990127

MINNESOTA MDH DEPARTMENT OF HEALTH

Protecting, Maintaining and Improving the Health of All Minnesotans

February 2, 1999

Patrick E. Flahaven
Secretary of the Senate
State Capitol, Room 231C
75 Constitution Avenue
St. Paul, Minnesota 55155

Edward Burdick
Chief Clerk of the House of Representatives
State Capitol, Room 211
St. Paul, Minnesota 55155

Kim Gunderson
Legislative Reference Library
645 State Office Building
100 Constitution Avenue
St. Paul, Minnesota 55155

Re: Filing of Report of the Information Policy Task Force

Dear Mr. Flahaven, Mr. Burdick, and Ms. Gunderson:

Enclosed please find the final report of the Information Policy Task Force, prepared as directed in 1997 Minnesota Laws, chapter 202, article 2, section 56. The Task Force was created to study and make recommendations regarding Minnesota law on public information policy, including government data practices and information technology issues. As required, the final report contains the Task Force's findings and recommendations, including any proposed legislation.

The Task Force has had a careful and deliberative process since it began meeting in October 1997. We have taken testimony from many persons with many points of view on many issues. We attempted to be open to everyone. As we worked to finalize the report, we were able to achieve consensus on some, but not all, of the findings and recommendations.

The report is not so much a checklist, as it is a description of issues related to public information policy. The report delineates points of agreement and disagreement. We hope the report serves its intended purpose of informing the Legislature on the many complex, contentious, and important issues surrounding public information policy.

85 East Seventh Place • St. Paul, MN 55

In closing, I want to commend the members of the Task Force for their time, effort, and dedication and for the contribution they have made to the development of public information policy in Minnesota. I also want to thank the staff of the Task Force for their dedication and for the large volume of high quality work they did in support of the Task Force.

Sincerely,

Anne M. Barry, Chair
Information Policy Task Force

REPORT OF THE INFORMATION POLICY TASK FORCE TO THE MINNESOTA LEGISLATURE

PREPARED AND PUBLISHED BY THE INFORMATION POLICY TASK FORCE

January 1999
St. Paul, Minnesota

Prepared in compliance with Minnesota Session Laws 1997, Chapter 202, Article 2, Section 56.

TABLE OF CONTENTS

I. Executive Summary

The Information Policy Task Force was created by legislation enacted in 1997. The Task Force, composed of eight citizen and four legislative members, was given a very broad charge to study and make recommendations concerning: the content and organization of data practices and related statutes; issues related to surveillance and other forms of information technology, including the impact of technology on data practices and privacy; procedures for developing and implementing a coherent and coordinated approach to information policy; approaches to information policy in other states and foreign jurisdictions; and, other information policy issues as identified by the Task Force.

The Task Force began meeting in October, 1997. Over these last several months, the Task Force has heard presentations on a number of issues; reviewed existing information policy principles drawn from certain Minnesota Statutes; concluded that some principles should be discarded and new principles articulated, heard public comment on its work; received and reviewed written submissions; and prepared a number of recommendations, including draft legislation to carry out those recommendations. Early on the Task Force decided that, whenever possible, recommendations and other actions taken by the Task Force would be done by evolving a consensus of the Task Force membership. Many of the Task Force's recommendations are the product of this consensus process. However, there were occasions when disagreement among Task Force members about the content of a principle or the statement of a recommendation was put to a vote of the members present. Most votes taken by the Task Force were close votes.

The full text of this Report: details the composition of and activities of the Task Force; articulates an updated set of information policy principles; makes a series of detailed recommendations; provides legislation to carry out those recommendations; analyzes the budgetary implications of recommendations with fiscal impact; and, includes written submissions presented by persons who appeared before the Task Force or who reacted to drafts of the Task Force's Report.

The recommendations of the Task Force are as follows:

Recommendation 1: Minnesota Statutes Section 15.17 should be amended to reflect the reality that important government records are increasingly kept in media which are not paper.

Recommendation 2: More education and assistance should be provided to government entities so that entities can effectively deal with the proper disposition of government records. There is a particular and growing need to assist entities at all levels of government with the proper disposition of computerized records. The Department of Administration and the State Archives Department of the Minnesota Historical Society should work, in conjunction with

government entities, to provide technical and policy guidance and to provide on-going education on issues of electronic records management.

Recommendation 3: The Data Practices Act should be amended to require each government entity to disseminate to the public, in some form, and at a minimum post in the entity reception area, the procedures in effect in the agency which tell the public how to gain access to public government data. Those procedures should be updated as personnel and other changes occur.

Recommendation 4: The Data Practices Act should be amended so that the charges that government entities can assess to the public for copying public government data are limited only to the marginal costs of providing the data in the form it is maintained by the government entity. The amendment should explicitly say that government entities should only be able to charge for the actual costs of making the copies and that those costs should not include labor, overhead and development costs incurred by the entity in providing the copies or maintaining the public data. Any government entity that has or receives specific statutory authority for charging more than marginal costs should be able to do so.

Recommendation 5: The Data Practices Act should be clarified to explain that public access to public government data using on line inquiry methods including examination of data, downloading data or printing copies of data, is, in this electronic age, a form of inspection of data. This type of inspection of government data, just like inspection by visual examination of paper records, should be at no cost to the individual making the inquiry as long as the individual is bearing the costs of the communication hookup to the government entity. Note: this would not require a government entity to put data on-line. It would only require that data that are already on-line be available for inspection without charge.

Recommendation 6: The Data Practices Act should be amended to require government entities that want to copyright various forms of government data have legislative authority to do so.

Recommendation 7: The Data Practices Act should be amended to specifically require that when government entities hold public government data in an electronic medium, the public should

be able to acquire copies of the data in that electronic medium. Government entities should design and implement new government data systems so that public data are easily accessible for electronic use and copying by citizens.

Recommendation 8: In authorizing any program intended to offer services and/or government information electronically, the Legislature should provide funding for any program intended to offer mechanisms that permit citizens to take advantage of the program whether or not they own or have ready access to electronic equipment.

Recommendation 9: The Data Practices Act should be amended to limit the authority of local government bodies to make decisions about disseminations of not public government data.

Recommendation 10: The Data Practices Act should be amended to change the notice requirements of Minnesota Statutes Section 13.04, subdivision 2, (the "Tennessen Warning") when the data being collected are private data about government employees or private data about students.

Recommendation 11: The Data Practices Act should be amended so that government entities should be required to provide data subjects with immediate access to data about themselves or to provide access within 10 days of the request of a data subject.

Recommendation 12: The Data Practices Act should be amended to require government entities to report to the Commissioner of Administration the acquisition of any electronic device that will enhance the government entity's ability to conduct surveillance on citizens. Exempt from this requirement should be acquisitions of surveillance equipment for compelling public safety reasons.

Recommendation 13: The Data Practices Act should be amended to prohibit government entities from requiring citizens to explain reasons for or to justify access to public government data. Government entities should be able to ask citizens for name and other identifying information for the sole purpose of facilitating access to the data.

Recommendation 14: A number of Minnesota Statutes should be amended to eliminate language that is inconsistent with the

nomenclature and philosophy used in the Data Practices Act. The Data Practices Act should be amended to reduce some of its complexity. Draft legislation to accomplish these tasks is found in Appendix 5.

Recommendation 15: The Data Practices Act should be amended to repeal the provision that appears in Minnesota Statutes Section 13.03, subdivision 3, that authorizes government entities in some situations to charge, in addition to the normal fees for providing copies of government data, an additional fee intended to allow government entities to recover the development costs for producing systems of data that have commercial value.

Recommendation 16: The Department of Administration should be specifically charged, by statute, with the responsibility for preparing model policies, procedures, and forms in order to assist state and local government entities in complying with the procedural and other requirements of the Data Practices Act. This responsibility must be performed in consultation with the affected agencies. The Department must be provided with sufficient resources to carry out this task.

Recommendation 17: The Data Practices Act should be amended to require that all government entities designate a Data Practices Compliance Officer or Officers who will be responsible for ensuring that the government entity is in compliance with the Data Practices Act. Each government entity should be required to inform the Department of Administration of the names, addresses and phone numbers of its responsible authority and compliance officer and must inform the Department of any changes.

Recommendation 18: The Legislature should appropriate sufficient resources to the Department of Administration to carry out the requirements of Minnesota Statutes Section 13.073, the public information policy training program.

Recommendation 19: The Data Practices Act should be amended to transfer all current duties and responsibilities of the Commissioner of Administration to an Office of Privacy and Freedom of Information. This office should also be given additional authority to investigate complaints brought by citizens and to resolve those complaints through alternative dispute resolution if possible, or by court action on behalf of the citizen if necessary.

Recommendation 20: The Legislature should amend Minnesota Statutes Section 13.072 to: provide that opinions of the Commissioner [or the Director of the Office of Privacy and Freedom of Information] are binding; authorize the Commissioner [or the Director] to bring an action in district court to compel a government entity to comply; and, authorize a government entity that disagrees with an opinion to seek a declaratory judgement that the opinion is not correct and need not be followed.

Recommendation 21: The remedies section of the Data Practices Act should be amended to provide for other means of resolving disputes, including mediation, arbitration or recourse to administrative law judges. Administrative law judges should be given the authority to award compensatory damages.

Recommendation 22: The Data Practices Act should be amended to require government entities, which contract out any of their functions to private sector persons, to include in those contractual provisions language that will ensure that the private sector persons administer data created, collected, received, stored, or maintained because of the contract in compliance with the Data Practices Act.

Recommendation 23: The Legislature, or some other body created by it, should study in greater depth a number of issues that the Task Force did not have time to fully consider. Those issues include:

A. Practical and other issues associated with implementation of the nonvisual access standards mandated by Minnesota Statutes Section 16B.104;

B. Utilization of surveillance technology and collection and use of data on individuals by the private sector;

C. Citizens' electronic interaction with government entities, including the classification, use, and dissemination of data collected in those interactions;

D. An ongoing process for reviewing information policy statutes; and,

E. The growing use by government entities of a variety of surveillance technologies and the effect of that use on citizens.

Summary/Conclusion

It is a common criticism of the Minnesota Government Data Practices that its content is excessively complex. The standard response to that criticism is that the content and language of the Act only reflect the complexity of its subject matter - information policy. Over the course of its work, the Task Force had the opportunity to review some aspects of the complex reality of government's collection, use and dissemination of data. During that review, the Task Force came to have some understanding of the complexity of issues associated with access to government data, privacy and fair information practices for citizens and the need for government to collect and use government data in a cost effective and efficient matter. The Task Force was often presented with very different views of perceived reality which depended entirely on whether the perspective of the presenter was that of a representative of a government entity or that of a citizen dealing with the government.

In response to the presentations from those widely varying perspectives, which were often perspectives that produced strong disagreements among Task Force members because they too shared those perspectives, the Task Force is able to make the following general conclusions.

There is no substantial sentiment to discard the State's Data Practices Act and to replace it with another model, for example, the federal "Freedom of Information Act."

There is general agreement, by both citizens and representatives of government entities, that using litigation to resolve disputes that arise out of information law and to enforce information policy law is ineffective for citizens and counterproductive for government agencies. Adoption of a variety of forms of alternative dispute resolution are much more preferable to resolve disputes and to promote compliance.

In most instances, representatives of government entities do their best to comply with information policy laws. However, there is an ongoing need for training for employees of government entities in what is actually required of them by information policy laws.

Not enough resources have been provided by the Legislature and other institutions of government to ensure that information policy laws are carried out so that citizens receive the benefits of these laws and government entities are not overly burdened by providing those benefits.

The resources that are allocated can be better spent if a stronger role is assigned to some organization at the state level that can assist both citizens and government entities in assuring that the objectives that the Legislature is trying to attain in the enactment of information policy laws are actually met.

Lastly, the Task Force concludes that the Information Society will continue to evolve and that most government entities will increase their collection and use of computerized government data. Those developments, when mixed with the ongoing clash of the interests of public access to government data, privacy and fair information practices for citizens and the need for government entities to make effective use of technology and of government data, will assure that public policy designed to deal with those developments and to accommodate and juggle those interests will continue to be complex.

II. Introduction

In the summer of 1997, the Minnesota Legislature and Governor Carlson asked eight citizens appointed by the Governor and the Legislature and four legislators to take on an immense task. These individuals, acting as an Information Policy Task Force were asked, over a period of about 18 months to study, among other things:

** issues related to surveillance and other forms of information technology, including the impact of technology on data practices and privacy;

** the content and organization of statutes dealing with access to government data, fair information practices and privacy; and,

** procedures for developing and implementing a coherent and coordinated approach to public information policy.

In other words, the Task Force was asked, in the words of one legislator, to take on a "truly daunting task" and to report on the results of that task to the Legislature. The Task Force has now completed its work and this report is the product of their study and deliberations.

In compliance with Minnesota Statutes Sections 3.197 and 3.302, the estimated cost for the preparation of this report is $20,000 and this report is submitted as required by Minnesota Session Laws 1997, Chapter 202, Article 2, Section 56.

III. The Information Policy Task Force

A. Task Force Creation and Composition.

The Information Policy Task Force was created by legislation enacted in 1997. During the 1997 legislative session, two separate bills were introduced, both of which had the general objective of creating a body to study the current state of information policy and to make recommendations for changes based on that study. One bill was introduced at the request of Governor Carlson. The other bill was introduced by the Senate and House Chairs of the subcommittees that deal with information policy, data practices and privacy in the Judiciary Committees of the Minnesota Legislature. Ultimately the two bills were merged into one and the resulting product was enacted into law as part of the omnibus state departments appropriations bill, Minnesota Session Laws 1997, Chapter 202 Article 2, Section 56. (A copy of the enabling legislation appears at Appendix 1 of this report.)

The enabling legislation created an Information Policy Task Force of twelve members. Membership was composed of four legislators, two from each party appointed through the normal legislative appointment processes, two citizens appointed by each house of the Legislature and four citizens appointed by the Governor. The Task Force was given a very broad charge to study and make recommendations concerning: the content and organization of information policy statutes, issues relating to the impact of technology on privacy and data practices; procedures for developing public information policy; approaches to information policy in other state and foreign jurisdictions; and other issues as determined by the Task Force.

Support for the Task Force was to be provided by the Department of Administration, the Office of Strategic and Long Range Planning, existing legislative resources and further assistance from the Office of Technology. The product of the Task Force's deliberations was to be a report to the Legislature. This report discharges that requirement and with the submission of this report, the Task Force ceases to exist.

B. Members of and Staff to the Task Force.

1. Members of the Task Force.

Between the effective date of the Task Force legislation on July 1, 1997, and October, 1997, the various appointing authorities appointed their members to the Task Force. The Minnesota Senate appointed Senators Betzold and Knutson and citizens Mr. Gene Merriam of Coon Rapids and Mr. Richard Neumeister of St. Paul. The Speaker of the House of Representatives appointed Representatives Broecker and Pelowski and citizens Mr. Thomas (Tim) Breza of Winona and Mr. Chris Sandberg of Minneapolis. Governor Carlson appointed: Ms. Anne Barry, the

Commissioner of Health; Mr. David Doth, the Commissioner of Human Services; Mr. John Gunyou, who at that time was the Director of the Office of Technology; and, Mr. David Johnson, the Chief of the Blaine Police Department.

On October 27, 1998, Chief Johnson resigned from the Task Force.

2. Staff of the Task Force.

Staff assistance to the Task Force was provided by: Mss. Kelli Johnson, Sandra Pizzuti, Onnalee Erickson and Mr. David Orren of the Minnesota Department of Health; Mr. Louis Thayer of the Minnesota Department of Human Services; Mss. Christine Yates and Michele Ford from Senator Betzold's office; Ms. Deborah McKnight from House of Representative Research; Ms. Kathleen Pontius from the Office of Senate Counsel; and Ms. Linda Miller and Mr. Donald Gemberling from the Department of Administration.

Although representatives of the Office of Strategic and Long Range Planning and the Office of Technology participated in some Task Force activities, those Offices did not provide substantial assistance.

C. Summary of Task Force Activities.

1. Preliminary Activities.

At its first meeting on October 30, 1997, the Task Force membership reviewed its charge from the Legislature, discussed the process of completing its work, elected Ms. Anne Barry the Chair and Mr. Gene Merriam the Vice-Chair and dealt with other organizational details. The Task Force agreed to meet monthly, at least during its initial deliberations.

At its meetings in the months of November, 1997, through January, 1998, the Task Force received background and other information from a variety of sources. Persons appearing before the Task Force included: resource experts from the Departments of Administration and Human Services; representatives of local government; a representative of the media community; and citizens, and attorneys representing citizens, who presented their views on how the Data Practices Act works in practice for citizens. Among the latter presenters was Mr. Gary Weissman who has also co-authored two law reviews on the Minnesota Government Data Practices Act. Mr. Weissman discussed problems of enforcement from a citizen perspective. His written materials are found in Appendix 2.

As one third of the Task Force was composed of legislative members, and a number of other Task Force members had significant roles to play during

the 1998 legislative session, the Task Force agreed that it would not meet until the end of the 1998 legislative session in April. Members of the Task Force were encouraged, during this hiatus in formal Task Force activities, to consider the charge to the Task Force and to acquire any information helpful to responding to that charge.

2. Task Force Chooses Six Critical Areas of Concern.

The Task Force resumed meeting on April 22, 1998. At that meeting, the Task Force conducted a facilitated discussion to establish priorities in order to accomplish the bulk of its work before the end of 1998. This discussion was facilitated by Ms. Judy Plante, the Director of the Management Analysis Division of the Department of Administration. This discussion provided the basic framework for a work plan and priorities for the Task Force. This framework included emphasis on examining six critical areas.

These six critical areas are:

- access to government data;
- fair information practices;
- enforcement of law;
- handling of electronic data including issues of surveillance and security;
- allocation of resources; and,
- development of information related law.

As a starting point for this examination, the Task Force decided to look at the principles that are implicit in existing information law with an eye toward validating, modifying or recommending elimination of those principles. The Task Force agreed to set aside a number of meetings to consider each of those areas and the existing principles, if any, associated with each area. To further facilitate completion of its work, the Task Force agreed to meet on a bi-weekly basis.

3. Task Force's Discussion of Two Important Principles.

From May through October, 1998, the Task Force focused much of its work on reviewing the existing principles which form the basis for current statutory information policy in Minnesota. The objective of this review was to determine whether current principles should be validated, modified or eliminated and whether new principles ought to be established. Two current principles in particular occupied much of the Task Force's attention.

The first principle considered at length by the Task Force is the presumption that all government data are public unless determined otherwise by the Legislature or the federal government. The second principle considered is the requirement that, in almost all instances when government entities are collecting private or confidential data from individuals, that those entities provide individuals with a notice about the information being requested. This notice is intended to help individuals decide whether they want to provide the requested data to the government and gives individuals a way to limit the uses and disseminations of the data once collected. (The latter principle is popularly known as the "Tennessen Warning.")

a. Presumption that Government Data are Public.

Some Task Force members expressed strong reservations about the presumption principle. In part, they felt it creates a legal reality, particularly in light of government's ever increasing collection of data about people, in which the privacy of individuals is increasingly compromised. Other members felt that the presumption really does not reflect the reality of Minnesota law. Although the presumption clearly exists and is clearly stated in Section 13.03, the presumption does not acknowledge that the Legislature has always been willing to decide that certain data are not public.

The general instances in which the Legislature historically has made data not public include the following: to establish privacy for and the protection of the security of individuals; to protect the integrity or to enhance the effectiveness of government programs; to comply with federal requirements; to protect confidentiality and security interests of businesses; and to protect the security of information or property. Legislative action to declare data not public is the primary driving force for the size and complexity of the Data Practices Act and other statutes. As long as the current presumption exists, as stated, that growth in size and complexity will continue.

The Task Force seriously considered a motion by member Johnson to modify the presumption so that it would state that all data on individuals are presumed to be not public but that data not on individuals would continue to be presumed to be public. On a 5-4 vote, the Task Force decided not to recommend a change in the current presumption. This close vote and the Task Force's very extensive discussion about this principle illustrate the difficulty of finding a simple answer to the issues associated with this principle.

b. Privacy Notice to Individuals.

The Task Force's discussion about the "Tennessen Warning" principle was far more controversial and protracted. The Task Force considered a written submission by the Public Law Section of the Bar Association. (The Public Law Section is an interest group of lawyers who represent public bodies and who have specific concerns about data practices and other information policy statutes.) A copy of this submission is found in Appendix 2.

