WEAKNESSES OF THE UNIFORM CODE

The weaknesses of the Uniform Code are as follows:

1. Exclusion of Two Branches of Government From All Provisions of the Uniform Code

Although the definition of agency is meant to be comprehensive, it only relates to agencies of the state of the executive branch of government. Both the legislative and judicial branches of government are excluded.

Exempting all agencies of the legislative and judicial branches from the provisions of the Uniform Code produces a double standard. That is, some agencies handling personal records are forced to comply with the provisions of the Code, while others are not. The potential abuses of the use of personal records may occur in any agency that handles personal records. The public right to access information is with regard to any branch of the government. Thus, there is no reason why these two main branches should be exempted from the Uniform Code's provisions, for they must also be accountable for their handling of personal records too.

Although it is stated in the Uniform Code that a potential separation of powers issue would come about as the result of including the legislative and judicial branches of government, this argument is not the major issue. The predominant issue is one of accountability, so if the judicial branch wants to contest the matter in court, that is fine. Before enacting the Uniform Code, though, all branches of government should be included.

2. Exemptions Granted to Agencies

Exemptions from certain provisions of the Uniform Code may be granted to designated agencies if the benefit derived to the agency from being exempt outweighs the public interest for disclosure. Already two branches of government have been exempted from all of the provisions of the Uniform Code.

If granted an exemption, an agency would not have to: (1) assure reasonable access facilities for duplicating records; (2) observe formalities when denying a request for access; (3) undertake measures to comply with the provisions of the Uniform Code; or (4) comply with the reporting requirements. However, it is not that difficult to comply with these provisions.

If exemptions were given, the most valid exemption is that of waiving the reporting requirements. Particularly because the reporting requirements of the Uniform Code are quite comprehensive, the amount of paperwork generated, and the confusion of agencies resulting from having to prepare such reports might be overwhelming. Most states have a tremendous number of databanks.

It has been mentioned that the Minnesota Act contained thorough reporting requirements in the 1974 Act. However, these requirements have been reduced substantially due to the problems just mentioned above. The reporting requirement is a valid exemption, then. Otherwise, the amount of information required in the reports might have to be reduced.

3. Position Similar to the Responsible Authority in the Minnesota Act Not Defined

Only the director of the Office of Information Practices is a position that has been created and assigned specific responsibilities in the Uniform Code. A position within the agency is not defined which would serve as a central authority for the agency with regard to carrying out the provisions of the Uniform Code.

Although reference is made to a head of the agency , this reference is, in fact, unclear. In section 4.5 (SECTIONS 2-102(f), 2-103(d), and (e)), a "head" of the agency is recognized. In section 4.6.4 (SECTION 3-116(2)), an "authority" under which the records are maintained is used. In the same section, the term, "officer," is used. Are they the same person? A specific position must be defined to interface with individuals and the director of the Office of Information Practices.

7.2 ANALYSIS OF THE CHARGES MADE AGAINST THE UNIFORM CODE

It is much easier to point out difficulties with the Minnesota Act because it has been enacted and in operation in the state of Minnesota for 7 years. The Act today is much different from its 1974 version because many amendments have been made to it over time. Because the Uniform Code has not been enacted in any state thus far, one can only speculate as to what it would be like in actual operation. In Chapter 3, it was mentioned that the major criticisms of the Uniform Code are that it allows the agency too much discretionary power, and that law enforcement uses are given too favorable treatment. These two criticisms will be discussed in this section.

1. Too Much Discretionary Power Given to a Government Agency

It is true that the agency head in the Uniform Code is delegated much more responsibility and discretionary judgment that the responsible authority in the Minnesota Act. However, this power is not absolute. The Uniform Code was designed to limit this power by placing the burden of proof upon the agency head. Perhaps the underlying question would be whether the judicial enforcement and civil remedies offered an individual are adequate enough to offset the power of the agency head.

The checks against the agency head are adequate. For example, the judicial enforcement section of the Uniform Code (section 4.7.2) is immediately after the list of information that the agency is not required to disclose to the public (section 4.5.1).

The Minnesota Act does not state that it will hear the case de novo, but the Uniform Code does.

Additionally, time limits for the agency's complying with an individual's request have been explicitly stated in the Uniform Code. One of the major strengths of the Code (see Chapter 7) is the extent to which definite procedures have been mapped out to which the agency must adhere. The purpose of these definite rules is to make it clear to the agency that court action can be taken against an agency if it should not stringently adhere to the stated procedures. For instance, definite time limits with which an agency must comply are not stated in the Minnesota Act for public access to information. They are, however, stated in the Uniform Code; and a requester may furthermore bring an action against an agency if the agency fails to meet the stated time limits.