The Task Force sought more detailed information about possible modifications to the "Tennessen Warning" principle and about enforcement of the Data Practices Act and other information law. As part of that inquiry, Task Force members thought it would be helpful to hear from attorneys who work in this field and who represent public bodies and citizens. Staff suggested that this presentation take the form of a debate.

On September 2, 1998, the Task Force heard a debate on two topics. The topics considered were: should the "Tennessen Warning" principle and the corresponding language in Minnesota Statutes be modified in any way; and, is litigation the best way to enforce information policy law? Debate participants representing government agencies were: Mr. James Moore, attorney for the City of Minneapolis, Ms. Tracy Smith, associate general counsel at the University of Minnesota, and Mr. Paul Ratwik, senior partner in a law firm that represents a number of school districts, counties and municipalities. Debate participants representing citizens were: Mr. Gregg Corwin, Mr. Marshall Tanick and Mr. Gary Weissman.

There was clear disagreement between the citizen and government agency sides on whether there should be any modification to the Tennessen Warning. The government attorneys strongly urged changes to the Tennessen Warning to make it, from their perspective, more practical and less restrictive for government agencies in two instances. Government attorneys specifically urged changes to the Warning when data are collected from public employees and when data are collected from students. The citizen attorneys strongly disagreed that any changes were needed. They argued that the current requirement is one positive way to give citizens, including public employees, students and their parents, a method to protect their privacy from the government. The complete text of this debate, reprinted from the "Legal Ledger" newspaper, is found in Appendix 3.

On the issue of whether litigation is the best way to enforce the Data Practices Act and other information laws, all of these attorneys were in agreement that litigation is not the best way to either bring about compliance or to resolve various kinds of disputes. Various forms of alternative dispute resolution were discussed. There was general agreement that any of the forms of alternative dispute resolution would be preferable to litigation.

4. Surveys to Determine Compliance.

In the course of reviewing current information policy principles, the Task Force identified the need to acquire information on how the principles were actually being dealt with, in a practical way, by both government entities and citizens. To that end, the Task Force asked staff to develop two different survey mechanisms. First, a written survey was developed and sent to a select sample of government agencies. Second, a "Sandberg Secret Shopper Survey" (named after the Task Force member who suggested this particular survey) was developed by staff. This survey was conducted by Task Force staff members and employees of the Minnesota Department of Health. The staff visited a variety of government entities and made certain requests for access to information.

The results of these two survey methods have been summarized and included as Appendix 4 of this report. Included with these summaries are blank copies of both the written and walk-in survey questions. It should be emphasized that the sample chosen for these surveys was small. The results of the surveys do not present statistically valid conclusions on the state of overall compliance with the Data Practices Act. However, the survey results do provide a helpful glimpse into the reality faced by a variety of agencies in administering the Act.

5. Research on Problematic Statutes and Issue of Electronic Surveillance.

Two additional legislative charges to the Task Force were also the subject of presentations, staff work and discussion by Task Force members. In response to the charge that the Task Force examine Minnesota Statutes for examples of inconsistent, contradictory and confusing provisions, staff of Senate Counsel, in consultation with staff of House Research and the Department of Administration, undertook to identify problematic provisions and to draft proposed amendments to deal with them. Research results and amendment drafts were reviewed periodically with the Task Force with the objective of including the results of this effort in the Task Force's report. This research and drafting is the subject of a recommendation by the Task Force and the actual product, in the form of draft legislation, is found in Appendix 5.

At its October 7, 1998, meeting, Don Gemberling made a presentation to the Task Force on the growing problem of electronic surveillance in society. This was followed by a presentation, by representatives of state agencies, on the process of doing data linkages for program evaluation and other purposes. The juxtaposition of these two presentations produced lively debate and discussion among Task Force members and the presenters. Some of the results of that discussion are found in the Task Force's recommendations on surveillance.

6. Compliance and Enforcement.

In November, staff presented to the Task Force, a variety of information about enforcement realities and the process of establishing information policy law. With that staff work before it, the Task Force began its deliberations about the administration of information policy laws, the enforcement of those laws and the process by which the laws come into existence.

In considering issues of enforcement, the Task Force looked at a variety of recommendations prepared by staff that focused on improving compliance with the Data Practices Act and on reducing the Act's reliance on citizen lawsuits as the primary method of enforcement in specific situations of dispute. In this discussion, the Task Force examined ways to make it easier and more effective for government agencies to comply, whether legal remedies ought to be changed, and whether there should be new or different methods or new or different organizations of government to assist government entities with compliance and citizens with actualization of their rights.

These discussions were the topic of discussion at the Task Force's meetings on December 2 and 16, 1998. The Task Force decided on a set of tentative recommendations in those meetings. The Task Force also concluded that it would be helpful to get public feedback on its tentative recommendations. The Task Force scheduled a public meeting for January 6, 1999, asked all persons who had previously made presentations to the Task Force and members of the public at large to appear at that meeting and provide written and/or oral commentary to the Task Force.

At the public meeting of the Task Force, twelve persons representing government agencies, a representative of the Minnesota Newspaper Association and one citizen appeared and presented comments. A number of other written comments were sent to the Task Force. All comments received by the Task Force are found in Appendix 9.

Following those presentations, the Task Force decided that it needed time to digest what it had heard, to review written

comments, to determine if any principles or recommendations should be revisited and changed, and to have another meeting. Concern was expressed that there might be negative reaction by the Legislature to the late filing of the Task Force's report. Senator Betzold was of the opinion that a reasonable delay so that the Task Force could review its work with the objective of producing the best report possible would not meet with criticism.

On January 19, 1999, the Task Force met to consider those recommendations that the staff, through analysis of written submissions to the Task Force, determined to be the most controversial. The Task Force reviewed staff comments, discussed the draft recommendations, made changes to some recommendations, and conducted some votes as to whether or not certain recommendations ought to be part of the report to the Legislature. After concluding those deliberations, the Task Force adopted this Report and approved its submission to the Legislature.

7. Summary/Conclusion.

It is a common criticism of the Minnesota Government Data Practices that its content is excessively complex. The standard response to that criticism is that the content and language of the Act only reflect the complexity of its subject matter - information policy. Over the course of its work, the Task Force had the opportunity to review some aspects of the complex reality of government's collection, use and dissemination of data. During that review, the Task Force came to have some understanding of the complexity of issues associated with access to government data, privacy and fair information practices for citizens and the need for government to collect and use government data in a cost effective and efficient matter. The Task Force was often presented with very different views of perceived reality which depended entirely on whether the perspective of the presenter was that of a representative of a government entity or that of a citizen dealing with the government.

In response to the presentations from those widely varying perspectives, which were often perspectives that produced strong disagreements among Task Force members because they too shared those perspectives, the Task Force is able to make the following general conclusions.

There is no substantial sentiment to discard the State's Data Practices Act and to replace it with another model, for example, the federal "Freedom of Information Act."

There is general agreement, by both citizens and representatives of government entities, that using litigation to resolve disputes that arise out of information law and to enforce information policy law is ineffective for citizens and counterproductive for government agencies. Adoption of a variety of forms of alternative dispute resolution are much more preferable to resolve disputes and to promote compliance.

In most instances, representatives of government entities do their best to comply with information policy laws. However, there is an ongoing need for training for employees of government entities in what is actually required of them by information policy laws.

Not enough resources have been provided by the Legislature and other institutions of government to ensure that information policy laws are carried out so that citizens receive the benefits of these laws and government entities are not overly burdened by providing those benefits.

The resources that are allocated can be better spent if a stronger role is assigned to some organization at the state level that can assist both citizens and government entities in assuring that the objectives that the Legislature is trying to attain in the enactment of information policy laws are actually met.

Lastly, the Task Force concludes that the Information Society will continue to evolve and that most government entities will increase their collection and use of computerized government data. Those developments, when mixed with the ongoing clash of the interests of public access to government data, privacy and fair information practices for citizens and the need for government entities to make effective use of technology and of government data, will assure that public policy designed to deal with those developments and to accommodate and juggle those interests will continue to be complex.

IV. Task Force Recommended Information Policy Principles

A. Existing Principles: The Starting Place for the Task Force's Deliberations.

To begin its discussion of which information policy principles ought to form the basis for information policy law in Minnesota, staff to the Task Force prepared a summary of the major existing principles that appear in Minnesota Statutes Sections 15.17 and 138.17, and in Chapter 13. Minnesota Statutes Chapter 13 is the "Data Practices Act," Section 15.17 is the "Official Records Act," and Section 138.17 is the "Records Management Act." These statutes contain the essential statements of information policy law that are generally applicable to all state agencies and most political subdivisions. A copy of this summary is found in Appendix 6.

B. Revised and New Principles.

In examining the summary of current information policy principles, the Task Force discussed whether, in its view, any existing principles should be discarded or modified. The Task Force also examined possible new principles drawn from staff recommendations and from the work of the Government Information Access Council. After considerable deliberation, the Task Force recommends that the following principles form the basis for the general statutory framework for regulating government information in Minnesota.

Principles presented in normal type are current principles in Minnesota Statutes which the Task Force determined should not be modified. Principles stated in **bold** type are either new principles being proposed by the Task Force or existing principles that the Task Force felt should be modified. Principles which the Task Force decided ought to be discarded are presented in an interlined format.

PRINCIPLES RELATING TO GOVERNMENT ACCOUNTABILITY[1]

1. Government entities must be required to keep at least some records and data that will document their official activities.

2. **Government entities should be able to copy and keep records and data that document their official activities in a variety of physical media that are efficient, but in media that facilitate public access.**

3. Certified copies of government records and data must have the same evidentiary weight and effect as original records and data.

4. **Custodians of government records must deliver all records, including computerized records, to their successors in office.**

---

[1]Drawn, in part, from Minnesota Statutes Section 15.17

PRINCIPLES RELATING TO THE PROPER DISPOSITION OF GOVERNMENT INFORMATION[2]

1. It is appropriate that the term "government data," as defined in statutes dealing with public access to data, not be the same as the definition of an official government record whose disposal is regulated by the Records Management Act.

2. Government Records subject to the Records Management Act must include records originated and maintained in electronic form.

3. An "official" government record should not be destroyed or otherwise disposed of unless the government entity holding the record complies with the Records Management Act.

PRINCIPLES RELATING TO THE PUBLIC ACCESS TO GOVERNMENT INFORMATION[3]

1. The public must be able to gain access to public government data, no matter what type of storage modality is chosen by the government to create, collect and store the data, as long as the data exist in some physical form, including computerized, video, paper, microfilm and all other forms of recorded data.

2. In a democratic society, government data should be presumed by law to be available for public access and examination to the greatest extent possible. Data held by the government should only be declared to be not public by statute, as required by federal law, or under the authority granted the Commissioner of Administration to issue temporary classifications of data.

3. Public government data must be kept and arranged so that they are easily accessible to the public.

4. **Government entities must establish and publish procedures to insure that requests for access to government data are complied with promptly and appropriately and to ensure that the public understands how to gain access to public data.**

5. **Public access to government information for the purpose of inspecting the data shall be at no charge to the person seeking to inspect the data. When a person asks for copies of government information, any**

---

[2]Drawn, in part, from Minnesota Statutes Section 138.17.

[3]Drawn, in part, from Minnesota Statutes Section 13.03.

charge for the copies shall not exceed marginal cost, which means that the cost of providing copies must exclude labor, overhead and development costs.

6. **Access by members of the public to government data in electronic form, using their own computers and incurring the cost of any communication charges, shall be considered inspection of government data at no cost to the public, regardless of whether the member of the public only examines the data in question, downloads the data, or prints a copy of the data.**

7. **With the limited exception of computer software, government data should not be copyrighted without express legislative approval.**

8. **To the greatest extent possible, public government data that are maintained in electronic form should be made available in electronic form to citizens who request data in that form. Government agencies should design and implement electronic government data systems in such a fashion that the public data contained in those systems are easily accessible for electronic use and copying by the public.**

9. **All citizens, regardless of geographic, physical, cultural, socio-economic status or other barriers, shall have equitable and affordable access to government information.**

10. **When a government entity contracts with a private sector entity to perform a government function, all data created, collected, received, stored and maintained by the private sector entity as it performs that function must be subject to requirements of the Data Practices Act.**

PRINCIPLES RELATING TO FAIR INFORMATION PRACTICES, I.E. "DATA PRIVACY."[4]

1. In order to function in an efficient and effective manner, and to advance the public good, government agencies must be able to collect and use data on individuals and businesses. All collections of data should be limited only to those necessary to administer and manage programs specifically authorized by the Legislature or mandated by the federal government.

2. **Collection, storage and use of data on individuals within a government entity must be limited to purposes authorized by the federal government, the Legislature, or local governing bodies.**

---

[4]Drawn, in part, from Minnesota Statutes Sections 13.04 and 13.05.

3. **Dissemination of not public data on individuals must be limited to purposes only as authorized by the federal government or by the Legislature.**

4. Government entities should not be able to share private or confidential data about individuals with one another unless there is statutory or federal legal authority to do so.

5. **In most instances when a government entity wants to collect private or confidential data from an individual, the individual must be told why the data are being requested; whether the data must be provided; what the consequences are of providing the data; what uses will be made of the data; and the identity of other entities to which the data will be disseminated. There are instances where it may be appropriate not to provide this type of notice to individuals. These instances include collections of criminal investigative data and certain collections of data from students and their parents and from government employees.**

6. Not public data collected from an individual should only be collected, stored, used and disseminated for those purposes communicated to the individual at the time the data were collected unless the individual gives informed consent, the commissioner of administration approves a change, or the Legislature or the federal government change the laws regulating what can be done with the data.

7. **Individuals must be able to inspect or to receive copies of public or private data about them immediately or no later than ten days after the individual makes a request to gain access.**

8. Government entities must assure, in their administration of data repositories and systems about individuals, that data on individuals are kept in an accurate and complete manner and that data on individuals are kept current for the purposes for which the data were originally collected.

9. Individuals must have the right to challenge the accuracy or completeness of public or private data maintained about them, to have that challenge acted on by the responsible authority within 30 days, and to be able to appeal the responsible authority's determination to a neutral party at the state level either for informal resolution, using conciliation, mediation or other alternative dispute resolution processes, or for formal resolution as a contested case matter under the Administrative Procedures Act.

10. **Except in those instances where there is a compelling public safety reason, a government agency should not acquire or implement technology that will enhance the capability of the agency to conduct**

surveillance of citizens unless the agency has given public notice of the acquisition or implementation of the technology. Public notice should be accomplished by notifying the Commissioner of Administration.

11. **Except when clearly authorized by state statute or federal law to do so, government agencies should not monitor citizen access to and usage of public government data. Monitoring includes the use of electronic "cookies" and similar techniques and requiring members of the public to identify themselves or to explain their reasons for seeking access to public government data. If a government entity chooses to use monitoring techniques, it must inform citizens that it is doing so.**

The Task Force determined that one existing principle should be discarded. The text of this principle, drawn from Minnesota Statutes Section 13.03, subdivision 3, is as follows:

> If the public requests a copy of an entire set of government data or a substantial and discrete portion of an entire set of government data in an instance where the government data has commercial value, the government entity may, in addition to charging for copies, charge an additional fee to recover its costs for developing the system of data.

V. Task Force Recommendations

Introduction

Based on the guiding information policy principles to which the Task Force agreed, the Task Force makes a number of recommendations that will serve, if implemented, to carry out the practical side of the principles. The Task Force also developed recommendations that grew out of their general deliberations. In these recommendations, the Task Force suggested certain specific activities or calls for new or different legislation. The Task Force's rationale for making each recommendation is also presented. In all instances where a Task Force recommendation would require legislative change, the Task Force, in Appendix 7 has drafted appropriate legislation.

For those recommendations that have budgetary implications, cost figures have been developed and those figures appear in Appendix 8.

A. RECOMMENDATIONS THAT RELATE TO THE INFORMATION POLICY PRINCIPLES

Recommendation 1: Minnesota Statutes Section 15.17 should be amended to reflect the reality that important government records are increasingly kept in media which are not paper.

Rationale: Minnesota Statutes Section 15.17 was first enacted in 1941. Since that time it has received minimal amendment. This section is the only section of general application which tells government entities that their duties include keeping at least some records, properly preserving those records and passing on those records to their successors in office. Although Section 15.17 makes reference to forms of record-keeping that are other than paper, it makes no explicit reference to computerized records. For that reason, and for the general purpose of updating this obscure but critical statute, the Task Force recommends that Section 15.17 be amended with language to update its provision to reflect the current reality of government record keeping and information processing.

Recommendation 2: More education and assistance should be provided to government entities so that entities can effectively deal with the proper disposition of government records. There is a particular and growing need to assist entities at all levels of government with the proper disposition of computerized records. The Department of Administration and the State Archives Department of the Minnesota Historical Society should work, in conjunction with government entities, to provide technical and policy

guidance and to provide on-going education on issues of electronic records management.

Rationale: Particularly when compared to Minnesota Statutes Section 15.17, the Records Management Act, Section 138.17 is much more clear in communicating to government entities that all forms of government records, including paper, disks, computer tapes, optical disks and so forth, must, at the end of their useful life, be disposed of pursuant to the Records Management Act. However, the accelerated pace at which government entities acquire and use computers to collect and maintain information, provide services and carry on correspondence, means that more and more government records are computerized. Increased computerization yields increased demands on government entities to answer to a variety of questions on how to fit computerized information into records management requirements.

Records management, on a statewide basis, is currently the responsibility of the Department of Administration. Because of its role on the Records Disposition panel and its responsibility for the state archives, the Minnesota Historical Society also has a strong interest in an effective records management program. These two entities are the logical place to deal with the increased demand for information and services concerning records management. They should be given resources adequate to address that task.

The primary purpose of the Records Management Act is to ensure that government records are preserved for auditing, legal and historical reasons and are disposed of only in a fashion that reflects preservation requirements. Without the kind of activity contemplated in this recommendation, these preservation requirements may very well not be met when the government records that Minnesota ought to be preserving are increasingly kept in computerized media.

Recommendation 3: The Data Practices Act should be amended to require each government entity to disseminate to the public, in some form, and at a minimum post in the entity's reception area, the procedures in effect in the agency which tell the public how to gain access to public government data. Those procedures should be updated as personnel and other changes occur.

Rationale: Currently, the Data Practices Act requires government entities to establish procedures to ensure that the public is able to gain access to public government data in an appropriate and prompt manner.

However, currently there is no requirement that those procedures be in writing. As government becomes more complex at many levels, it is imperative that the public be afforded the information it needs to be able to fully access the public data maintained by each agency. One way to assure that the public is afforded prompt and appropriate access to public government data is to require that public access procedures be in writing, that they be disseminated to the public in some reasonable fashion, including posting, and that they be updated to reflect agency personnel and other changes.

Recommendation 4: The Data Practices Act should be amended so that the charges that government entities can assess to the public for copying public government data are limited only to the marginal costs of providing the data in the form it is maintained by the government entity. The amendment should explicitly say that government entities should only be able to charge for the actual costs of making the copies and that those costs should not include labor, overhead and development costs incurred by the entity in providing the copies or maintaining the public data. Any government entity that has or receives specific statutory authority for charging more than marginal costs should be able to do so.

Rationale: Under the current language of the Data Practices Act, government entities may, in assessing the costs of providing copies of public data, include in that assessment ". . . the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling . . . the data . . . ." (Minnesota Statutes Section 13.03, subdivision 3.) As is attested to by a number of opinions of the Commissioner of Administration, this language has been the source of numerous disputes between government entities and citizens. These disputes focus on arguments about what the words "actual," "making," "certifying" and "compiling" really mean.

The reason for ensuring public access to government data is to advance the principle that in a democracy we should be facilitating the public's ability to monitor what its government is doing and to hold that government accountable. The policy on charging for copies for public data should facilitate the advancement of that rationale. It should not, as it does now, produce interminable disputes about proper charges. In some cases, limiting what government entities can charge for copies of data will have a positive financial impact on persons who make extensive use of government data for commercial and other purposes. However, this seems to be a reasonable price to pay for the greater good of

facilitating public access to government data for any and all purposes, commercial or otherwise.

Recommendation 5: The Data Practices Act should be clarified to explain that public access to public government data using on line inquiry methods including examination of data, downloading data or printing copies of data, is, in this electronic age, a form of inspection of data. This type of inspection of government data, just like inspection by visual examination of paper records, should be at no cost to the individual making the inquiry as long as the individual is bearing the costs of the communication hookup to the government entity. Note: this would not require a government entity to put data on-line. It would only require that data that are already on-line be available for inspection without charge.

Rationale: Inspection of government data at no cost to the person doing the inspection has been a fundamental principle of the Data Practices Act since 1981. The evolution of technology and how government uses technology have put a new spin on the realities associated with this principle. More and more government data are being made available on-line through web sites and other technological mechanisms. Increasingly, citizens seek to inspect government data that are available on-line, not by stopping at government offices to look in file cabinets, but by sitting down at a personal computer and reaching out to electronically look at the data. Sometimes, this looking causes the citizen to print the data at the citizen's location or to download the data being viewed into the citizen's own computer.

Except for the obvious technical difference, electronic access is a method by which the public can effectively inspect public government data. The Data Practices Act can be interpreted to mean that some of these methods of access to government data are actually acquisitions of copies of data for which the agency ought to be able to charge. However, the fact that an individual chooses to exercise their right to inspect public government data by "typing in" rather than "walking in" should not negate or modify that right. Over time, the use of computers will make requests for public access to data less of a burden to government agencies and more convenient to members of the public. The Data Practices Act should be modified to facilitate the promotion of the objective of convenient access.

Recommendation 6: The Data Practices Act should be amended to require government entities that want to copyright various forms of government data have legislative authority to do so.

Rationale: Currently, agencies of state and local government in Minnesota, unlike agencies of the federal government, are not prohibited from acquiring copyright protection for various forms of government data. The potential for government entities to make extensive use of this authority can have a serious and negative impact on the public's right to gain access to government data, including the right to acquire copies of the data, and to use that data in any manner. The growing practice of copyrighting government data will inevitably lead government entities to sue the State's citizens for copyright infringement and has the potential for discouraging public access to government data.

Given those potentially negative affects, government's practices in copyrighting data should be closely monitored for abuses. In light of existing principles which try to facilitate and encourage public access to government data, the Legislature is the best body to decide whether or not certain types of data should be copyrighted. Among other things, this will ensure that the public will have access to the process by which issues about the copyright of various types of government data are decided.

The Task Force does not intend that government entities be required to get copyright approval from the Legislature for every item that is copyrightable. The Legislature should establish a process for approving general copyright authority for various types of copyrightable information.

Recommendation 7: The Data Practices Act should be amended to specifically require that when government entities hold public government data in an electronic medium, the public should be able to acquire copies of the data in that electronic medium. Government entities should design and implement new government data systems so that public data are easily accessible for electronic use and copying by citizens.

Rationale: Currently the Data Practices Act does not authorize the public, when requesting copies of government data, to specify what form or media the copies should take. A government entity complies with a request for copies of data under the Act, as long as it provides copies in some medium even though that medium may not be one that can be used conveniently by the public. As a State,

we should be doing everything possible to maximize public access to and use of public government data. The societal value of increasing public access to and use of computerized data can best be advanced by a statutory change that would require government entities to, whenever possible, provide copies to the public of computerized data stored in an electronic medium in the medium in which the data are stored.

Recommendation 8: In authorizing any program intended to offer services and/or government information electronically, the Legislature should provide funding for any program intended to offer mechanisms that permit citizens to take advantage of the program whether or not they own or have ready access to electronic equipment.

Rationale: This recommendation is drawn from a principle adopted by the Task Force, which was first articulated by the Government Information Access Council (GIAC) in its 1996 report. The GIAC report contains detailed recommendations on methods by which Minnesota can avoid creating a situation in which there are information and services "haves" and "have nots." The Task Force strongly recommends that the Legislature, as it considers the funding for systems to provide electronic services and information, to establish and fund those recommendations.

Recommendation 9: The Data Practices Act should be amended to limit the authority of local government bodies to make decisions about disseminations of not public government data.

Rationale: In the current language of the Data Practices Act, local governing bodies are not authorized to make decisions about whether certain data should be public or not public. However, they are authorized to make decisions about the dissemination of not public data. The Task Force felt that the authority of a local governing body, by ordinance or resolution, to decide how not public data can be disseminated, was not consistent with the law that says local governing bodies are not authorized to make decisions about classification of government data. Therefore, the Task Force concluded that this inconsistency ought to be eliminated.

Recommendation 10: The Data Practices Act should be amended to change the notice requirements of Minnesota Statutes Section 13.04, subdivision 2, (the "Tennessen Warning") when the data being collected are private data about government employees or private data about students.

Rationale: Although the Task Force had sharp divisions of opinion about this recommendation, it was the consensus of a majority of Task Force members that collections of personnel and educational data should trigger the giving of a different form of the Tennessen Warning. The majority thought it would be sufficient if employees and students and parents received an appropriate Tennessen Warning at the beginning of an individual's employment or contact with an educational entity and at other critical times in the relationship such as collection of data for disciplinary purposes. The draft legislation that is being proposed will put these issues before the Legislature.

Recommendation 11: The Data Practices Act should be amended so that government entities should be required to provide data subjects with immediate access to data about themselves or to provide access within 10 days of the request of a data subject.

Rationale: Currently, the Data Practices Act states that when individuals attempt to exercise their rights to access to data about themselves government agencies must provide certain information, allow inspection of data and provide copies of data. Government agencies must respond immediately, or within five days of the request. If a government agency gives notice to the individual of a difficulty of responding within five days, they can then respond no later than ten days after the individual makes a request. After discussion of the practical aspects and implications of the current policy, the Task Force was of the opinion that the intermediate step of giving notice of the inability to respond within five days was a relatively meaningless exercise. The effect of this particular recommendation of the Task Force will be to eliminate the five day notice requirement while still providing for either an immediate response or a response not later than ten days after an individual's request.

Recommendation 12: The Data Practices Act should be amended to require government entities to report to the Commissioner of Administration the acquisition of any electronic device that will enhance the government entity's ability to conduct surveillance on citizens. Exempt from this requirement should be acquisitions of surveillance equipment for compelling public safety reasons.

Rationale: Over the last several years, government agencies have implemented a variety of electronic devices and related

capabilities, including such things as video cameras, on line monitoring of data access, ATM usage reports, interactive location sensors, and equipment that monitors e-mail transmissions and Internet transactions. Acquisition of these and similar devices greatly enhances the capability of government agencies to conduct surveillance of citizens.

Development of greater capacity and faster computers bring us closer to the day when even the most trivial events and incidents in every citizen's life may be captured for future retrieval and manipulation. Surveillance devices are acquired and implemented with little or no public notice or attention. The Task Force struggled with formulating what recommendations might be appropriate to address the government's use of surveillance technology. Giving public visibility to the growing impact that these devices can have on the lives of citizens has the potential for contributing to a dialogue about whether Minnesotans really do want to live in what one author has called a "surveillance society." Although "inelegant," in the words on one Task Force member, this recommendation attempts to make a small step toward beginning that dialogue.

Recommendation 13: The Data Practices Act should be amended to prohibit government entities from requiring citizens to explain reasons for or to justify access to public government data. Government entities should be able to ask citizens for names and other identifying information for the sole purpose of facilitating access to the data.

Rationale: The Task Force learned that it is fairly common practice for government entities to ask citizens who are seeking access to data to identify themselves and to state reasons for seeking access. Task Force members felt that asking citizens for some types of identifying information was reasonable as part of fulfilling the citizens' requests. However, there was general agreement that citizens should never have to justify their requests to access government data or to explain why they are seeking access and that government entities should not condition access on receiving justifications or explanations.

B. GENERAL RECOMMENDATIONS

Recommendation 14: A number of Minnesota Statutes should be amended to eliminate language that is inconsistent with the nomenclature and philosophy used in the Data

Practices Act. The Data Practices Act should be amended to reduce some of its complexity. Draft legislation to accomplish these tasks is found in Appendix 5.

Rationale: The Task Force was given the charge by the Legislature to examine the content and organization of a variety of Minnesota Statutes, including Chapter 13, that relate to information. The objectives of this examination were to determine if any provisions are obsolete or inconsistent and whether any provisions could be simplified. Staff to the Task Force conducted the detailed work associated with this examination and made recommendations in the form of draft legislation to the Task Force. If enacted, these draft legislative changes will deal with some problems of obsolescence, inconsistency, and complexity. Total consistency and simplicity are not attainable goals because the world of government information often presents very complex issues. Resolution of those issues by the Legislature and other policy makers may appear to produce inconsistent solutions. These seeming inconsistencies tend to disappear when the context in which the solution was formulated is examined and understood.

Recommendation 15: The Data Practices Act should be amended to repeal the provision that appears in Minnesota Statutes Section 13.03, subdivision 3, that authorizes government entities in some situations to charge, in addition to the normal fees for providing copies of government data, an additional fee intended to allow government entities to recover the development costs for producing systems of data that have commercial value.

Rationale: This recommendation grew out of the Task Force's discussion of existing principles of information policy and whether they ought to be changed. Some Task Force members felt very strongly that the statutory language which authorizes government agencies to charge an add-on fee operated as impediment to public access to data and particularly access to data held in electronic form. They also pointed out that tax dollars already go to pay for the development of systems. Use by government entities of the provision in existing law means that those members of the public receiving copies of government data who are charged the add-on fee, essentially end up paying twice for the development and implementation of the data system. Other Task Force members were of the opinion that the public, in general, benefitted from the application of the existing principle because it allows government

agencies to collect dollars from those who are receiving financial gain from the use of the data in these systems. After some discussion, the Task Force agreed, with dissent from some members, to adopt this recommendation.

Recommendation 16: The Department of Administration should be specifically charged, by statute, with the responsibility for preparing model policies, procedures, and forms in order to assist state and local government entities in complying with the procedural and other requirements of the Data Practices Act. This responsibility must be performed in consultation with the affected agencies. The Department must be provided with sufficient resources to carry out this task.

Rationale: In attempting to ensure that a number of policy objectives are met, the Data Practices Act requires government entities to prepare procedures, prepare and deliver notices and take certain actions. The extent to which a government entity has actually done the work required by the Act will great affect how citizens actualize their rights under the Act. For example, the right of a citizen to access public data held by government entities will be greatly enhanced if the citizen is able, before making any request, to know, by examining the policies and procedures of the entity, who s/he has to contact, where data are located, what the time frames are for receiving public data, and how, in general to go about making a request.

The Task Force learned that preparation of procedures and notices does not receive a particularly high priority from government entities. The work required of government entities is often looked upon as just another unfunded mandate. Oftentimes, citizens are frustrated in attempts to actualize their rights because government entities have not prepared the policies, procedures and notices associated that citizen can actually use to give practical meaning to their rights. The Task Force concluded that compliance with the Act could be significantly advanced by making the preparation of required policies and procedures less burdensome for government entities.

One way to do so would be to direct the Department of Administration to prepare model policies and procedures for government entities. The Department has the technical expertise to do so and is, on an informal basis, already helping government entities by reviewing policies and procedures. The Task Force also

concluded that it would be far more efficient if these policies and procedures could be prepared as models so that each of the 2000 plus public entities would not have to "reinvent the wheel" by acting on their own.

Recommendation 17: The Data Practices Act should be amended to require that all government entities designate a Data Practices Compliance Officer or Officers who will be responsible for ensuring that the government entity is in compliance with the Data Practices Act. Each government entity should be required to inform the Department of Administration of the names, addresses and phone numbers of its responsible authority and compliance officer and must inform the Department of any changes.

Rationale: Compliance with the Data Practices Act in its current version requires that each government entity not only have a responsible authority but have a responsible authority who acts in the manner contemplated by the Act. The Task Force learned that attainment of that objective is often frustrated because of a number of factors. There are occasions when government entities do not even appoint responsible authorities. In many cases, responsible authorities are actually the heads of government entities who have a number of higher and conflicting priorities. The original rationale for the Legislature's creation of the position of responsible authority in Chapter 13 was an attempt to assure that there would be one clearly identifiable individual in each government entity responsible for that entity's compliance. The Task Force believes that the underlying concept is still valid but that the concept can be better advanced by the specific designation of a compliance officer or officers in each entity.

Recommendation 18: The Legislature should appropriate sufficient resources to the Department of Administration to carry out the requirements of Minnesota Statutes Section 13.073, the public information policy training program.

Rationale: The Task Force received both testimony and written comments about the need for more and improved training for both citizens and government entities about information policy laws. Staff of the Department of Administration discussed the legislative history of Minnesota Statutes Section 13.073, including years of testimony to the Legislature about training needs, a consultant study that

was the basis for the legislation, and decisions by the Legislature to not fund the training program, but to compensate for that lack of funding by making the activities associated with the program permissive and not required. The Task Force determined that the best way to deal with the training issue was for the Legislature to provide sufficient resources to the Department of Administration to be able to carry out the details of the training plan contemplated in Section 13.073.

Recommendation 19: The Data Practices Act should be amended to transfer all current duties and responsibilities of the Commissioner of Administration to an Office of Privacy and Freedom of Information. This office should also be given additional authority to investigate complaints brought by citizens and to resolve those complaints through alternative dispute resolution, if possible, or by court action on behalf of the citizen if necessary.

Rationale: In its discussion of methods to better enforce the Data Practices Act, Task Force members discussed whether an agency of the government should be given a stronger role in enforcing the Data Practices Act. Although the Commissioner of Administration is assigned various duties under Chapter 13, the Commissioner is not given the authority to actually enforce information policy law in the sense of giving orders to government entities to act in conformity with the law. Task Force members extensively discussed whether it was appropriate and even workable to have the functions of education, advocacy, advice giving, opinion rendering and enforcement all in the same entity. Some Task Force members expressed support for the idea of an independent agency but expressed concern that given the some time political nature of information policy issues, that it was fundamentally important that an enforcing agency be as independent in its operation as possible.

A clear model of how to attain independence for such an agency is present in the Canadian system of privacy and freedom of information offices. Task Force members discussed the operation of the Privacy and Freedom of Information Commissioner for the province of British Columbia. (The GIAC report suggested the Legislature look at the British Columbia Office as a model of what Minnesota might want to do to better enforce information policy law.) Task Force members were concerned about and not receptive to the idea of having the independent agency function as part of the

legislative branch of government which is the case in the British Columbia statute and in many instances in Canada.

The Task Force concluded that the idea of an independent office was an idea whose time had come. There was some feeling that, if nothing else, proposing an independent office, both in this report and in a bill to be introduced possibly by legislative members of the Task Force, would make the idea of such an office part of the public policy discussion as to how best to enforce information policy laws. Therefore, a majority of the Task Force recommends the establishment of such an office, independent of all other state departments and agencies, and to be headed by a director appointed in a manner to be determined by the Legislature. The Task Force felt it was most appropriate for the Legislature to determine how this office should be organizationally located to most guarantee its independence.

Recommendation 20: The Legislature should amend Minnesota Statutes Section 13.072 to provide that opinions of the Commissioner [or the Director of the Office of Privacy and Freedom of Information] are binding; to authorize the Commissioner [or the Director] to bring an action in district court to compel a government entity to comply and to authorize a government entity that disagrees with an opinion to seek a declaratory judgement that the opinion is not correct and need not be followed.

Rationale: Advisory opinions of the Commissioner of Administration play a variety of roles. They inform citizens and government entities of the legal and practical meaning of various provisions of the Data Practices Act and other information policy laws. They provide an opportunity for the Department of Administration to share its expertise and knowledge of legislative intent in the area of information policy law with the courts and other interested persons.

One of the primary reasons for the enactment of the advisory opinion authority was to give citizens a simple and impartial forum in which, without having to incur the cost of an attorney and other costs associated with traditional legal actions, the citizen would be able to determine whether a government entity's interpretation of the law is correct. In practical terms, that objective is not met if a citizen receives an advisory opinion favorable to his or her position and the government entity who is the other party to the dispute resists the conclusion reached by the Commissioner.

After considering this dilemma and a variety of methods of dealing with it, the Task Force concluded that it would be appropriate if the Commissioner of Administration or, if Recommendation 19 were to become reality, the Director of the Office of Privacy and Information, were given the authority to issue opinions. The Commissioner or the Director should also be given the authority to seek enforcement of an opinion in a court of law. This would shift the burden of enforcing policy, made for all Minnesotans, from one taxpayer and citizen to all taxpayers and citizens. It might also increase the probability that opinions would be followed by government entities. They would know that not only is an opinion binding on them but that it will enforced by another government entity that has comparable legal and other resources.

Some Task Force members expressed concern that there may be reasonable disagreement on various points of the law. They felt that while changing the statute to make Commissioner's opinions binding and enforceable by the Commissioner was reasonable from a citizen's perspective, there should be a relatively simple way for government entities to challenge a Commissioner's opinion. The Task Force concluded that one way to do that was to authorize government entities to challenge a Commissioner's opinion by bringing an action for a declaratory judgement that the Commissioner's opinion is in error to a district court.

A motion to not make this recommendation failed on a vote of four (4) for and five (5) against.

Recommendation 21: The remedies section of the Data Practices Act should be amended to provide for other means of resolving disputes, including mediation, arbitration or recourse to administrative law judges. Administrative law judges should be given the authority to award compensatory damages.

Rationale: The Task Force heard a very strong message from citizens, from government entities and from attorneys representing both government entities and citizens that the current statutory provision that authorizes an action for damages was a very poor method of attempting to assure that government agencies comply with the Data Practices Act. A number of persons suggested that the Act should be amended to provide a variety of alternative dispute resolution mechanisms to resolve disputes. The Task Force heard that an action for damages was not particularly helpful to citizens because of the difficulty of even being able to prove damages in the wide variety of disputes that arise under the Act. The Task

Force also heard that the availability of an action for damages often caused government entities to be reluctant to release public data to the public and that the possibility of having to pay damages was a major cause of the "when in doubt, don't give it out" phenomenon that often drives government decision making.

After some discussion about making somewhat drastic changes to the remedies provision of the Data Practices Act, the Task Force agreed that the Act should only be amended to provide for alternative dispute resolution processes.

Recommendation 22: The Data Practices Act should be amended to require government entities, which contract out any of their functions to private sector persons, to include in those contractual provisions language that will ensure that the private sector persons administer data created, collected, received, stored, or maintained because of the contract in compliance with the Data Practices Act.

Rationale: The discussion of the underlying principle which produced this recommendation evidenced contrasting and strong points of view held by Task Force members. A number of members were concerned that increased privatization of a variety of government functions put those functions, and accountability for them, outside public purview because private entities are not subject to the Data Practices Act in most instances. There was some feeling that the availability of privatization sometimes made it easy for government entities to contract out functions to avoid public scrutiny. In contrast to that position, other Task Force members pointed out that contracting out government functions was an acceptable way of doing government business. They also pointed out that in some instances, contracting out and other activities that lead to the privatization of government functions makes up for the lack of resources available to government entities. Contracting with private sector persons allows government entities to acquire the capability and benefits of using technology when the money for technology innovation would not be otherwise available.

Recommendation 23: The Legislature, or some other body created by it, should study in greater depth a number of issues that the Task Force did not have time to fully consider. Those issues include:

A. Practical and other issues associated with implementation of the nonvisual access

standards mandated by Minnesota Statutes Section 16B.104;

B. Utilization of surveillance technology and collection and use of data on individuals by the private sector;

C. Citizens' electronic interaction with government entities, including the classification, use, and dissemination of data collected in those interactions;

D. An ongoing process for reviewing information policy statutes; and,

E. The growing use by government entities of a variety of surveillance technologies and the effect of that use on citizens.

Rationale: Late in its deliberations, the Task Force determined that there were a number of significant issues it would not be able to address. The Task Force decided that it would recommend that those issues be considered by the Legislature or some other body.

APPENDIX 1

Task Force Enabling Legislation
Minnesota Session Laws 1997
Chapter 202, Article 2, Section 56

Sec. 56. [INFORMATION POLICY TASK FORCE.]

Subdivision 1. [CREATION.] An information policy task force is created to study and make recommendations regarding Minnesota law on public information policy, including government data practices and information technology issues. The task force consists of:

(1) two members of the senate appointed by the subcommittees on committees on committees of the committee on rules and administration;

(2) two members of the house of representatives appointed by the speaker;

(3) four members appointed by the governor;

(4) two nonlegislative members appointed by the subcommittee on committees of the committee on rules and administration of the senate; and

(5) two nonlegislative members appointed by the speaker of the house of representatives.

At least one member from each legislative body must be a member of the majority party and at least one member from each body must be a member of the minority party or an independent.