For civil remedies, the burden of proof is still upon the agency to establish the non-disclosability of an accessible record, with the exception of agency indemnification from an employee who has willfully disclosed an individually identifiable record to a third party. Although the agency has the power to disclose or not disclose personal records, the ultimate determination as to what can and cannot be disclosed is left to the courts to decide. Thus, the agency does not really have unlimited power, which is contrary to one of the major criticisms of this Code.

Furthermore, the Office of Information Practices is delegated the authority to conduct inquiries into an agency's recordkeeping practices, examine an agency's records, recommend disciplinary action to be taken, and so forth. This is one more check against the discretionary powers of an agency.

2. Too Favorable Treatment is Accorded Law Enforcement Uses of Data

This charge arises because reference is made to law enforcement uses of data in sections 4.5.1, 4.5.3, and 4.5.4. The guidelines offer protection from disclosure if disclosure would impair an ongoing investigation, identify a confidential informant, reveal investigative techniques, or endanger an individual's life. Also exempted are inter-agency or intra-agency deliberative material that is communicated for decision-making or that would impair the decision-making processes of the agency. Section 4.5.3 lists information that is compiled and identifiable as part of an investigation into a possible violation of criminal law as an example of a situation where the individual has a significant privacy interest. Section 4.5.4 prohibits inter-agency disclosures of individually identifiable records unless it is for the purpose of a civil or criminal investigation or to disclose identifying particulars of an individual. (These are two exceptions given for law enforcement purposes.) Thus, the concern that the Uniform Code is lax with regard to law enforcement uses is a valid one.

The Uniform Code states its position as follows:

"...it is difficult to state with precision how much confidentiality is crucial to effective law enforcement and agency decisionmaking. The exemptions, therefore, must be read against the background of case law developed at the federal and state level. Agency attempts to abuse these exemptions should be amenable to judicial control. It should not be forgotten, however, that numerous other mechanisms exist to insure the accountability of public officials in law enforcement activity and general decision-making: criminal sanctions, civil sanctions, exclusionary rules, judicial review of agency action, legislative oversight and ultimately the electoral process. Sub-sections (a)(1) and (a)(2) supplement the established structure of checks and balances; they do not supplant it." 11

It is difficult to say how much confidentiality is necessary for law enforcement purposes, but a comparison with the Minnesota Act is due. There is an abundance of law enforcement related data in section 4.15.5 in the Minnesota Act. For instance, investigative data collected by a law enforcement agency to prepare a case against a person is confidential while the investigation is active. In the Uniform Code, the agency head may decide whether to disclose such information, so actually, the Minnesota Act is more stringent because the data is not public.

Whereas the Uniform Code allows the disclosure of individually identifiable records to other agencies if it is for revealing identifying particulars of an individual for law enforcement purposes, no mention is made of what identifying particulars will be disclosed. The Minnesota Act lists all of the identifying particulars which may be disclosed. Depending on the agency head's decision, more or less information may be divulged than the Minnesota Act. Thus, the system of checks

and balances still holds because judicial actions can be taken against a law enforcement agency.

CHAPTER 8

RECOMMENDATIONS FOR THE MINNESOTA LEGISLATURE

Taking the comprehensive comparison and the analysis of strengths and weaknesses into consideration, it is now possible to make a recommendation with regard to the action that the Minnesota legislators should take. There are several possible alternatives. The state of Minnesota can:

1. Reject the Uniform Code and keep the Minnesota Act in its current form.
2. Reject the Uniform Code and keep the Minnesota Act, with amendments.
3. Reject the Minnesota Act and accept the Uniform Code in its current form.
4. Reject the Minnesota Act and accept the Uniform Code, with amendments.

Based on the discussions in the previous chapters, it is recommended that the fourth alternative be taken. The Uniform Code is favored over the Minnesota Act for a number of reasons. First, the omnibus portion of the Minnesota Act is being overwhelmed by the portion containing the various categories of data. The latter portion

arises from the extensive classification system. Difficulties with the present classification system have been pointed out in this comparison, and major changes to the Act must be made to correct them. Moreover, the classification system does not really deal with intimate privacy issues because disclosure is not determined on a case-by-case basis. Data privacy issues cannot be dealt with by means of the blanket protection offered in the exceptional categories of information. Such is not the nature of data privacy abuses. The case-by-case basis is much fairer than the Minnesota system to the individual because it is based upon the purpose for which data will be used.

The classification system is also inefficient, and it tends to lock a particular category of information to one definition of data. Although this specificity is clear-cut, it is inflexible. On the other hand, the guidelines stated in the Uniform Code are very sketchy, but this means that there will be room for interpretation and change. The nature of data privacy is dynamic, so it would be better to have a law which could be decided upon according to the given situation.