Subd. 2. [DUTIES; REPORT.] The task force shall study:

(1) the content and organization of government data practices statutes in Minnesota Statutes, chapter 13, and related statutes dealing with access to government data, fair information practices and privacy;

(2) issues related to surveillance and other forms of information technology, including the impact of technology on data practices and privacy;

(3) procedures and structures for developing and implementing a coherent and coordinated approach to public information policy;

(4) approaches to information policy in other states and foreign jurisdictions; and

(5) other information policy issues identified by the task force.

In its study of statutes under clause (1), the task force shall include an evaluation to determine whether any statutes are inconsistent or obsolete.

The task force shall submit a progress report to the legislature by February 1, 1998, and a final report of its findings and recommendations, including any proposed legislation, to the legislature by January 15, 1999.

Subd. 3. [SUPPORT.] The commissioner of administration and the director of the office of strategic and long-range planning shall provide staff and other support services to the task

force. Legislative support to the task force must come from existing resources. The executive director of the Minnesota office of technology or the executive director's designee shall assist in the task force's activities.

Subd. 4 [COMPENSATION.] When authorized by the task force, members of the task force who are not legislators or full-time employees of the state or a political subdivision shall be compensated at the rate of $55 a day spent on task force activities, plus expenses in the same manner and amount as authorized by the commissioner's plan adopted under Minnesota Statutes, section 43A. 18, subdivision 2, and child care expenses that would not have been incurred if the member had not attended the task force meeting. A member who is a full-time employee of the state or a political subdivision may not receive the daily payment, but may suffer no loss in compensation or benefits from the state or the political subdivision as a result of service on the task force. A member who is a full-time employee of the state or a political subdivision may receive the expenses provided for in this subdivision unless the expenses are reimbursed by another source. A member who is an employee of the state or a political subdivision may be reimbursed for child care expenses only for time spent on task force activities that are outside their normal working hours.

Subd. 5. [EXPIRATION.] The task force expires upon submission of its final report to the legislature under subdivision 2.

APPENDIX 2

Written Submissions to the Task Force.

(Not available electronically.)

A. Submission from Public Law Section of Minnesota Bar Association.

B. Submission from Gary Weissman, Attorney at Law.

C. Submission from Advocates for Fair Information Practices.

UNIVERSITY OF MINNESOTA

Office of the General Counsel

By Fax and U.S. Mail

325 Morrill Hall
100 Church Street S.E.
Minneapolis, MN 55455
612-624-4100
Fax: 612-626-9624

April 21, 1998

Commissioner Anne M. Barry
Chair, Information Policy Task Force
Minnesota Department of Health
P.O. Box 9441
Minneapolis, MN 55440-9441

Re: *Minnesota Government Data Practices Act*

Dear Commissioner Barry:

We write on behalf of the Data Practices Committee of the Public Law Section of the Minnesota State Bar Association. The committee is composed of members of the state bar association who have an interest in data practices issues, including lawyers representing public clients such as state agencies, counties, municipalities, schools and universities, and law enforcement agencies. The committee appreciates the opportunity to present here some views regarding data practices. The committee would also appreciate the opportunity to meet in person with the Task Force. We propose having two or three members attend one of your meetings to answer questions and present ideas, and, if agreeable, we will work with the Task Force staff to arrange a time.

As lawyers familiar with the Data Practices Act, we appreciate the complexity of your task in proposing reform. The goals of the Data Practices Act — protecting the public's right to know while at the same time protecting the privacy rights of individuals and businesses, all in the context of promoting efficiency in government — too often conflict. And, as this conflict manifests itself in new circumstances each year, the Legislature has needed repeatedly to modify the Act and has attempted to anticipate each new circumstance that might materialize. Over time, this has resulted in a lengthy, complicated, and inflexible statute that is often difficult to apply. While the Task Force may respond to this problem with more systemic reform, our committee wanted to highlight several serious and concrete problems with the Act as it exists now.

Tennessen Warning.

The "Tennessen warning" imposes an almost impossible task on government with often little public value. The Tennessen warning had the laudable purpose of informing private citizens as to which government entities

would see their private information. The Tennessen warning, however, is increasingly being misused by persons as a defense to lawful government action. The Tennessen warning is being advanced as a sort of Miranda warning that carries an exclusionary rule even broader in scope than any found in criminal law. Not only is the Tennessen warning impeding the legitimate exercise of governmental authority, but increasing litigation in this area is prompting government entities to issue Tennessen warnings so broad and so all-inclusive as to become meaningless to the private citizens whose interests the warning was designed to protect.

A major problem area is public employment. Public employers increasingly see their employees assert "failure to provide a Tennessen warning" as a defense to disciplinary action for poor work performance or even illegal conduct. For example, an employee at the University of Minnesota was suspected of billing two departments for the same hours worked. The employee argued — and the Commissioner of Administration agreed — that the University of Minnesota violated the Data Practices Act by not giving the employee a Tennessen warning before asking her to identify the hours she had worked. (The Commissioner opined that whenever a supervisor asks a public employee for work-related information that could be used to evaluate the employee's performance, a Tennessen warning is required. Questions that would require a Tennessen warning under this reasoning include: Were you at work this morning? Why did you miss yesterday's meeting with the commissioner? What have you done on the project you were assigned? Where is the computer you signed out? Etc.) In another case, a former employee sued the University of Minnesota for violating the Data Practices Act when the University questioned him about a horse under his control and took adverse employment action when the employee revealed he had, in effect, stolen it.

The Tennessen warning presents problems in contexts other than public employment. Public schools face Tennessen warning issues all the time, as school officials find themselves asking such "private" questions such as who started the fight in the hall, where was a student who was missing during third period, and so on.[1] At a recent legal seminar, a presenter even advised school districts that they should provide a Tennessen warning to students and parents, advising them of the intended use of the students' *homework* and the consequences of failing to provide it. Although absurd, the Data Practices Act technically requires it.

[1] It is another flaw of the Tennessen warning requirement that law enforcement officials are exempt from giving Tennessen warnings, but other agencies, schools, employers, etc., that investigate potentially criminal conduct are not.

The Tennessen warning — especially the "exclusionary rule" that is being grafted onto it — needs, at the very least, to be subjected to a major overhaul. Before they have the information, government entities cannot always envision in advance every person or entity that might be authorized to receive the information (and, in circular fashion, only those entities identified in the warning are authorized to receive it). Moreover, the "exclusionary rule" is all out of proportion to the purpose of the warning and is inhibiting the government from taking appropriate action based on truthful information. In addition, the Tennessen warning does not belong in the arena of employee management — all public employees already know without formal warning that they may be questioned about their work performance and conduct, and the technicality of failure to provide a Tennessen warning should not be available to inhibit accountability of public employees.

Strict Liability for Government Entities.

Another important issue is the strict liability that is imposed on government entities for violation of the Act. Under the black-or-white system of the Data Practices Act, a given sheet of paper is either private or public, and the government entity is liable if it calls it wrong either way — regardless of the entity's good faith reason for its decision. The Data Practices Act, however, is not always susceptible of black-or-white interpretation — indeed, even the Commissioner of Administration has reached conclusions not upheld in court. Not every document is easily pigeonholed into only one classification of data. Documents of necessity often contain a mix of private and public information, or a mix of private information about different individuals (*e.g.*, virtually every investigation conducted for purposes of providing human services, resolving personnel disputes, etc.). In addition, even the same document (or the same piece of data within a document) can fit within more than one pigeonhole. For example, a sexually explicit videotape by a former public employee, which resulted in a conflicting Commissioner's opinion and court decision, could reasonably have been considered private personnel data (as the Commissioner concluded), public personnel data (as the court concluded), or civil investigative data as it was part of an ongoing series of lawsuits by the fired employee against the public entity.

Given the Act's all-or-nothing set up, the statute should be changed to stop the punishment of public entities (and thereby the public) for making a good faith, but ultimately incorrect, decision. The federal Freedom of Information Act (FOIA) is instructive in this regard. Under FOIA, attorney's fees are within the discretion of the trial court. Even when a plaintiff prevails under FOIA, the court may decline to award attorney's fees if the interest motivating the plaintiff was more private than public, if the plaintiff is gaining a commercial benefit from the information, or if the

government had a reasonable basis in law for its position. These factors should be introduced to data practices litigation, as the public should not have to pay for private interests when the government acted reasonably in interpreting an extraordinarily complicated law.

Data Practices Issues in Government Litigation.

The public interest is being poorly served by the interplay between the Data Practices Act and litigation against the government. Public entities are routinely litigants in contested matters. Agencies bring enforcement actions, individuals sue government entities, licensing boards bring actions against licensees, and so on. An important part of any litigation — as recognized in the oft-imposed requirement of alternative dispute resolution — is the confidential exploration and discussion of settlement among the parties. Confidentiality in settlement negotiations gives parties the space to explore creative and less costly solutions and reduces unnecessary and expensive litigation. While any ultimate settlement will be public and appropriately subject to public scrutiny, during the course of litigation parties must be able to engage in protected settlement discussions. At this point, however, the Commissioner has opined that proposed settlements exchanged with government entities are public data, even during litigation. Such a rule runs counter to the presumptive confidentiality of settlement discussions in other contexts, and puts government entities — and the public they represent — in an unfair position with respect to litigation. This rule needs to be changed.

A second issue in government litigation is the use of the Data Practices Act by private parties to a lawsuit to avoid the lawyers' ethical rule governing contact with represented parties. The practice of using data practices requests to do an end-run around the public's attorneys and the ethical rules is a disservice to the public and should be stopped. When a matter is in litigation against a government entity, the ethical rules should govern, and parties suing the government entity should be required to conduct their discovery/data practices requests through the entity's attorney.

Intellectual Property, Research Data, and Trade Secret Data.

The Act as presently written is insufficient to protect the legitimate intellectual property and trade secret interests of government entities and their employees. Government entities should be able to copyright their original work, yet there is a lack of clarity on this issue. The Attorney General has issued an opinion that conflicts with the Commissioner of Administration's advisory opinion on the topic. In addition to the copyright question, attention must be paid to protection of

public research. Unlike federal government regulations under FOIA, the Data Practices Act does not give specific protection to active, but unpublished, research data, even though premature disclosure of such data can ruin a public researcher's opportunity to publish, thwart a government entity's ability to patent and license an invention, and squander the public's investment in the research. The Data Practices Act also gives insufficient protection to the privacy interests of third-party research subjects — for example, protection of homeowners subject to research by the Pollution Control Agency for lead levels, or by the Metropolitan Airport Commission for noise levels. The public has a strong interest in encouraging government entities to engage in valuable research projects. The Data Practices Act must be amended to protect intellectual property rights in ongoing research and to permit agencies that perform research to deem as "private" sensitive information about research subjects.

Financial Information.

The Task Force should also consider the issue of protection of nongovernmental financial information. Proposals provided in response to government requests for proposals (unlike sealed bids) do not clearly enjoy protection under the Act during the proposal stage, discouraging some companies from participating in the RFP process. In addition, smaller, nonpublic companies are sometimes reluctant to seek out government contracts as their otherwise private financial data (provided to demonstrate that they are "responsible" bidders) may then be publicly available under the Data Practices Act.

Deliberative Process.

Two years ago, the Minnesota Legislature provided for a deliberative process exception for executive branch agencies in drafting legislative proposals. The Legislature recognized the need for agencies under the control of the governor to deliberate in private when drafting legislative proposals. Balancing this need against the public's right to know, the Legislature provided that proposals become public when agencies create their final draft. A deliberative process provision may serve the public in other areas, such as drafting rules, conducting investigations, and drafting reports. The Task Force should examine other areas where a deliberative process provision could be extended.

Corporate Licenseholder Data.

The Data Practices Act currently classifies licensing data as public, private, or confidential. Because no licensing data is assigned a classification for "data not on individuals," all licensing data on corporations is presumably public. This results in inequitable treatment for individual licensees and corporate licensees — while inactive investigative data of an individual licenseholder is private, inactive investigative data about a corporate licenseholder is not. The drafting flaw also harms the public's interest — while the licensing agency can hold investigative data about an individual licensee confidential during its investigation, it appears that even active investigative data about corporate licenseholders is public.

Five- or Ten-Day Deadline for Responding.

The Act's strict time-line for compliance with requests for access to data by the data subject (five or no more than ten days) fails to take into account the size of many government entities, the complexity of many of the record-keeping systems that are mandated by state and federal law, the frequent necessity of legal review and consultation prior to disclosure to ensure that other individuals' privacy rights are protected, the need to redact private information, and so on. Even Commissioner's opinions, which come to the Commissioner relatively neatly outlined and often already researched, take twenty and often fifty days to issue. Yet public entities and their lawyers are supposed to gather all the data, review it and make legal determinations, redact where appropriate, and reproduce the data all within five or ten business days of receiving the request. It is often not realistic.

Burdensome Requests.

At present, the Act provides no protection of the public interest from burdensome data requests. Too often, government entities spend untolled numbers of hours gathering thousands of documents to satisfy, at public expense, the personal interests of one requester. Some requests are so broad as to be impossible to respond to without combing virtually every file within the institution. There is nothing in the Act requiring requesters to identify with some specificity the type of documents requested (as opposed to under FOIA), and there is nothing in the law to give a court or some other neutral body the discretion to manage burdensome or harassing requests. The Task Force should address the real costs to the public of compliance with the Data Practices Act and consider means to distribute or manage those costs in the public's interest.

Accuracy and Completeness Hearings.

The accuracy and completeness challenges permitted by the Act have posed difficult problems for government entities. At present, there is no "statute of limitations" for challenging the accuracy and completeness of government data — information that is decades-old can still be challenged even if there are no longer any witnesses available to testify concerning the data. In addition, the law does not give clear guidance to administrative law judges regarding the burden of proof in accuracy and completeness challenges, resulting in confusion and inconsistency in this area of law. Other problems include the unresolved question whether decisions in other administrative proceedings take precedence over accuracy and completeness hearings, slowness in the administrative process resulting in stale claims, and the unlimited scope of data that may be challenged for accuracy and completeness, including such things as doctors' notes in public hospital records, grades and homework evaluations at public schools, etc.

Uniform Costs for Copies.

A minor issue is the recovery of copying costs under the Act. At present, numerous advisory opinions by the Commissioner of Administration address the issue whether a government entity has factually established its *actual* cost of reproducing documents (considering factors such as the actual cost of paper, the depreciation of copying machines, the salary of person making copies, etc.). To avoid the unnecessary use of government time and money to calculate and defend the costs of copies, the law should be changed to permit government entities to charge reasonable rates.

Review for Consistent Language.

Doubtless because of the numerous amendments made to the Act over time, some sections of the Data Practices Act apparently misuse terms that are terms of art under the law, or inexplicably make some information "confidential" when "private" would make more sense. Examples include the Tennessen warning, Minn. Stat. § 13.04, subd. 2, and the section addressing property complaint data, Minn. Stat. § 13.44. The entire Act needs review to make sure that the classification terms used are appropriate in each context.

Thank you for the opportunity to present these comments to the Task Force on behalf of the bar association's Data Practices Committee. We hope to contribute

to your difficult but important task of improving the Data Practices Act for the public good.

Very truly yours,

Tracy M. Smith
Associate General Counsel
Co-Chair, Data Practices Committee
Minnesota State Bar Association

Brian J. Asleson
Assistant County Attorney for
Wright County
Co-Chair, Data Practices Committee
Minnesota State Bar Association

TMS

DATA PRACTICES TASK FORCE

Weissmanesque suggestions

▸ *Recognize* that the most valuable thing government agencies possess is information;

*****

▸ *Accept* that any statute attempting to achieve what Karl Menninger, in another context, called the "vital balance" among the public's right to know, individuals' right to privacy, and government agencies' need to carry out their missions will necessarily be complicated.

*****

▸ ***Keep your eyes on the prize:*** The Task Force needs to remain focused on the larger policy issues and should resist being led into blind alleys which will divert the Task Force's energies into fine-tunings.

*****

▸ *Define the task* in a way that will enable you to comment on (and recommend) intelligently about the key policy frameworks:

- ~ Open records;
- ~ Privacy & due process;
- ~ Restricted access;
- ~ Govt. accountability & remedies.

*****

▸ ***Establish*** user-friendly processes for citizens:

(a) sanctions for governmental non-compliance;
(b) easy enforcement mechanisms;
(c) institutionalized A.D.R. (pre-suit);
(d) an ombudsman spin on Commissioner's Opinions;

*****

▸ *Propose that the Legislature*:

(a) adopt Bill Safire's suggestion of a Privacy Impact Statement in every new piece of legislation;

(b) create a Joint Legislative Commission on Information Policy to ensure uniformity in nomenclature, classification, and policy.

(c) authorize an **independent FOIA\Privacy Commission.**

CITIZEN FRUSTRATIONS WITH GOVERNMENTAL RESPONSES UNDER THE DATA PRACTICES ACT

//	*NATURE OF PROBLEM*
1	**COLLECTION**: Agencies collecting data which are not necessary to operate. <No adequate remedy>
2	**INADEQUATE TENNESSEN WARNINGS**: Either not given (and the failure trivialized); or data subjects provide what's requested for fear of not getting services.
3	**DISCLOSURE DELAY**: Foot-dragging on the release of public or private data <only relief is an expensive lawsuit, which only the media can afford>.
4	**NOSE-THUMBING AT COMMISSIONER'S OPINIONS**: A citizen obtains a Commissioner's Opinion interpreting the law in favor of the citizen; the agency responds, "we disagree." <no adquate remedy>.
5	**EXPENSIVE RIGHT TO CONTEST**: If a citizen wants to contest the accuracy of data which an agency maintains on him or her, s/he can have an evidentiary hearing in front of an ALJ; but the citizen has to underwrite the legal fess while the agency gets free legal services.
6	**HIDDEN DATA**: The statute does not distinguish between official files and "desk drawer" files; but some agencies wink at the practice of supervisors' maintaining files on employees -- and citizens -- whose existence they deny when formally requested.
7	**WHEN IN DOUBT, DON'T GIVE IT OUT**: Fearing lawsuits over what they deem a pesky and complex law, many agencies simply refuse to turn over public data, notwithstanding the Legislature's and the Supreme Court's having declared that public accessibility is the core concept of the statute.
8	**CONFLICT OF INTEREST**: The interpreter of the law in most agencies are the County Attorneys (or the Attorney General), who define their roles as defending the governmental agency rather than enabling citizen access or the protection of citizen privacy. Despite the statutory threat of criminal punishment for violation of the law, only county attorneys and the A.G. can prosecute; as a result, no one is.

9	**CATCH 22**: The law (§13.39) exempts active investigative data from disclosure; government lawyers argue that if someone asks for data, by definition those data are part of an active investigation retained in anticipation of a civil legal action -- which they "anticipate" precisely because of the request.
10	**LEGAL ESOTERICA**: Tens of thousands of tax dollars are expended each year on legal briefs arguing such esoteric concepts as mootness, standing, justiciability, and immunity -- to avoid dealing with the issues on their merits.
11	**FOXES IN CHARGE OF THE CHICKEN COOP**: If a citizen wants to know what his or her rights are under the MGDPA without having to pay a private attorney, the only people to ask (namely, government officials) are the very ones whose conduct the law was enacted to restrict.
12	**GENERAL NON-COMPLIANCE**: The Legislature hoped that by delineating several specfic compliance requirements in the statute, most government agencies would become sensitized to the important information policy issues. Twenty-four years after the enactment of the statute, most agencies are still not in compliance, and there is no easy way to enforce compliance.

ADVOCATES FOR FAIR INFORMATION PRACTICES
c/o Gary A. Weissman
701 Fourth Avenue South, #500
Minneapolis, MN 55415

August 5, 1998

Hon. Anne Barry, Chair
Information Policy Task Force
c/o Minnesota Department of Health
P.O. Box 9441
St. Paul, MN 55440

re: ***MGDPA***
AFIP's Reply to the Govt. Lawyers

Dear Commissioner Barry:

The ADVOCATES for FAIR INFORMATION PRACTICES ("AFIP") respectfully submits this reply to the Letter dated April 28, 1998, by the MSBA's Public Law Section's Data Practices Committee ("Government Lawyers").

The Government Lawyers propose that the task force which you chair ought to seek 14 discrete modifications in the Minnesota Government Data Practices Act ("MGDPA"). The chart below reflects our views on these same topics; but they are organized in a different sequence.

ISSUE	*Govt. Lawyers say:*	*AFIP replies:*
A.	**MATTERS ON WHICH WE AGREE**	
3) Settlement Discussions[1]	Settlement proposals, notes, offers, demands should be protected from disclosure so long as the ultimate settlement is subject to public scrutiny.	This makes sense. We would support such a change.
5) Public Research[2]	Unpublished research should be protected from copyright, patent, and license infringement.	We agree that academic research should receive protection -- so long as government agencies cannot refuse to disclose "policy papers" by calling them "public research."
14) Consistency in Language	Classification terms should be consistent throughout the statute.	We are in full agreement.

[1] The Government Lawyers include "Settlement Discussions" as a subset of their third bolded paragraph, entitled "Data Practices Issues in Government Litigation."

[2] The Government Lawyers' bolded fourth paragraph, "Intellectual Property, Public Research, and Trade Secret Data" contains three separate concepts.

B. MATTERS ON WHICH THERE MAY BE COMMON GROUND		
ISSUE	**Govt Lawyers Say:**	**AFIP Replies:**
6) Sensitive data about research subjects	Agencies should be able to engage in valuable research without having to expose the research subjects to the glare of public access	We agree that such research serves the public interest and that the law should protect the privacy of individual research subjects. **HOWEVER**, to preclude governmental agencies from keeping information out of the public domain simply by characterizing it as "sensitive research data,"some entity other than the governmental agency itself must make the determination. Perhaps a separate Commissioner of Fair Information Practices, or an Ombudsman.
7) Financial Information	The statute should protect financial info. from private bidders in RFPs.	We agree that proprietary and financial information about the bidders should be protected; **BUT** there should be no blanket protection for the bidder's proposal, bid, or budget.
8) Deliberative process	Rule drafts, report drafts, and investi-gations should be classified as "not public."	**IT DEPENDS:** Rule drafts and report drafts should be part of open government <It's too late for the public to comment if only the final draft is made public>. On the other hand, facilitative processes where two or more agencies' interests need to be harmonized ought to be protected.

ISSUE	Govt Lawyers Say:	AFIP Replies:
9) Corporate Licenseholder data	The MGDPA inequitably treats licensees, depending on whether they are individuals or corporations.	They may be right: We'd like to hear more details.
C. FUNDAMENTAL DISAGREEMENTS		
1) Tennessen Warning	Overhaul the exclusionary rule.	THE EXCLUSIONARY RULE IS THE ONLY REAL PROTECTION DATA SUBJECTS HAVE AGAINST OVERBEARING AND INTRUSIVE GOVERNMENTAL INTERROGATIONS
2) Strict liability	Deny fees to prevailing plaintiffs unless they can prove bad faith.	GOVT. AGENCIES GET FREE LEGAL REPRESENTATION. PLACING THE BURDEN ON PLAINTIFFS WOULD EVISCERATE THE ENFORCEMENT OF THE LAW.
4) Discovery[3]	**Plaintiffs should not be allowed "end runs" around the ethical rules.**	**THE GOVT. LAWYERS' PROPOSAL WOULD VIOLATE THE EQUAL PROTECTION CLAUSE -- PROHIBITING CITIZENS FROM SEEKING GOVERNMENT DATA JUST BECAUSE THEY ARE SUING, OR BEING SUED BY, A GOVT. AGENCY.**
10) Deadlines	The 10-day deadline for responding to requests is unrealistic.	IN MOST CASES, 10 DAYS SHOULD BE ADEQUATE TO FIND DATA IN FILES. THE REAL PROBLEM IS THAT COURTS DON'T PUNISH AGENCIES FOR TARDINESS.
11) Burdensome requests	The law should permit agencies to tax the real costs of assembling public data in response to requests.	THE GOVT. AGENCY CANNOT OBJECTIVELY DISTINGUISH BETWEEN BURDENSOME REQUESTS AND INEFFICIENCY. SOME INDEPENDENT ENTITY SHOULD MAKE THE DETERMINATION.

[3] Listed as the "second issue" in the Government lawyers' paragraph entitled "Data Practices Issues in Governmental Litigation."

ISSUE	Govt Lawyers Say:	AFIP Replies:
12) Accuracy hearings	[no specific proposal] Concerns about statutes of limitations, burden of proof, stale claims, scope of challenge, etc.	THE ONLY REASON GOVERNMENT COLLECTS DATA IS TO USE THEM TO MAKE DECISIONS. WHATEVER DATA GOVT. HAS SHOULD BE ACCURATE. A SUCCESSFULLY CHALLENGING DATA SUBJECT CANNOT RECOVER ATTORNEY FEES, BUT A LOSING STATE OR COUNTY GOVT. AGENCY IS ENTITLED TO FREE REPRESENTATION.
13) Photocopying costs	Let the Government charge reasonable rates.	WHO DETERMINES WHAT IS "REASONABLE?" WHY SHOULD ANY GOVT. CHARGE MORE THAN KINKOS DOES FOR PHOTOCOPYING?

Should the task force want to have any or all of these issues aired, AFIP would be willing to engage in a public debate with representatives of the Government Lawyers for the Task Force's benefit.

As a professional courtesy, we are providing the signers of the Letter from the Government Lawyers with a copy of this letter. We should be grateful if the Task Force would ensure that AFIC receives copies of any further correspondence from the Government Lawyers. Thank you in advance.

Respectfully,

Gary A. Weissman
President

Greg Corwin
Vice President

Marshall Tanick
Reconditer

ISSUE	Govt Lawyers Say	AFIP Replies
12) Accuracy hearings	[no specific proposal] Concerns about statutes of limitations, burden of proof, stale claims, scope of challenge, etc.	THE ONLY REASON GOVERNMENT COLLECTS DATA IS TO USE THEM TO MAKE DECISIONS. WHATEVER DATA GOVT. HAS SHOULD BE ACCURATE. A SUCCESSFULLY CHALLENGING DATA SUBJECT CANNOT RECOVER ATTORNEY FEES, BUT A LOSING STATE OR COUNTY GOVT. AGENCY IS ENTITLED TO FREE REPRESENTATION.
13) Photocopying costs	Let the Government charge reasonable rates.	WHO DETERMINES WHAT IS "REASONABLE?" WHY SHOULD ANY GOVT. CHARGE MORE THAN KINKOS DOES FOR PHOTOCOPYING?

Should the task force want to have any or all of these issues aired, AFIP would be willing to engage in a public debate with representatives of the Government Lawyers for the Task Force's benefit.

As a professional courtesy, we are providing the signers of the Letter from the Government Lawyers with a copy of this letter. We should be grateful if the Task Force would ensure that AFIC receives copies of any further correspondence from the Government Lawyers. Thank you in advance.

Respectfully,

Gary A. Weissman
President

Greg Corwin
Vice President

Marshall Tanick
Reconditer

ISSUE	Govt Lawyers Say:	AFIP Replies:
12) Accuracy hearings	[no specific proposal] Concerns about statutes of limitations, burden of proof, stale claims, scope of challenge, etc.	THE ONLY REASON GOVERNMENT COLLECTS DATA IS TO USE THEM TO MAKE DECISIONS. WHATEVER DATA GOVT. HAS SHOULD BE ACCURATE. A SUCCESSFULLY CHALLENGING DATA SUBJECT CANNOT RECOVER ATTORNEY FEES, BUT A LOSING STATE OR COUNTY GOVT. AGENCY IS ENTITLED TO FREE REPRESENTATION.
13) Photocopying costs	Let the Government charge reasonable rates.	WHO DETERMINES WHAT IS "REASONABLE?" WHY SHOULD ANY GOVT. CHARGE MORE THAN KINKOS DOES FOR PHOTOCOPYING?

Should the task force want to have any or all of these issues aired, AFIP would be willing to engage in a public debate with representatives of the Government Lawyers for the Task Force's benefit.

As a professional courtesy, we are providing the signers of the Letter from the Government Lawyers with a copy of this letter. We should be grateful if the Task Force would ensure that AFIC receives copies of any further correspondence from the Government Lawyers. Thank you in advance.

Respectfully,

Gary A. Weissman
President

Greg Corwin
Vice President

Marshall Tanick
Reconditer

APPENDIX 3

Full Text of Public/Private Attorney Debate from the "Legal Ledger"

Information Policy Task Force

Expert debate on Tennessen Warning, 9/2/98
Originally Published 9/10/98, St. Paul Legal Ledger

As part of its review of the Government Data Practices Act, the Information Policy Task Force convened a group of lawyers to debate whether the Tennessen Warning should apply to public sector employment relationships.

The 20-year-old law requires that government employees explain how information will be used when requesting private data from individuals. Its application to the public workplace was not contemplated at the time, but recently failure to give a Tennessen Warning has been used as a defense by employees facing discipline.

Representing governmental entities were Jim Moore, assistant city attorney in Minneapolis; Paul Ratwik, whose law firm represents 150-plus school districts; and Tracy Smith, associate general counsel for the University of Minnesota. They were dubbed Group A.

Representing public employees were Gregg Corwin, who represents public unions; Marshall Tanick, a faculty member at the University of Minnesota, an administrative law judge and an attorney specializing in labor, employment and constitutional law; and Gary Weissman, an adjunct professor of alternative dispute resolution at William Mitchell College of Law and an attorney working in family law, employment law and data privacy. There were dubbed Group B.

The question posed by the task force: "There are concerns that giving the Tennessen Warning in educational and employment settings produces results that seem to lack common sense. Given these concerns, should those individuals be exempt from the Tennessen Warning or should language be drafted to avoid nonsensical/absurd results? Or is there another way?"

Panelists gave opening statements and then questioned each other.

[Group A is in regular type; Group B, in italics.]

Jim Moore: Should the Tennessen Warning language be amended as it applies to the educational and employment context? Yes, absolutely. ...

The first question is: What is the public policy that is sought to be served by the imposition of the Tennessen requirement in the Data Practices Act? And the answer to that question, as I see it, is that you want individuals to have fair notice when they're asked to provide private data, particularly about them, about the use that the government is going to put that data to.

If you are an applicant for public assistance, and you are asked to provide income-information private data about you, shouldn't you have the right -- and clearly the law recognizes the right -- to be told why it is that the government entity that's collecting the data needs the data, what the consequences of refusing to provide are, and what use it will be put to? That makes sense in that context.

It doesn't make sense in an employment context where we have, Section 13.43, which makes in the employment context virtually every contact between the employer and the employee private data. The task force is well aware of the requirements of 13.43; the task force knows that there's a laundry list of things that are public, and everything else in the important relationship is presumed private data under Section 13.43.

So the question is, does the public policy underlying the Tennessen requirement serve any legitimate purpose in that context? Now let me suggest to you that it does not.

The reason for that is that I, as a public employee, or other public employees, clearly know that when they're dealing with their bosses that the information that they're providing is to be used to complete a task and to analyze the completion of the task that was assigned. We all know when we get assigned something by our boss that it is to be done to a particular professional standard and that we're subject to having that performance reviewed.

How is that done in the real world? That is done by, in my case, the city attorney walking by my door and saying, "Jim, you know that memo I asked you to do for the city council? Do you have that done yet?" Does the city attorney have to give me a Tennessen Warning every time we have that conversation? In the real world, it's not done. Nor should it be.

I as a public employee coming into public employment know that I'm protected by the Data Practices Act. I know there are certain things about me that aren't available to the public. ... That's not to say it should not be available to my employer without a bunch of hoops being jumped through. The idea of public employment is to get the public's work done. ...

Does the public employer know at the time that they're gathering information from me or other employees what the potential classification of the data is? The Tennessen Warning applies when an individual is asked to provide private or confidential data. If my boss asks me, "What time did you get in this morning?", that's work hours, which is public information. If the purpose of asking that question is to document that I'm never on time ... it will be used in a private context later.

There are a myriad of situations in which individual supervisors in the real world are going to be asking their employees to provide information that may, *at some point*, be private or confidential data, depending that they don't know at the time they asked the question.

For example, a police sergeant arrives on the scene of a police shooting, and goes up to an officer holding a gun, and says, "Did you fire your gun, officer?" Answer: "Yes sir, I did." "What happened?" Answer: "The other individual pointed a gun at me, sir. I discharged my weapon." "Give me your gun; go sit in the squad car."

What data was that? Was that law enforcement data that's confidential? Is it personnel data under 13.43? Will it become public law enforcement data when the investigation, whatever that might be -- into either the other actor's conduct, or the police discharge of a weapon -- is resolved? That supervisor in the real world doesn't know the data classification. We sitting here in this pristine room don't necessarily know.

To impose a Tennessen requirement and then impose a remedy that says if you collected the data without giving a Tennessen Warning you can't use it for any purpose, is not in the best public interest. If the answer is "Yes sir, he pointed a gun at me," and further investigation reveals that the individual who was shot had no gun, never pointed it and there are a myriad of other witnesses, that's a criminal offense by my hypothetical police officer. Are we to be told that his false answer to his supervisor can't be used either in the employment context or in the prosecution of that criminal offense?

That seems to be the result when you impose the requirement -- that makes sense when you're filling out forms -- to the conversations occurring within a real world situation in the employment context.

Tracy Smith: We are here not to, trying to change practice in public employment but rather to stem a novel and growing use of the Tennessen Warning as a defense to disciplinary action. ...

Public employees literally are arguing now, and the commissioner of administration agrees, that public employers cannot ask employees questions about their work performance or

conduct without first giving them a Tennessen Warning because those questions might be -- and I'll quote from the commissioner's opinion -- "relevant to a legitimate evaluation of the employee's performance."

So if you ask an employee any question that will become relevant to an evaluation of that employee, a Tennessen Warning will be required. That, to me, means every virtually question and every interaction that I have or I receive in my office connected to my work.

Let me give you some real world examples, because we don't have to work in the world of hypotheticals here, unfortunately.

The commissioner's opinion that gave rise to this issue came about because the university had a clerical employee that apparently was double-billing two departments for the same hours worked. The university's response: Ask the employee, "What hours were you working? Were they reported on the time sheet? What work were you performing?" The university had considered discipline. There was an investigatory meeting with a representative of the employee pursuant to her union contract. ...

The employee argued to the commissioner, and the commissioner agreed, that the university violated that employee's rights by asking her about the hours she worked without giving her a Tennessen Warning. ...

And the reason for that was, there were two alternative rationales, but one rationale was because those questions ... were actually going to be -- surprise! -- relevant to an evaluation of that employee. And the commissioner went one step further deciding not only did it violate the act ... but taking the criminal Miranda exclusionary rule even one step further, decided that the university had to go ahead and destroy all the documents that reflected this employee's responses to questions about her work. Well, that case resulted in discipline; it didn't end up resulting in further litigation. ...

However, based on that opinion, we now have a court case that we're defending.

This is an employee of the University of Minnesota, a professor of veterinary medicine, who got a family to donate a sick horse to the university. The family took a deduction on their tax returns, and so forth. This professor then treated the horse, cured it, turned around to sell it for his own personal profit, for himself. His supervisor, an assistant dean, heard talk of it and asked the employee about this ... and the employee acknowledged that he planned to sell it himself and keep the money. Needless to say ... the horse was returned to the university, and the university sold it.

This same employee also was accused by a student and advisee of sexually propositioning her. Later this employee asked for tenure -- permanent, lifetime appointment to the university -- and was denied.

He has sued the university for every manner of private action -- ... breach of contract, defamation ... violation of the Data Practices Act. Why? Because he was not given a Tennessen Warning that his statements about theft of property and sexually propositioning an advisee might actually be relevant to an employer deciding whether to grant him lifetime employment ...

Now we've been to district court three times, the Court of Appeals four times and the Supreme Court once. What's the claim that we're having to go to trial on, thanks to the earlier commissioner's opinion? Violation of the Data Practices Act ...

I might also add that those facts are not really in dispute. He acknowledged wanting to sell the horse; he acknowledged seeking a sexual relationship with his advisee. OK, that's where we are. We are spending our money litigating that issue. Legitimate questions of a public employee.

It promotes terrible public policy. ... I can tell you as a public employee my rights to privacy are protected by 13.43. My due process rights, unlike private employees, my due process rights to be heard prior to discipline are protected by the Constitution, so I already have those rights, unlike a private employee. We don't need a Tennessen Warning to tell us that comments about our performance and our work might actually be used to judge our performance and work.

It's worth noting, by the way, that both employees ... were represented by legal counsel from the start. So it's disingenuous to suggest that we don't understand what the consequences of providing information are.

Paul Ratwik: I endorse the views of my co-presenters ... and our experience is the same as theirs. ...

Virtually all information maintained by any Minnesota school district in some physical format which can be identified to a specific student is educational data and therefore is private data under the act. The answers to questions like, "Where did the pilgrims land?", "What is the sum of 36 plus 64?", "Of what material is a shark's spine composed?", are all private data if the answers are written by a student or otherwise recorded in some format.

Thus the question: Must a Tennessen Warning be given prior to assigning book reports, asking a first-grade student to add two and two on the blackboard, handing out any homework assignment or administering a quiz or test?

And the answer, not only pursuant to a literal reading of the statute but also in the form of interpretations offered by the director of the public information policy analysis division [of the Department of Administration], is yes.

Now they recognize that that constitutes a somewhat silly statutorily mandated outcome, and they do so by suggesting that school districts can comply with the requirements of the act by following what they refer to as a middle ground, by which they mean giving a full and complete Tennessen Warning at some point in time and then periodically administering additional or supplemental Tennessen Warnings.

The fact of the matter is that very few school districts in Minnesota annually publish a generic Tennessen Warning. When they do, it says something like this: "Students will be assigned academic tasks and will be expected to provide responses to homework, quizzes, tests, book reports and similar responses. The responses will be used by the teacher or teachers in determining the level of the student's acquisition of knowledge. And while the student is not legally required to supply the information, failure to do so may adversely affect the student's grade." *[laughter]*

There is no authority in the Government Data Practices Act for the administration of periodic or umbrella Tennessen Warnings. Rather, 13.04, Subd. 2, says there is a specific requirement that a Tennessen Warning will be given whenever an individual is asked to supply private or confidential data.

Moreover, the concept of an umbrella or blanket Tennessen Warning -- and this is the case whether we're talking about education law or employment law, generally -- directly conflicts with the commissioner's opinion in conclusion 93-004, P. 9, that one of the purposes of a Tennessen Warning is to give a student, in that particular case, an opportunity to make an informed decision in regard to that particular solicitation for information as to whether the information requested by the school district will be provided.

Let's not forget here: We're dealing with youngsters, ages 5 to 18, or 19, and some cases 21, who are going to have a hard time understanding the concept of a Tennessen Warning, much

less remembering for periods of days, weeks or months at a time. ... Imagine for a minute the concept of administering a Tennessen Warning so that you can give a quiz in order to confirm that the student understands the concept of a Tennessen Warning. *[laughter]* ...

The solution is to repeal the Tennessen Warning in its entirety, or to amend Minnesota Statutes 13.04, Subd. 2, to specifically provide that no Tennessen Warning be given when academic or instructional data is requested from students in a teaching situation when the information is requested by educators.

Similar problems exist ... with regard to gathering information from students which may have disciplinary implications.

Gregg Corwin: *I always love to listen to lawyers tell war stories about their cases, then ask the Legislature to bail them out.*

The fact of the matter is we don't expect criminals to know the criminal law. We don't expect state legislators to know the laws that they pass. We provide protections, procedural protections, not assuming that people automatically know their rights. Otherwise, there would be no such thing as Miranda. ...

I think I want to emphasize to this panel that what we're talking about is a procedural requirement, to act as sort of a prophylactic to protect the citizen so that a citizen isn't forced into a position where their rights are already violated and then they seek to enforce them after the fact. If Tennessen were uniformly carried out, we'd have a lot less litigation because it attempts to prevent the violation before it occurs.

I think that you cannot confuse the issue of classification with the procedural protection that the Tennessen Warning gives . Most of the arguments you've heard from counsel on the other side are really arguments against the classifications and how the statutes protect data. Because all Tennessen does is give a person fair warning as to what is protected by the Data Practices Act as private information.

Their attack really is to the information itself and how it's classified. Are they really saying people shouldn't be informed ahead of time as to what their rights are and that the data they're being asked to provide is really private? That's what they're really saying. They're saying we should let these people be ignorant; we should not tell these people because they should know -- being a public employee means you should know everything about employment law ... you should know all your constitutional rights. Quite frankly, most lawyers in this state don't have the requisite knowledge that they attempt to attribute to all public employees. They don't.

So are we to assume that they have this knowledge, that most lawyers don't even have about the Data Practices Act? I could question everyone in this room and no one would have that knowledge -- what is private, what is public, what are the classifications, and so on.