Secondly, the Uniform Code is much more comprehensive in nearly all respects. A glance at Table 1 (Chapter 5) would show one that it contains many important provisions, such as an audit trail or purpose, that are not covered in the Minnesota Act.

At the same time, may of the provisions were taken directly from the Minnesota Act and elaborated upon, so there are many commonalities between both acts.

One must also not overlook the benefits of uniformity. Currently, each state has its own laws regarding, for example, interstate data transfers. This creates much confusion which could be reduced through enactment of the Uniform Code in all 50 states. The number of personal records being maintained, and the number of computers used to handle these records is increasing rapidly, and a uniform law would promote increased efficiency in handling records. The individual would also be assured of consistent rights, which is very different from the situation which currently exists. Many states do not even have legislation relating to data handling practices.

As mentioned in Chapter 7, there are a few weaknesses with the Uniform Code at present. Instituting changes to (1) make the Code applicable to all branches of government; (2) sever the fifth article; and (3) define a responsible authority position, would further enhance the Code's attractiveness. Thus, it is recommended that the Code be considered by all states for enactment, provided that the above three changes be made to it.

CHAPTER 9

SUMMARY OF THE TWO APPROACHES TAKEN TO DATA PRIVACY LEGISLATION; GLOBAL OBSERVATIONS

If one were to read through the new 1981 amendments to the Minnesota Statutes, a trend toward discretionary power to the responsible authority becomes apparent. Because the data classifications cannot possibly cover all present and future exceptions to classifying the data as public, the new amendments allow the responsible authority to decide when information shall be disclosed. An example of this would be examination data in section 4.15.13: "Completed versions of personnel, licensing, or academic examinations shall be accessible to the individual who completed the examination, unless the responsible authority determines that access would compromise the objectivity, fairness, or integrity of the examination process."[12] Although the data is given a classification, the responsible authority may decide to withhold the information; and thus, the result would be similar to the discretionary judgment exercised by the agency head in the Uniform Code.

One more interesting provision is in section 4.15.5.2 concerning law enforcement data: "When data is classified as public under this section, a law enforcement agency shall not be required to make the actual physical data available to the public if it is not administratively feasible to segregate the public data from the confidential."[13] This provision covers accessibility of data, and it would be useful to define an accessible record as defined in the Uniform Code.

Therefore, one can see that the Minnesota Act is truly evolving toward the structure of the Uniform Code, even though the beginning approach taken was completely different. The Minnesota legislature, then, should seriously consider taking these provisions and moving them to the omnibus portion of the Minnesota Act so that repetitious classifications would not have to be added each year as amendments to the Act.

CHAPTER 10

CONCLUSION

In performing a comparison such as this research, it is of utmost importance that all factors be taken into consideration. Although a provision-by-provision comparison will reveal the strengths and weakness of each act, it is unfair to unduly penalize one act without first researching other factors. Three major external factors would be (1) the intent with which the act was drafted; (2) the time lapse differential between the two acts; and (3) the amount of expertise available to the drafters of the act during the time that the act was being drafted. Only then can one have a full appreciation for the tremendous amount of time, deliberation, and reconsidering which went into the creation of each act.

Although the Uniform Information Practices Code has been recommended for enactment over the Minnesota Statutes, this conclusion could possibly change in the future. The law is constantly evolving to meet the needs of the people whom it protects; and it is imperative that legislators and citizens carefully review it to ensure that it works for them.

FOOTNOTES

[1]Robert Ellis Smith, Compilation of State and Federal Privacy Laws 1978-79 (Washington D.C.: Privacy Journal, 1978), p. 2.

[2]Willis H. Ware, et. al., Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Massachusetts: The Massachusetts Institute of Technology Press, 1973).

[3]Don Gemberling, Data Privacy Division of the Department of Administration, St. Paul, Minnesota, interview, July 1981.

[4]Minnesota Statutes, sec. 15.162, subd. 11.

[5]Alicia V. Pond, National Conference of Commissioners on Uniform State Laws, Chicago, Illinois, interview, July 1981.

[6]Uniform Information Practices Code, sec. 1-102.

[7]Ambrose Kottschade v. Gerald Lundberg, 160 N.W. (2d) 135 (MN 1968).

[8]Minneapolis Star and Tribune Company v. State and Others, 163 N.W. (2d) 46 (MN 1968).

[9]Ibid.

[10]Gordon C. Everest, University of Minnesota, Minneapolis, Minnesota, notes, August 1981.

[11]Uniform Information Practices Code, page 18.

[12]Minnesota Statutes, section 15.1672.