The law is meaningless if it can't be enforced, or if people can't be given notice of their rights beforehand. And an exclusionary rule is the only way to protect the public from violations ... because after the fact is too late. ...

All we're telling an employee is whether or not they have to give the information, whether they're required to give it, who will see it, how it will be used, and things like that, which I think are fundamental. It doesn't affect the classification of the data itself. ...

A perfect example ... is a case I have with Koch Refining, where the MPCA goes to employees of Koch Refining and says, "You voluntarily cooperate with us, give us this information." And so the employees give that information. And what happens? Now, they're threatening to turn it over the Minneapolis Star Tribune and make it public. Were the employees

told that one of the consequences of giving a voluntary statement was that it would be made public and given to the newspaper? No, they weren't, and we're alleging a Tennessen violation. And well we should, because had the employees been given that choice and had been told that the information that they were being asked [for] might be turned over to the newspaper, they might not have voluntarily complied.

And it's the same situation with every factual situation that those attorneys have given you: Had the employees been told that by voluntarily complying they would in effect incriminate themselves, they might not have answered those questions and incriminated themselves. It's no different than the Fifth Amendment protection against self-incrimination. What these lawyers would rather have is, ask the questions, incriminate you and then you're screwed -- we're not going to tell you your rights ahead of time. That's what I think the issue is here.

Gary Weissman: *I think that Jim Moore asks the right questions: What is the underlying policy, and is it a legitimate advancement toward that policy to carry out the Tennessen Warning as we do?*

However, the answer that he and his colleagues give is basically we should drown the baby because some of the bath water has soap bubbles.

If we really look at what the purpose is, it is to advance a core concept of the Data Practices statute, which is to protect citizens ... to make sure that information extracted for one purpose is not used for a second purpose.

Here's why that's important:

All of us reveal information about our charitable and religious goals and objectives when we ask for a tax deduction on our state income-tax return. And we're willing to give up that information in exchange for the tax return -- that is, the tax deduction.

But how would we feel if we went to the Job Service looking for employment, and the employee there said, "Well, there's this great opportunity for you at Catholic Charities, it's an administrative position paying $50,000 a year and you're absolutely qualified, but we know from the Department of Revenue that you contribute to Planned Parenthood, so we're not going to match you"? Nobody would fill that out on the tax return, would you?

Or you go to the chairperson's Health Department because they're interviewing you, to try to stamp out sexually transmitted diseases, and you reveal the partners that you've had. And then you apply for a job seven years later in the government, and they say, "Well, you would really be a good fit for this job, but it turns out, the Health Department has told us, you used to have sex with the assistant commissioner back in the early '90s, and we think that would make for a conflict of interest." Nobody would tell the Health Department anything.

Precisely to make sure that every citizen can do a cost-benefit analysis and decide, "Am I going to give up certain rights in exchange for the service the government is going to give me?" And how do I make that analysis, is by finding out who gets to look at the information I'm giving up. Because the government collects information for one purpose only: To use it. ...

The three members of Group A have used basically what my high school debate coach called the strategy of hyperbole: When you don't like something, you extend it to its logical absurdity and then beat it to death with a club called ridicule. Nobody is saying [you can't] ask a second-grader how much two plus two is without giving them a Tennessen Warning. That's not what anybody intended in this Legislature or on this side of the table, for sure.

What we are concerned about is, if there is going to be an adverse action taken. Nobody cares if Jim Moore's boss says, "Did you get the memo done, Jim?" And nobody cares if Tracy Smith's boss says, "How was your weekend?" Now she might get a little testy if they ask, "With

whom did you spend your weekend, and where did you spend it, and how many hours?" -- because that's nobody's boss' business.

The exclusionary rule is the way to protect. The reason we call it a Tennessen Warning is precisely to have an analog[y] to the Miranda Warning. And in the '60s, when the Supreme Court created the Miranda Warning, politicians and law enforcement officers all over the country were wringing their hands, saying Western civilization will collapse and the scofflaws will go free. And 30 years later, Western civilization is semi-intact, we have four times as many people in prisons, and every cop carries a little card [in case] he or she can't remember what the Miranda Warning is supposed to be.

More importantly, the Supreme Court found out you have to enforce it. Just requiring it doesn't do any good if the police department says, "Well, OK, so Sarge forgot to give the warning, we'll slap his wrist and give him paid suspension the Friday before Labor Day." The only way you can enforce is to say you can't use the information if you didn't give it. That works.

Same with the Tennessen Warning. The surest way to make sure that government officials will give the Tennessen Warning before they're going to take adverse action against somebody is to say you can't use it if you don't give it. It's that simple.

Now, there are absurd lines, and there are fuzzy lines. ...

I had a client who was mugged on Hennepin Avenue. He was knocked unconscious. He was knocked unconscious in front of a tavern, so the cop assumed he was drunk and said that on his report and turned it into somebody -- because he [the victim] happened to be a city of Minneapolis employee. And on Monday morning, he was grilled: "What are you doing in taverns? Why are you getting into fights? You must go to employee assistance; if you don't, we're going to take adverse action against you." "I don't drink." "That's called denial. You must go there."

Now why did he get that? It's because somebody made a mistake and transferred information given for one purpose to another agency and used it improperly.

That's what the legislative policy is all about; that's why it has to stay. If you want to draw a bright line which will not solve all the fuzzy problems say, "If you're going to take adverse action against somebody, if your intention is to do that, then you must ask the Tennessen Warning notice." But if it's something as simple as, "How are you?", "How was your weekend?", "What are two plus two?", then of course it wouldn't apply. ...

Marshall Tanick: *I think it is naive and simplistic and wrong to assume that public employees know their rights and therefore don't need these warnings. ... [Four lawyers in a current case] can't agree amongst ourselves, and we all do a lot of work in this area. It's therefore axiomatic that most public employees don't know, can't be expected to know specifically what is and what is not public or private, and therefore I think it's extremely important that they have these kinds of rights.*

By the same token, I agree with much of what, or some of what the members of Group A have said. I think there are some deficiencies in the law as it currently exists, but I don't think they're deficiencies that they've identified.

I would submit that the law ought to be changed. I submit that the law ought to be strengthened in one particular respect: I submit that the law ought to specifically require that when adverse action of a disciplinary nature is contemplated or reasonable or reasonably anticipated that not only should the employees be given the warnings that are currently in the law, they should be given one more warning, too, and that is their right to seek legal counsel

before they make any decision as to whether they're going to agree to furnish any information or not. ... So many employees are confused, sometimes acting under coercion or duress, simply not understanding what they can or can't say, and what the consequences are. ...

Moore: [If] lawyers cannot agree at times whether something is public or private under the law, how do you expect these middle managers, supervisors, clerk/typist II, who has to supervise a clerk/typist I, to make that kind of evaluation and know whether they're obligated to do a Tennessen Warning because they're asking for private data?

Corwin: *Well, I think that if your agency is doing its job, it should have someone that's designated as the person that deals with data practices issues. And I assume that if they have a proper job description that in their job description would be to do training, to provide procedures for obtaining data. Normally, people that ask questions are given some training in how to ask questions or do investigations.*

To the extent that this forces you to professionalize your investigation, I think it's a good thing, to the extent that it provides some accountability on your side, to do training and to provide rules and procedures, and do things right. I think that's fine. But to shrug your hands and say, "We're not capable of making those distinctions," so the answer is to ignore the law completely, I think, is a very lazy way to approach things. ... I think a lot of it is simply common sense. ...

Every one of the examples that you gave were examples of situations where it was pretty obvious that the questions were really part of an investigation concerning a complaint or issue. So, as far as the examples that you gave, those are no-brainers. I think anyone who has any common sense would understand that you were asking for private data which may lead to an adverse action being taken. ... You look at what's been litigated, it's all issues where I don't think there'd be any dispute that the information obtained was going to be used for some kind of adverse action.

Smith: If you read the Tennessen Warning, you will not find anywhere in there the words "discipline," "adverse action," "supervisors" -- anything like that. There is nothing except a whole cloth, made-up *[inaudible]* on the Tennessen Warning that suggests that it applies when you're asking questions and there's only a subjective intention on the part of someone asking it to discipline somebody. In fact, the commissioner's opinions are much broader. They talk about whenever they ask you a question that will lead to an evaluation. ...

The problem is not the classification of data. I have no desire to make more data private or less data private about employees. The problem is that the Tennessen Warning turns on the classification of the data. ... If [an employee] fails to give a Tennessen Warning because she couldn't figure out if it was private or public because not even lawyers know, how do we discipline that employee ... ? How else do we get our employees to do it except by doing that? ... Let's assume there's a university surgeon who has a patient ... who's failing, and he asks a medical resident, "What treatment did you give this patient?" Is a Tennessen Warning required? ... The medical resident might have screwed up and be subject to discipline, or he might have done it right. ...

Corwin: *Well, as you know, I've represented interns and residents who have been disciplined in the program and removed from the program, which effectively ended their career as a physician. ... Yes, this is a perfect example of why we need the Tennessen Warning because the answer that that intern or resident gives may end their career, effectively. ...*

I just want to say one thing about your problem with training people. We have the same problem with the Americans with Disabilities Act, with Title VII, with the Human rights Act. You

know that there are hundreds of laws that deal with employment that supervisors have to make day-to-day decisions about, whether to exercise reasonable accommodation, whether what's happening is discriminatory ... what is sexual harassment. I would submit that whether data is classified as public or private is no more difficult legally or as far as figuring out what the right answer is than what constitutes sexual harassment, what constitutes a hostile environment, any of the other things that the United States Supreme Court is dealing with on a daily basis. ... They're at least as complicated and difficult and require as much daily decision-making as the issue of data practices ...

Ratwik: Are you suggesting that if at the time the question was asked of any employee it could be ... reasonably anticipated to lead to some sort of disciplinary action, that a Tennessen Warning is then required?

***Corwin**: What we're saying is that we're in favor of clarifying the law so that the consequences part of the question, if the information sought is going to have some consequence to the individual employee, then we think the warning should be given. And I think that's a way of getting rid of this parade of horribles that you're talking about.*

Ratwik: And consequences would be defined how?

***Corwin:** "Consequence" would be some kind of adverse action against the employee, some kind of action that would affect the employee's terms and conditions of employment.*

Ratwik: Aren't you literally saying that any time a public employee asks any question of any public employee with regard to the nature of their duties and how and to what extent they performed their duties, a Tennessen Warning would be required to be given?

***Corwin:** I think you have to exercise common sense. ...*

You know, look at the Miranda thing. Most questions cops ask don't lead to any criminal indictment or criminal charges or criminal complaints. You could make the same argument with Miranda: "You mean that a police officer every time they [ask] a question of someone who's ostensibly in custody that they have to give a Miranda warning? Every time? That they can't investigate anything or ask questions or find out what's going on ... ? If they come upon an accident scene and they start asking questions?" I could make the same arguments you're making, and those arguments were *made against the Miranda Warning.*

Smith: The vast difference between Miranda and here is that public employers are liable for the acts of their employees. They *have* to know what's going on. Any supervisor who doesn't ask their employee what they're up to is shirking his or her responsibilities as a supervisor. And you're also not dealing with a trained police force that pulls out their card and reads the standardized Miranda Warning when *objective* factors show that that person is in custody.

What is being advocated here is a specially tailored Miranda Warning by any public employee whenever there's some hypothetical possibility -- even subjective in his mind, and maybe not even in his mind yet, like my hypothetical doctor -- who's asking the questions of an employee about his work that might reflect on his employment status, which to me is everything: raises, promotions, evaluations, discipline, and so on. There's nothing comparable about a Miranda Warning and an employer asking an employee, "What are you up to?"

***Weissman:** Well, this is another line ... that can be drawn.*

If I was the intern, and I thought your motive in asking me was coaching or teaching, "Doctor, what diagnosis did you make?" ... I'd be comfortable [answering your] questions in the future, and we have a good relationship. But if I thought you were wearing your hobnailed boots and the reason you were asking the question is you were trying to kick me out of medical

school, I'd have a different response.

And since I can't read your mind, the only way to know -- as to whether your intent is to be a good coach, a teacher ... or your real goal is to try to take adverse action against me -- is the Tennessen Warning.

Ratwik: Are you suggesting that [the employer] has an obligation at the time the question is asked to say to the person, say to the employee, "Here is what my intent is"? ...

Weissman: *I think that most of the time most employers in governmental agencies are trying to help their employees perform better. ...*

Ratwik: [If] I ask the question of the supervising doctor, in exactly the mode that you've set up, and the answer he'll give is, "Holy Toledo, I left the forceps in the body," was a Tennessen Warning required or not?

Weissman: *I think you'd have to say, "Whoops, that's not the answer I was looking for. ... I think I have an obligation to report this. ... " And then the issue becomes, "Can you use the answer to my question to prosecute me ... ?"*

Ratwik: At the time I asked you the question, I didn't know what answer you were going to give. And here you give an answer in response to a question that was intended to be helpful, which is incriminatory but at least at a minimum it indicates a dereliction of duty of your part. In your reading of the act, as it presently exists, am I excluded or am I not excluded?

Weissman: *Yes, I think you are.*

Ratwik: And why is that?

Weissman: *What I talked about before: You ask for one purpose; you're using it for another. I'm assuming you're asking it for the purpose of enabling me to do my job better, and in fact you're going to use it to try to destroy my career or put me in jail or cause me to lose a lot of money.*

Ratwik: If I don't know, I don't have that purpose when I ask the question. And --

Weissman: *If you change your mind, you have to give a Tennessen Warning.*

Ratwik: Is there some specific language in the statute that compels that conclusion? I can't find it.

Corwin: *Well, you know, what's the parade of horribles here? ... You can ask the question again by giving the proper warning.*

Smith: Why, why would we do that? I mean, why would we ask each and every question ... and then have public employees on public time go back and ask the same question again after giving them a warning? This is not efficient or accountable government. It is silly government. ...

Weissman: *[I]f the Group A lawyers were really concerned about this, they have two possibilities: They can come and beat their breasts in front of the task force and hope that the law is changed so that's gone, or more simply they could have written to the commissioner and said, "We'd like to get the commissioner's opinion on whether we have to give a Tennessen Warning to a first-grader when we ask her or him, 'Are two plus two four?'" I want to ask you, which ones of you wrote to the commissioner asking for an opinion on that subject?*

Ratwik: The reason that an opinion has not been asked for specifically on that question is that the director of the session has said ... that a Tennessen Warning is required, and we do not consider it to be in the interest of our clients to have reduced to writing a decision that we consider to be adverse ... The answer is absolutely we did not. ...

Moore: I could write until we're all blue in the face asking scenario after scenario after scenario. ... The requirement as currently interpreted is a hindrance to good public work. ...

Ratwik: [A]nyone who says that the administration of the Tennessen Warning does not impede the free and open flow of information to an employer is not being realistic. And I think two of you specifically recognize that in your comments: "If we had known that there was any chance that this information would have been used against us in our capacity as employees, we never would have answered that question."

Employers are not asking the question merely because they want to punish the employee. They're also looking out for their obligations to taxpayers and citizens generally ...

Tanick: *First of all, I would agree with you that the Tennessen Warning does have the effect of impeding the flow of information. ... [So do] attorney-client privileges ... doctor-patient privileges, marital privilege ... The question is whether the nature, degree and extent of that outweighs the other purposes and values that both sides are seeking to achieve. ...*

There are other considerations beyond, "Don't tell them something that might incriminate you." The employee may have certain information that's privileged, may have certain information that should be conveyed beyond the employment context -- because they're a whistleblower, maybe they should report something to somebody else -- and instances like that, where the role that we play with the Tennessen is not simply to use that as some kind of Fifth Amendment "don't say anything, you may incriminate yourself," but rather having the opportunity to consult with the employer about the implications of what they're going to say, how it might not only impact them but impact the workplace in general. ...

Corwin: *The law says that you can require that information of an employee. All we're saying is that the employee should get a warning before that information is released so the employee can contemplate what the alternatives are. For example, the employee may decide that they'd rather* be *fired than provide information which may be used to incriminate them somehow or may be used for other purposes -- it may be made public. And what we're saying is at least by giving them a warning the employee has the opportunity to seek counsel before making those decisions.*

It's like every other provision of every other statute: Taken to extremes you can make any statute seem absurd. There has to be some reasonableness. ... I'm sure you don't tell your clients that they're going to have to give a Tennessen Warning to their first-graders. ...

You can't draft a statute that is so complete that it addresses all these types of situation. In fact, we're criticized when we do that ...

I think there is a way out of this quagmire. And that's to at least provide that the answer to the question would have some adverse impact on this person, on the employee. And that way the other kind of issues that were raised ... would go away.

But I think it's unfair to treat public employees different than others. Is that what you're saying, that all other citizens of this state would have those Tennessen rights, but the people who happen to work for the government would not have the same rights as other citizens? ...

Ratwik: I don't think we're saying that at all. ... It's not suggesting that public employees be treated any differently than private employees with regard to release [of information] to the public. ... Similarly, we are not suggesting that public employees be treated any differently than private employees in regard to the use of information obtained from them which is necessary for an employer to administer his business or perhaps even administer discipline. Private employees don't have that right [of the Tennessen Warning].

APPENDIX 4

Mail and Walk-in Compliance Surveys.

A. Survey instruments.

B. Survey results summaries.

SANDBERG SECRET SHOPPER SURVEY

I. Purpose and Methodology of the Survey

In August, 1998, the members of the Information Policy Task Force (IPTF) requested that an in-person survey be conducted to assess government agencies' compliance with the data practices act. The survey design and implementation was overseen by IPTF staff and conducted by field staff of the Department of Health located throughout the state. Surveyors visited a total of eighteen government agencies representing a cross section of law enforcement, school districts, social services, municipal and state government. Surveyors were instructed to enter the government agencies and ask the person at the "front desk" to whom a data practices request should be posed. When it was clear to whom questions should be posed, the surveyors posed two questions to each of the agencies: one private data question and one public data question. In addition, the surveyors were instructed to follow up on the public data question with questions about cost and time to make copies. Finally, the surveyors were instructed to thank the agency for its time and provide a letter of appreciation signed by Chair Anne Barry.

II. General Analysis of Results and Administrative Problems with the Survey

The results show a mixed range of government agencies' compliance with the data practices act. The surveyors averaged 20 minutes per agency visit. Staff at seven of the agencies visited requested that the surveyors identify themselves and explain why they wanted the public data. Public data should be available to anyone for any purpose without any a person having to explain their interest or intended use of the data. The surveyors were instructed to respond that they were simply citizens with an interest in the data. After asking all of the survey questions, the surveyors were to identify themselves as surveyors for the IPTF.

Another general observation was that surveyors often were directed to multiple places (often three people or more) within the government agency before finding someone who could help with the data request. Oftentimes, the "front desk" staff person directed a surveyor to someone within the agency more familiar with the data and then that person would direct the surveyor to yet a third person with more intimate knowledge of the data. Being directed to multiple staff people within an agency may highlight and agency's poor organization or compliance with the data practices act or may simply reflect the general complexity of the data being sought. It could also point a problem with the complexity of the act itself and thus a need to have agency "specialists" for tackling specific data questions. In addition, it could highlight a problem with government resources for training staff to deal with specific data questions resulting in the staff person who has historically answered the question getting assigned to the matter. Finally, the manner in which data are organized by the agency seemed to cause difficulties. At least two agencies could not provide data that they agreed was public because the data were not organized in a manner which allowed for disclosure. The Department of Health death records could not be reviewed unless the surveyor knew the name of a specific individual

and was willing to pay the price of a copy prior to review. At one of the school districts, the salary information of the superintendent and principals was read to the surveyor but the surveyor could not be given a copy until the sheet from which the government employee was reading could be redacted.

The specific data questions posed to government agencies may have solicited unexpected results as well because of the complexity of the data classification or the manner in which the agencies organize the data. For example, the data question posed to school districts assumed that the names and home addresses of the school districts' students were private data. However, the classification of the data vary and may be public data if the school district included the information as part of its definition of "directory information."

The survey was not "scientific" because too few agencies were surveyed; the data requests were not completely analyzed before being posed; and too many variables were too dissimilar such as time of day, physical characteristics of surveyors, and mental impressions of surveyors. On the positive side, most surveyors reported that the government employees who actually responded to the data requests were helpful and courteous when explaining whether the data were public and if public, explaining the cost and time to make copies. Although not required to do so, some surveyors also highlighted the physical lay out of the government offices and generally noted that the reception areas had sufficient seating and were handicapped accessible. In short, any analysis of the results must be weighed against the methods used to obtain the information.

Summarized Results of Specific Agency responses:

County Welfare/Social Services Offices

Data questions posed:

Private Data: May I see a list of recipients in the county receiving public assistance?

Public Data: May I see a list of all the licensed day care facilities in the county? How much would it be for copies? How long would it take to make a copy?

Beltrami County Social Services Center

Response: No, MFIP client data is private. Day Care Licensee list is public, five page list was immediately provided to surveyor without cost.

Lyon County Human Services-Region VIII

Response: No, list of MFIP recipients is private data. Yes, list of licensed day care facilities is public data, copies available at no charge. Surveyor was asked why he wanted the public data.

Olmsted County Community Services

Response: No, list of MFIP recipients is private data. Yes, list of licensed day care facilities is public data, copy available for $50.00, it would not take too long to make copies. If information is wanted for mailing labels, the cost is 25 cents per label. Surveyor was referred to at least three different

people at two building locations. Surveyor was asked why s/he wanted the data.

Otter Tail County Department of Social Services

Response: No, MFIP recipients data is private. List of license holders in the county is maintained by a private sector entity, pose your question to them, they do not charge for copies.

School District Offices

Data questions posed:

Private Data: Do you have a list of names and the home addresses of juniors (11th graders) in the school district?

Public Data: Do you have the current salaries of the district superintendent and the principals of the schools in the district? How much would it be for copies? How long would it take to make copies?

Bemidji School District

Response: List of juniors students and home address is protected by confidentiality. Surveyor was asked why she wanted the information on students. Salary data is public and copies could be made but no specific time frame to make copies. Surveyor was asked how soon she needed the information. Surveyor responded "in about a week." Staff person said that would be no problem.

Duluth School District

Response: Referred from superintendent's office to Human Resources division. Student addresses cannot be given out. Salary information is public, offered to make copies of contracts at no charge.

Fergus Falls School District

Response: Names and home addresses of juniors is not kept by the school district, pose your question to the high school. The salary amounts but not the names of the superintendent principals can be provided. No charge for the salary amounts. The question about juniors was posed to the high school administrative staff. The high school asked three times why the information was being sought. The surveyor was told to come back at a later time to speak to the principal.

Mankato School District

Response: Student home addresses are private data; salary information is public, no charge for copies. Salary information would have to be taken from documents containing private data, redaction required.

Marshall School District

Response: Yes, list of names and home addresses could be provided. Yes, salary information could be provided at no cost. Surveyor had to pose questions

to a couple of different people and the person who could provide data was out to lunch at time of the request.

Rochester School District

Response: No, names and addresses of students are private. Yes, salary information is public but the principles had not settled contract negotiations so data was not current. No charge for copies of public data. Surveyor was referred to a couple of different people for assistance.

St. Cloud School District

Response: Initial answer was that the home addresses of students are kept but did not know if the information could be made available, referred to Human Resources division. HR person said the data on students cannot be given out. Salary information is public, copies can be made at no cost and will take about a week to complete.

St. Paul School District

Response: Data on students' home address is private. Yes, salary information could be provided if surveyor provided specific names of principals. The names then could be read with salary range for their positions. Data are in files containing private data and would have to be redacted before hard copy can be provided, there would be no cost. Surveyor had to pose question to four different staff people on different floors before given definitive responses. A secretary accompanied the surveyor throughout the building.

Local Police/Law Enforcement Departments

Data questions posed:

Private Data: May I see the names of juveniles arrested in the last twenty-four hours? May I listen to the tape of 911 calls made in the last 24 hours?

Public Data: May I see the arrest reports for last nights arrests? May I see a transcript of 911 calls? How much would it be for a copy? How long would it take to make a copy?

Mankato Police Department

Response: No, data on juvenile arrests is private. No, tapes of 911 calls are private. Yes, agency could read the list of people arrested in the last 24-hours but since list contains private data as well, it could not be provided until redacted. Yes, transcript of 911 calls could be made at cost of $4.00 a piece and take two days to complete.

City Administrative Offices

Data questions posed:

Private Data: May I get the home address of the City Administrator?

Public Data: May I see city council minutes from meetings in September 1998? How much would it be for copies? How long would it take to make a copy?

City of Duluth

Response: Home address of city administrator is not available. Council minutes can be reviewed at no cost in the government office. A copy can be made at no cost. A video tape of the meeting will cost $5.00.

City of St. Cloud

Response: Initial response was that data are on a brochure of the city council. An HR person arrived and stated city administrator address is private and could not be made available. Referred to the Mayor's office for copy of council meeting minutes. Extra copies are routinely printed. Copy could be provided immediately at no cost if extra copies are available. If not a charge for copy would be required.

State Agencies

Data questions posed:

Private Data: May I see a birth certificate for XX who's parents were not married ?

Public Data: May I see copies of death certificates? How much would it be for a copy? How long would it take to make a copy?

Minnesota Department of Health

Response: The birth certificate information is private and cannot be made available. Death certificates are public. You must fill out form with name of certificate and pay $5.00 for a copy. Death certificates cannot be perused because they are kept on floor with other private files. Statistical data on deaths and causes of death are available from another part of the agency located in St. Paul.

MAIL SURVEY SUMMARY

Four state agencies and 13 local units of government completed the survey. Of particular note, the surveys from the Hennepin County Sheriff's Office, Washington County, and the Minnesota Department of Agriculture reflect an obvious and substantial amount of time, effort, and insight in their responses. The Task Force should consider sending a thank you to the seventeen governmental entities that completed the survey. A special thank you would be in order to the three specifically mentioned above.

The huge majority of surveys showed that the governmental entity had at least a basic understanding of and commitment to following the MGDPA. Some surveys showed that the governmental entity had a comprehensive grasp of the MGDPA as it applied to that governmental entity.

The responses indicated varying degrees of internal organization and attention to the MGDPA, for the most part, appropriate to the size of the governmental entity and the sensitivity and complexity of the data handled by the governmental entity.

One thing that became apparent to staff when reading the surveys was that the MGDPA compliance wheel has been invented and reinvented and reinvented again. To one degree or another, many governmental entities have prepared written materials to aid in complying with the MGDPA. Organizations representing classes of governmental entities (such as cities) have prepared MGDPA compliance materials. We could not help but feel that it would save time and effort while resulting in a better product if the state were to coordinate a project to glean the best of these materials for use by all types and sizes of governmental entities.

Such an effort would also result in a more focused understanding of the problems with the MGDPA faced by the different types and sizes of governmental entities, which in turn would result in a better ability to address these problems.

The Minnesota Department of Agriculture included with its survey a copy of its "Data Disclosure Procedures," a comprehensive document designed to guide MDA employees in complying with a data request. If any state-agency-wide effort is made to develop form materials for use by all state agencies, the MDA Procedures form should be considered as a starting point.

Submitted 9/16/98
By Dave Orren
Department of Health

GOVERNMENTAL ENTITIES REPLYING TO THE SURVEY.

Cities.
Eagan.
Mankato.
Rochester.
Thief River Falls.
First Unnamed City.
Second Unnamed City.

Law Enforcement.
Brainerd Law Enforcement Center.
Hennepin County Sheriff.
Unnamed Law Enforcement Agency.

Counties.
Washington County.
Unnamed County.

Schools.
Minneapolis Public Schools.
Unnamed School.

State Agencies.
Department of Agriculture.
Department of Employee Relations.
Board of Medical Practice.
Department of Natural Resources.

SUMMARY OF RESPONSES

1. **What person or position is designated as the responsible authority for your agency or organization under the MN Government Data Practices Act (M.S. §13)?**

This ranged from the elected or appointed head of an agency to a designated manager or administrator or attorney.

How many additional employees in your agency or organization are designated by the responsible authority to receive and comply with data requests for government data?

This varied with the size of an agency and the complexity or sensitivity of its data. For small agencies, there was often just a small handful of persons designated. For large agencies with complex or sensitive data, there often were data managers designated for each division or program.

What is (are) their classification level(s) (e.g., clerical, technical/professional, managerial, legal, administrative)?

This ranged from clerks who dealt with the public and with routine data on a regular basis to professional, supervisory, and legal staff who were specifically trained to deal with complex or sensitive data maintained by the agency.

2. **Who or what position handles most of the requests for information under the Minnesota Government Data Practices Act?**

This ranged from front-line clerks who dealt with data on a regular basis to professional, supervisory, and legal staff with specific training in the MGDPA.

3. **List and describe any mechanisms (e.g., training, user groups, working committees, employee orientation) you have in place at your agency or organization for keeping staff who handle data requests, current on the requirements of the Minnesota Government Data Practices Act.**

MGDPA training mechanisms mentioned in the surveys include:

- new employee orientation with periodic follow up.
- training by the governmental entity's legal counsel.
- the governmental entity prepares and distributes written materials to employees
- annual training meetings for staff by managers and supervisors
- whenever possible, training by Don Gemberling's office
- training provided by Munici Pals organization
- on-the-job coaching programs
- self-directed training by reviewing chapters 13 & 1205, and Opinions

There is no formalized training program by the state to ensure that government

employees at all levels of state and local government have the necessary expertise to adequately administer their data in compliance with the MGDPA.

4. **Which staff are trained?**

In some governmental entities, all staff get general training, while those who have greater responsibilities for managing or handling data get more intense and specific training. In other governmental entities, only those who have responsibilities for managing or handling data receive training.

5. **Approximately how many requests for government data does your agency or organization receive each year?**
What proportion request access to _____% public data; _____% non public data?

The answers to this question ranged from "less than 5" to "in excess of one million" requests for data each year. This wide range of answers is at least partly because this question could be interpreted in two ways: (1) broadly to mean every request for data from whatever source, either in person or via phone, fax, mail, Internet, or other media; or (2) narrowly to mean only formal requests for data made under the MGDPA. Likewise, the percentage of public versus non public ranged from 98%-2% to 50%-50%.

6. **Describe the procedures you agency or organization uses for dealing with requests for (a) public data; (b) non public data?**

For routine requests of public data, the request is processed right away by a front-line staff person. For non-routine requests, for requests of not public data, or when there is any doubt about the classification of data, the request is referred to legal counsel or a supervisor.

Most governmental entities said they require requests to be in writing for complicated or not public data; some governmental entities require all requests to be in writing, regardless of the classification of the data. Some survey respondents require prepayment of costs.

Other comments of note:

- for some frequently requested reports that contain both public and not public data, one governmental entity routinely prints these out with the not public data redacted;
- written consent forms are routinely required for an individual or insurance company to access not public data;
- One governmental entity described its efforts to work with individual to supply private data on that individual within the five-day and then ten-day timeline and how it keeps the individual informed when it is not possible to supply the data within ten days;
- When data is protected from disclosure, the governmental entity informs the requester what is being withheld and why.

7. **What proportion of these requests for access to public data under the MN Government Data Practices Act fit the following categories?**

routine requests	ranged from 70% to 98%
unusual requests	ranged from 0% to 20%
complicated ("special handling") requests	ranged from 0% to 25%

There were some comments that unusual requests and complicated requests were really the same thing, in which case, these combined requests ranged from 2% to 30%.

8. **Please provide an example of the type of request that would be considered "routine" in your agency or organization.**

These examples included such things as: initial complaint reports provided for the media on a daily basis; accident reports; information on prospective tenants; information on individuals who will be working with youth in city sponsored programs; city council materials; code sections; resolutions; planning information; information on public improvement projects; criminal investigative data; feasibility reports for improvement projects; resolutions; ordinances; personnel file; utility info; computerized records; media request for jail inmate booking photograph; theft reports; "How many books do I have checked out?"; "What titles do you have on building a deck?"; amount of tax owing on real or personal property; verification that no delinquent taxes exist on a property; tax description or parcel information for a particular property or for all property in a city or township or for the entire county; forms filed by candidates for public office; birth, death, or marriage data; highway right-of-way information; mortgage verification; salary information; job title; map sales; digital data sales; court case file; business inspection file; client information released to a counselor (based on a written release); client information released to a health, financial, or social service agency; student records; requests to view or copy paper documents that are entirely public or that require limited redacting; requests for computer lists that are regularly requested so that a standard query can be developed to generate updated lists; disciplinary orders; HR policies and processes; eligible list information; protected group information; employment reference or wage verification; copy of firearms safety certificate; list of boats registered in Minnesota.

9. **Please provide an example of the type of request that would be considered "unusual" in your agency or organization.**

These examples included such things as: copies of all reports made regarding family problems involving child custody/visitation incidents; HRO and OFP violations (unsubstantiated or otherwise); certification or license numbers for employees; historical information on public improvement projects; copy of an entire file dealing with zoning issues; copies of tape recordings; "How many people have been granted CUPs in the past 5 years?"; copy of property appraisal; media request for every bench warrant on file that involves theft from motor vehicles; statements; juvenile crime with traffic accidents; domestic assault - restraining order uncertain; "My boyfriend lost a book of yours. I want

to pay for it. Can you tell me how much it is?"; traffic data for accident analysis; Brown's Creek watershed data; a map of all brain cancer cases in Stillwater; all tax parcel owners along County Road 15; all tax parcel owners within Clear Lake sub-watershed district; how to qualify for Medical Assistance (a request from funeral homes to develop marketing tool for burial plans); client or attorney wants client's community services record; outcome of disciplinary action; third party requests; StarTribune requesting a student file and employee data; requests for large volumes of a wide range of public data (e.g., info from records dating back 20 years or more); requests for much dissimilar public data that requires pulling data from several sources or locations (e.g., all info on a company that may be licensed, registered, permitted, inspected, or investigated by multiple divisions in the agency); "to be an unusual request, the type, range, or scope of data requested would be unusual and could take one or many employees hours, days, or weeks to process;" a breakdown of numbers of physicians by zip codes; alien certification; affirmative action plans; "any and all correspondence between this agency and the AG's Office for the last six years;" and a private jurisdiction requesting private data on one of our employees.

10. Please provide an example of the type of request that would be considered "complicated" or would require "special handling" in your agency or organization.

These examples included such things as: information requested by divorced parents or relatives on juvenile who had committed suicide; individuals being 'long-formed' for charges and file sent to appropriate attorneys; any request for data in a format in which it is not stored or kept (e.g, the number of development applications processed for a particular applicant); documents which contain both public and non-public data (e.g., personnel files, license applications, and employment applications); police documents are usually the most delicate and require that they be reviewed prior to information released; information on city development projects where proposals have been received; extremely large amount of materials; materials pertaining to pending litigation; materials in archive storage; copy of a background investigation; a request for duplicate tape and transcript of audio recording of 911 call made by juvenile that results in multiple police agency response to domestic abuse incident which leads to emergency mental commitment hold on individual who is suspect in two active assault investigations (The entire incident from initial 911 call to final radio transmission consumes more than six hours of audio tape. One of the officers who responds to the call is the subject of pending disciplinary action as the result of his conduct during the incident.); sexual assault information; child abuse or neglect information; printout of the names of all your registered borrowers in the 55125 zip code; requests for taxpayer info that includes numerous parcels and types of tax related info; access to documents that include both public and private data; special drainage request which involves finding old highway plans and analysis from many years ago; information on property with values over a certain amount; request for not public data by the media; a map of all felony cases combined with crisis response calls in Cimarron Trailer Park; define and map the limits of the Stillwater fire district or the Lakeview Memorial Hospital paramedics response area; a request for a copy of investigative file by the person investigated in order to sue the person who filed the complaint; request to social services agency from out-of-state sheriff for address of

children of divorced father to notify children of accidental death of father; request by client to review entire file, when file contains lots of confidential data that must be removed; data related to litigation; name and address of person active in a drug prevention program; requests that require extensive redacting; requests that involve obtaining informed consents for release of private data; attorney discovery requests; some media requests; any request where the individual processing the request must have considerable knowledge of the MGDPA and other applicable state and federal statutes; a subpoena for private or confidential info which would require redacting identifiers and would require involvement by the AG's Office; settlements to state employees; certification lists; tobacco case data; investigation, performance, or discipline data; all violation records for the last ten years via a FTP file transfer; expense reports for ten agency personnel over the last ten years; and any request involving pending litigation, hearings, or grievance.

11. Describe your method of processing these "special handling" requests.

A typical response to this question includes having a supervisor review the file, review the MGDPA, consult with legal counsel, consult with Don Gemberling's Office, determine how data is classified and what part of the file can be released, redact as necessary, copy, and notify requester when document is ready. When there will be large copying or assembly costs, the requester will usually be notified in advance to make sure they still want the data at that cost. If the governmental entity is not able to supply the data within the five or ten day timelines, then the requester is notified and given the opportunity to view or get copies of as much of the data as can be assembled now, with the rest as soon as it is assembled.

The response from the Hennepin County Sheriff's Office is worth repeating verbatim: "Processing requests of this nature is a real administrative challenge and the methodology utilized requires tight coordinated staff response. Managerial and professional/technical staff address all aspects of the request, i.e., numerous data access issues, mechanics related to producing duplicate audiotape in which all unrelated 911 calls and radio transmissions must be excised, allocation of overtime clerical resources needed to produce transcript, etc., etc. Diverting limited staff resources to complete the diverse and multiple tasks required in responding to "special handling" requests of this nature can be particularly disruptive by adversely impacting established timelines in providing other essential services unrelated to the request."

12. How much time do you estimate is allocated to filling these requests?

- Several of the governmental entities gave estimates of the time per request. These estimates were: from 1 to 3 hours per request; 2 to 10 hours per request; 5 to 60 minutes per request; from a few hours to several days.
- A number of governmental entities indicated that the time spent on this was minimal because the number of requests is so small.
- The Hennepin County Sheriff's Office estimated that the total accrued staff time to respond to requests of this nature easily exceeds 2,500 staff hours per year.

- The Washington County Community Services Office estimated that it takes 6,000 hours per year to fill requests for not public data.
- The Minneapolis Public Schools estimated that it takes approximately 4 FTEs to fill these types of requests.
- The Minnesota Department of Agriculture estimated that special handling requests take 30-45% of the Data Practices & Records Manager's time and about 10% of the Department Legal Counsel's time annually, plus a substantial amount of assistance from clerical, professional/technical, and administrative staff.
- The Minnesota Department of Natural Resources estimated that the time varied from a few hours for a routine request to days for more complex requests.

13. Are you familiar with the authority of the MN Department of Administration to issue opinions on MN Government Data Practices pursuant to M.S. §13.072?

Sixteen survey respondents said, "Yes." One survey respondent said, "No."

14. Has your agency or organization ever sought such an opinion from the Department of Administration?

Of the survey respondents, two cities, one county, one law enforcement agency, one school district, and one state agency said, "Yes."

Other responses included:
- No, but we are on the mailing list for opinions and review them.
- No. County Attorney fields these questions for us.
- No. However, we periodically consult Don Gemberling and his staff and we occasionally search previous opinions for interpretation assistance.

15. If you have sought such an opinion, did you find it to be beneficial to your agency or organization?

Two surveys said, "Yes," two said, "Extremely," one said, "Yes, verbal have been extremely helpful as well," and one said, "Somewhat – we still have a difference of opinion about exactly what the opinion meant."

16. Does your agency or organization have difficulty complying with the Minnesota Government Data Practices Act? If so, why?

Six survey respondents did not indicate having trouble complying with the MGDPA. The responses on the remaining surveys are:
- Not with compliance per se, but with accurate interpretation.
- No for routine matters. Yes for anything that is in the various gray areas as to type.
- Yes. Definitions are complex and confusing. There are areas which are not clearly determined. Statute is awkward to use.
- No, but data classification can be confusing.