[13]Ibid., section 36, subdivision 8.

BACKGROUND REFERENCES USED

Books

1. Gerbereck, Dahl A., Chairman. Privacy, Security, and the Information Processing Industry. The Ombudsman Committee on Privacy, Los Angeles Chapter. New York: Association for Computing Machinery, 1976.

2. Goldstein, Robert C. "A Management's View of Data Base Privacy." In Managing the Data Resource Function, pages 233-249. Edited by Richard L. Nolan. St. Paul, Minnesota: West Publishing Company, 1974.

3. Mayer, Michael F. Rights of Privacy. New York: Law-Arts Publishers, Inc., 1972.

4. Miller, Arthur R. The Assault on Privacy, Computers, Data Banks, and Dossiers. Ann Arbor, Michigan: The University of Michigan Press, 1971.

5. O'Brien, David M. Privacy, Law, and Public Policy. New York: Praeger Publishers, 1979.

6. Packard, Vance. The Naked Society. New York: David McKay Company, Inc., 1964.

7. Rule, James; McAdam, Douglas; Stearns, Linda; and Uglow, David. The Politics of Privacy. New York: Elsevier, 1980.

8. Smith, Robert Ellis. Compilation of State and Federal Privacy Laws 1978-79. Washington D.C.: Privacy Journal, 1978.

9. Westin, Alan F. and Baker, Michael A. Databanks in a Free Society: Computers, Record-Keeping and Privacy. New York: Quadrangle Books, 1972.

10. Ware, Willis H., et. al., Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Massachusetts: The Massachusetts Institute of Technology Press, 1973.

Books - continued

11. Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967.

12. Young, John B. Privacy. New York: John Wiley & Sons, 1978.

Articles

1. Canning, Richard G., "The Debate on Information Privacy, Parts 1 & 2," EDP Analyzer 13:11 and 12 (November and December 1975): 1-12 and 1-14, respectively.

2. Canning, Richard G. "Integrity and Security of Personal Data," EDP Analyzer 14:4 (April, 1976): 1-14.

3. Hirsch, Phil. "Europe's Privacy Laws--Fear of Inconsistency." Datamation February 1979, 85-88.

4. Prosser, William L. "Privacy." California Law Review 48 (August 1960): 383-423.

5. Turn, Rein. "Cost Implications of Privacy Protection in Databank Systems." Data Base (6:4), 1975 Spring, 3-9.

6. Ware, Willis H. "Records, Computers, and the Rights of Citizens." Datamation, September 1973, 112-114.

7. Warren, Samuel D. and Brandeis, Louis D. "The Right to Privacy." Harvard Law Review 4:5 (December 15, 1890): 193-220.

Documents, Proceedings, Cases

1. A Report on Certain Aspects of the Massachusetts Criminal Justice Information Systems. The Commonwealth of Massachusetts Governor's Commission on Privacy and Personal Data, By Arthur R. Miller, Chairman. Boston, Massachusetts: n.p., December, 1974.

2. A Scholar's Right to Know Versus Individual's Right to Privacy, Proceedings of the First Rockefellers Archive Center Conference. New York: A Rockefeller Archive Center Publication, December 5, 1975.

3. Ambrose Kottschade v. Gerald Lundberg in Minnesota Reports Volume 280 Cases argued and determined in the Supreme Court of Minnesota, March 22, 1968-July 5, 1968. Ruth Jensen Harris, Reporter. St. Paul, Minnesota: North Central Publishing Co., 1969.

4. Assembly Bill 2656, Protection of Individual Rights in A Computer Environment. Hearing Before the Committee on Efficiency and Cost Control. By Mike Cullen, Chairman. California: n.p., December, 1973.

5. Combined Annual Reports for Fiscal Years 1977 and 1978. The Security and Privacy Council. Boston, Massachusetts: n.p., 1978.

6. Computer Data Systems and Their Effect on Individual Privacy--Staff Research Report No. 117. By David A. Johnston, Director. Columbus, Ohio: n.p., February, 1975.

7. Federal Reports Act from United States Code Annotated Title 44 Public Printing and Documents. St. Paul, Minnesota: West Publishing Company, 1969.

8. Freedom of Information Act 5 USC 552 from United States Code Annotated Title 5 Government Organization and Employees 881 to 703. St. Paul, Minnesota: West Publishing Co., 1977.

9. Minneapolis Star and Tribune Company v. State and Others from Minnesota Reports Volume 282 Cases Argued and Determined in the Supreme Court of Minnesota November 1, 1968-February 28, 1969. Ruth Jensen Harris, Reporter. St. Paul, Minnesota: North Central Publishing Co., 1969.