- Complying with the MGDPA can be challenging particularly when responding to unusual or "special handling" requests for data. Additionally, statutory ambiguities exist within the Act, and numerous data practices statutes are located outside the Act which involve time-consuming cross-referencing. The often overly verbose interpretive Advisory Opinions issued by the State Commissioner of Administration can be especially burdensome and compound the frequent need to cross-reference various sources in dealing with non-routine requests for data. Compliance can also produce significant economic hardship, particularly in responding to data inspection requests where administrative costs incurred in compiling the requested data and explaining its meaning to requesters (who often are overly deliberate) are not recoverable by the agency. Such requests have potentially catastrophic ramifications for the agency with limited economic and staff resources. Reductions in the delivery of other essential services is often the only option available to the agency that must deal with such requests for data that arise with increasing frequency.
- Yes – Poor report forms, poor report writing, poor computer software not designed for compliance.
- Law is very complex and each request needs to be reviewed. There is no such thing as an "easy" request. Especially when private data is involved. We collect a lot of information and rules/laws are subject to interpretation. It is difficult to provide services (case management) to vulnerable people when you constantly need releases.
- No, although sometimes staff feels that the public would be better served if we could provide more information.
- Yes -- time required, difficulty of accommodating format requirements.
- The Minnesota Department of Agriculture included a lengthy list of problem areas that could be addressed by the Task Force. "At times, yes. The Act is not very user friendly—portions of the Act are complex, difficult to interpret, and sometimes conflicting. Definitions of important terms are lacking. Some examples to illustrate:
    - MS § 13.99, subd. 53b indicates veterinary records on clients are classified by MS § 156.082 <u>when a veterinarian is under investigation</u>. MS § 156.082 does not make this limitation and implies a broader interpretation by including the veterinary records of a client maintained by <u>a state agency, statewide system, or political subdivision</u>. If you only look at 156.082 without also looking at the context of the statutes before and after it, interpretation could easily encompass the veterinary records collected by this agency (e.g., during investigations of complaints against pesticide applicators when livestock or pets allegedly suffered injury or died as a result of the application). Looking at the statute within the context and presumed intent of those surrounding it, the limitation in MS § 13.99 makes sense. It remains unclear, however, what state agencies, statewide systems or political subdivisions would be required to keep veterinary records private or nonpublic and how they would know when a veterinarian is being investigated by the Board of Veterinary Medicine under whose jurisdiction enforcement of Chapter 156 falls.

- MS § 13.41 and MS § 13.02 do not define "active investigation" and "inactive investigation," potentially subjecting the section to a wider range of interpretation than is likely intended. Without benefit of a definition, one interpretation might be that an investigation is active the moment a complaint is filed with an agency and inactive when the case is closed. Another interpretation might be that it is active only when an investigation is actually initiated and remains so until statute of limitations for appeal of any disciplinary or enforcement action expires. Yet another is that an investigation becomes active when the chief attorney acting on behalf of the agency declares the investigation a pending civil legal action and inactive when the statute of limitations expires, time to appeal expires, and/or a decision is made not to pursue the action. All seem reasonable interpretations, but the first two eliminate much more public access than does the latter. Definitions would narrow the scope of interpretation, lessen confusion, and promote better compliance.
- In MS § 13.41 it is inconsistent and illogical to only protect the identity of persons who file complaints against licensees who are individuals. Is it any less important to protect the identities of persons who file complaints against licensees who are not individuals or against companies and individuals who are not licensed but should be? A person may be reluctant to file a complaint if they believe their identity will be disclosed. Anonymous pesticide misuse complaints, for example, can be impossible to properly investigate when the allegations made indicate the complainant suffered damage to his/her property, exposure, or injury to livestock or pets. In such cases, anonymity eliminates our ability to collect samples, take pictures, observe damage, collect medical or veterinary records, etc. Evidence is critical in any investigation. Without it, there is no way to determine if a violation occurred. Environmental quality and human and animal health potentially could be impacted.
- The term "license" is not defined in MS § 13.41 or anywhere else in the Act. In addition to standard licenses, our agency considers permits, registrations and certificates/certifications part of its licensing functions. It is unclear, however, whether these other authorizations are covered under the Act's licensing data section. Defining this term would clarify what data is covered under this section.
- In 1997, the legislature added subdivision 59b to MS § 13.99, referencing MS § 181.932 (statute that protects the identity of "whistle blowers"). The current language may restrict public access to state and local investigations and inquiries in which employees were contacted, indicate a much greater need for Tennessen warnings, and result in substantially more time-consuming redacting. Until Koch Refinery's attorneys recently argued that the statute prevented public access to investigative files on their client because employees were interviewed and received no Tennessen warning, it is unlikely agencies were aware of the language problem and what effect it may have on state and local agencies' data practices. Some agencies may still be unaware of the data practices concerns this language raises.

Those who are aware of the concerns, likely are confused.

- The general nonpublic section (MS § 13.37) permits protection of qualifying data. What data actually qualifies for protection under this section is sometimes gray. It could be argued that certain commercial data and financial data is eligible as security data. This kind of data clearly qualifies as trade secret under the Minnesota pesticide and fertilizer laws but not under other laws within the department's jurisdiction."

17. Do you advise individuals from whom you solicit information of the purpose for the collection of that information?

Uniformly, the survey answers were, "Yes." Except for one unnamed law enforcement agency, which said that it does not give a Tennessen Warning -- we assume/hope this means that they are referring to when they are exempt from giving the Tennessen Warning when asking for criminal investigative data under section 13.04, subdivision 2. Some comments given with answers include:

- Yes, to the extent the solicited data is private or confidential information on individuals and the individual is not being asked to supply criminal investigative data in compliance with Minnesota Statutes, section 13.04, subdivision 2.
- Yes, Tennessen warnings are typically included on forms we use to collect private or confidential information.

18. Please describe the process you use in determining when to administer a Tennessen Warning as provided in M.S. §13.04, subd. 2?

For the most part, survey respondents said they give a written or oral Tennessen Warning when they ask an individual for private or confidential data on the individual. Some examples given of when this occurs include: Social Service investigations; police office misconduct investigations; liquor license applications; library card registration; marriage license applicants; offenders at intake; charged persons at bail evaluations; disciplinary actions; when creating a case file; and when employees or students may be subject to discipline; licensing and complaint review.

- From Hennepin County Sheriff's Office: "A basic two-step process occurs: (1) Is the individual being asked to supply criminal investigative data? If so, administration of Tennessen Warning is not required pursuant to MS 13.04, subdivision 2; (2) Is the individual being asked to supply private or confidential data on individuals? If so, then Tennessen Warning must be administered."
- From an unnamed school: "We seek the advice of legal counsel and also use them to deliver the Warning."
- From the Minnesota Department of Agriculture: "When we develop new forms or revise existing ones, we review the forms for legal authority to collect the data, business need for the data, and whether any of the data requested is classified as private or confidential data on individuals. If we determine that the private or confidential data is necessary and we have the authority to collect it, a Tennessen warning is supplied directly on the form. Department forms standards require that

when Tennessen warnings are applicable, they be placed conspicuously at the top of the form just under the form name. We also produce and supply additional information through newsletter articles, fact sheets and privacy notices as the need arises to help our clientele understand their privacy rights."

19. If you have a Tennessen Warning available in writing, please provide a copy or sample.

The sample Tennessen Warnings include:

- Brainerd Law Enforcement Center included a Garrity/Tennessen Warning for an investigation of an employee for possible disciplinary action.
- Rochester attached a warning given in relation to a job application.
- Hennepin County Sheriff had a warning used on employment application form.
- The Minneapolis Public Schools had a generic, fill-in-the-blanks Tennessen Warning that appears to cover all the bases in leading a government employee through the Tennessen requirements when asking an individual for private or confidential data on the individual.
- The Minnesota Department of Agriculture's first sample was an authorization for the release of medical records for the purpose of investigating human exposure to pesticides. The Minnesota Department of Agriculture's second sample was an information sheet to pesticide registrants.
- The Medical Practice Board attached an information sheet produced by Don Gemberling's Office containing the requirements of the Tennessen Warning.
- The Minnesota Department of Natural Resources included a sample Tennessen Warning to be used for an employee misconduct investigation.

20 & 21. The answers to these two questions were very similar or, in many cases, referred to each other, so this summary will combine survey responses to these two questions.

20. Are there any federal laws or state statutes outside of the MGDPA (M.S. Chapter 13) that classify or restrict the use, access or dissemination of the data collected by your agency or organization? If so, please list the statutory/law citations where the classification or restriction may be found.

21. Identify those places in statute outside of the M.S. §13, the Minnesota Government Data Practices Act, which contain classifications for data collected by your agency or organization?

Mankato listed:

- Economic development data, section 469.154, subdivision 2;
- Self-insured claims, section 471.617, subdivision 5;
- Undercover buy fund, section 299C.065, subdivision 4;
- Criminal Justice info network, section 299C.46, subdivision 5;
- Arson investigations, section 299F.055-056;
- Hazardous Material Emergency, section 299F.095-096.

Rochester said there were too many to list.

The Hennepin County Sheriff's Office listed:

- MS 626.89, subd. 12 restricting public release of officer photos;

- MS 176.231, subd. 8 restricting access to workers' compensation reports;
- MS 260.161, subd. 3 restricting access to peace officer's juvenile records;
- MS 471A.03, subd. 3 authorizing county to classify vendor proposal data as nonpublic;
- MS 299F.04, subd. 3a classifying arson investigative data contributed to state marshal's related database as confidential;
- MS 168.346 (a) classifying certain motor vehicle registration data as private based on written request of owner filed with Department of Public Safety;
- MS 181.954, subds. 2-3 classifying employee drug and alcohol test results;
- MS 181.961 establishing employee right to review his/her personnel record;
- MS 181.973 restricting dissemination of data acquired during employee peer counseling debriefing session with limited exception;
- MS 181.932, subd. 2 restricting disclosure of identity of employee whistle blower by investigating law enforcement agency;
- MS 243.166, subd. 7 restricting dissemination of certain predatory offender registration data to the extent it does not conflict with community notification;
- MS 299C.091 classifying gang task force data contributed to Bureau of Criminal Apprehension related database as confidential;
- MS 171.07, subd. 1a classifying driver's license photos as private data;
- MS 65B.82 classifying auto theft insurance data as confidential;
- MS 609.3471 classifying data on sexual assault victims as confidential;
- MS 299C.48 restricting access to data maintained by users of state criminal justice data communications network;
- MS 299C.54, subd. 4 classifying data in missing children bulletins;
- 42 USCS 4582 (d) restricting access to alcoholism treatment data;
- 20 USC 1232g and 34 CFR Part 99 restricting access to law enforcement unit records which fall within scope of Family Educational Rights and Privacy Act.

An unnamed law enforcement agency list included:

- MS 260.161;
- MS 168.346; and
- MS 171.12.

Washington County listed:

- 1997 MN Laws, 1st Sp Session, ch 3, sect. 27;
- MS 290.611
- MS 201.091
- MS 297B.12
- MS 325F.73-744
- MS 144.218
- MS144.225
- MS257.73
- MS 259.89
- Americans With Disabilities Act
- Family and medical leave of absence
- Vulnerable Adults Act
- 45 CFR 303.21
- 45 CFR 205.5

- MN Rules of Public Access to Records of the Judicial Branch
- IRS 7213(a)

The Minneapolis Public Schools list included:

- IDEA 20 USC sec. 1400-1435
- MS 625 through MS 656
- FERPA 20 USC sec. 1417(c)
- Section 504, 20 USC sec 1232(g)

The Minnesota Department of Agriculture listed:

- Agricultural Commodities Producer's Financial Data. M.S. § 17.62. Not classified, but treated as private or nonpublic. (Cross-reference M.S. § 13.99, subd. 6e.)
- Agricultural Commodity Handlers Report Data. M.S. § 17.694, subd. 2. Not classified, but treated as private or nonpublic data (Cross-reference M.S. § 13.99, subd.6d. NOTE: subd. 6d incorrectly references subd. 1 of 17.694—it should be subd. 2.)
- Agriculture Best Management Practices Loan Program Data. M.S. § 17.117, subd. 12. Private or nonpublic (Cross-reference is in M.S. § 13.99, subd. 6b.)
- Aquaculture data. M.S. § 17.498, subd. d. Nonpublic if the applicant or permittee requests this protection (Cross-reference is in M.S. § 13.99, subd. 6c. Note: reference lists only MPCA, though MDA also maintains this data.)
- Aquatic Farm Operation Data. M.S. § 17.4984, subd. 7. Nonpublic (No cross-reference in MGDPA.)
- Commercial, Financial and Trade Secret Data . *Pesticide:* M.S. § 18B.38 and 7 USC § 10 [136h] *Fertilizer:* M.S. § 18C.405. Not classified, but treated as nonpublic providing trade secret protection rights under pesticide and/or fertilizer law have been properly exercised. (No cross-reference in MGDPA.)
- Dairy Financial and Production Data. M.S. § 32.71, subd. 2. Private or nonpublic. (Cross-reference is in M.S. 13.99, subd. 8a.)
- Dairy Production Reports. M.S. § 32.19. Not classified although section does state "confidential nature," treated as private or nonpublic data. (Cross-reference M.S. § 13.99, subd. 8.)
- Environmental Response Data. M.S. § 115B.17, subd. 5. Private or nonpublic, providing it meets trade secret/security data criteria in MGDPA general nonpublic section and protection rights have been properly exercised. (Cross-reference exists in M.S. 13.99, subd. 22, but only lists Pollution Control Agency even though Agriculture has 115B jurisdiction as well and is specifically listed in the definition of "Agency" in 115B.)
- Family Farm Security Loan Data. M.S. § 41.63. Private. (Cross-reference M.S. § 13.99, subd. 9)
- Meat Inspection Data. M.S. § 31A.27, subd. 3. Not classified, but treated as private or nonpublic data. (Cross-reference M.S. § 13.99, subd. 7b.)
- Pesticide Applicator Chemical Application Records Dealer Report s/Records of Restricted Use Pesticide Sales. M.S. § 18B.37, subd. 5. Private or nonpublic (Cross-reference is in M.S. § 13.99, subd. 7.)
- Pesticide Gross Sales Brand Name Data. M.S. § 18B.26, subd. 3(c). Not classified, but treated as private or nonpublic data. (No cross-reference in

MGDPA.) NOTE: Although the cited law allows a summary of the information when brand name is not disclosed, disclosing gross sales by the alternative, active ingredient, would be the same as disclosing brand name of proprietary products. Registrants do then have the option to exercise protection rights under M.S. § 18B.38.

- Pesticide Inert Ingredient Data. 7 USC § 10(d)(B) and (C). Not classified, but treated as nonpublic data. (No cross-reference would be listed in MGDPA for federal law.)
- Pesticide Manufacturing or Control Processes Data. 7 USC § 10(d) (A). Not classified, but treated as nonpublic data. (No cross-reference would be listed in MGDPA for federal law.)
- Plant Variety Protection Application Data. 7 USC § 2426. Confidential but equivalent to private or nonpublic. (No cross-reference would be listed in MGDPA for federal law.)
- Rural Finance Authority Data. M.S. § 41B.211. Private or nonpublic. (Cross-reference M.S. 13.99, subd. 10.)
- Wholesale Produce Dealers' Financial Data. M.S. § 27.04, subd. (c). Private or nonpublic. (Cross-reference M.S. § 13.99, subd. 7a.)

The Minnesota Medical Practice Board listed:

- Medical Practice Act, MS 147.

The Minnesota Department of Employee Relations said, "ODEO may have some federal requirements but did not provide cite."

The Minnesota Department of Natural Resources listed:

- MS 43A
- MS 10A
- Portions of MS 609
- MS 15
- MS 626.89
- MS 103I.605, subds. 2 & 4

22. How do those provisions work in conjunction with the Minnesota Government Data Practices Act?

There were no in-depth responses to this question. Several responses indicated that they interpret and enforce these other provisions in accord with the MGDPA. A couple of responses said that if the Federal Restriction is tougher, this supersedes the MGDPA.

23. Please describe any conflicts you are aware of in the statutory classifications of data collected by your agency or organization?

- One city replied: "The statutory classifications are confusing and next to impossible for a lay person to deal with with any degree of confidence."
- The Hennepin County Sheriff's response to this question:
  - "Under Minn. Stat. sect. 13.44 identities of individuals who register complaints concerning violations of state laws or local ordinances concerning the use of real property are classified as confidential but

pursuant to Minn. stat. sect. 13.82, subd. 3(b) the identity of individuals who request law enforcement services (including those who register complaints concerning law violations about the use of real property) is public data to the extent the identity is not protectible under Minn. Stat. sect. 13.82, subd. 10.

- Pursuant to Minn. Stat. sect. 13.43, subd. 2 and subd. 3 training background on employees and applicants is public but if the training falls within the scope of Minn. Stat. sect. 13.47, it is private data pursuant to subd. 2 of that section.
- According to Minn. Stat. sect. 13.99, subd. 114a police reports on domestic abuse are classified under Minn. Stat. sect. 629.341, yet no classification is so indicated and pursuant to Minn. Stat. sect. 13.80 domestic abuse data is classified as confidential 'until a temporary court order made pursuant to subd. 5 or 7 of section 518B.01 is executed or served upon the data subject who is the respondent to the action.'"

- An unnamed law enforcement agency said, "13.80 Domestic Abuse Data – very vague and consults with Gemberling's staff say it can be interpreted in various ways, and try to see the intent of the law.
- Washington County comments were:
  - Accident data/reports prevents us from recouping costs due to damage to roadway because lack of name prevents us from contacting people.
  - Maybe with the new child protection reconsideration process, does the State Department of Administration still follow up on data challenges regarding accuracy of collected information and if so why?
- The Minnesota Department of Employee Relations said, "Employee ID# established with intent it be public data – that language was not approved.

Eagan.
Your Task Force would do a great service if we could get this law and the implementation of same into a format and process that real people can understand and use. To have Mr. Gemberling at the State as the expert does not translate to people in the trenches trying to comply. At times, it seems like a choice as to which side you want to be sued by. There should be a process by which well meaning, capable people can comply without an attorney from one or both sides looking over your shoulder.

Thief River Falls.
Would like to receive better training and/or information concerning this area.

Hennepin County Sheriff.
The responses above demonstrate the need for significant legislative reform in data practices administration. Re-engineering strategies designed to facilitate MGDPA user-friendliness should focus on three major areas:

(1) Re-organization of the MGDPA -
- Redundant, conflicting statutory provisions (e.g., domestic abuse-related) must be restructured;
- Subject-related statutes currently scattered within and beyond the MGDPA must be repositioned to reduce cross-referencing frequency;
- Statutory ambiguities must be resolved in furtherance of legislative objectives and administrative efficiency in responding to requests for data.

(2) Redesigning Advisory Opinions -
- Concisely-drafted analytical treatment of issue(s) promotes clarity and enhances user friendliness; Opinions tend to be excessively verbose;
- Conclusions which clearly impede public policy must be redetermined; (e.g., Advisory Opinion 98-034 obstructs ability of Department of Economic Security to collect data from employers in determining reemployment insurance benefit eligibility; such conclusion defeats public interest in ensuring that ineligible applicants are disqualified from receiving such benefits;

(3) Relieving Administrative Hardships in Complying with the MGDPA -
- Responding to complicated data requests within strict MGDPA time frames stress limited human resources and disrupt continued delivery of essential services; collection of actual costs up-front should be authorized;
- Responding to requests to inspect data adversely affects financial stability of agency; limits on free data inspection authority must be established.

Finally, the demands of the mega-information age and rapidly-developing technology must be addressed. Emerging trends involving paperless data systems present new challenges for the data practices administrator.

An Unnamed Law Enforcement Office.
An index of various references would be helpful. Include:

- Guardian Ad Litem - many G.A.L. request data on abuse victims. Most have no paperwork to prove they have authority to access.
- Clarify Real Property as referenced in 13.44.
- Clarify detox report classification.

Washington County Library.
In response to question 5 on the number of requests for government data received each year: 500,000 (estimate). This is a very difficult number to determine as the library's computerized database of holdings (books, magazines, videos, and so on) is available to any member of the public at a computer in the library or at a home, office or school computer using dial-up access or the Internet. In addition, any person can browse the shelves of the library to see what is owned. Finally, a registered patron may look up his or her record at a library computer or from a home, office or school computer. We only do a sampling of requests made to library staff for holdings database information and maintain no accurate records of "do-it-yourself" searching.

Department of Natural Resources.
Difficulties in complying:

It's often difficult when there are mixed interpretations as to our responsibilities to collect the data being requested. It can be very difficult to find copies of all material related to a specific subject when that information can be found throughout the department in multiple formats.

It can also be difficult to find accurate historical data without extensive research.

Requests are often vague "give me all you got." These types of requests eat up a lot of staff time and are costly.

The classification of the data can vary greatly depending on the purpose and request, i.e., civil investigative data vs. criminal investigative data vs. employment data.

Because there are penalties for not releasing data, and for releasing data that should not be released, staff are very cautious in releasing and determining classifications. This sometimes calls for review of lots of information and takes time, which has been misconstrued as stalling to release information.

APPENDIX 5

Draft Legislation

A. Legislation to deal with confusing and inconsistent language in Minnesota Statutes.

B. Legislation to reduce some complexity of language in Minnesota Statutes Chapter 13. (Not available electronically.)

A bill for an act

relating to government data; clarifying and providing for data classifications; amending Minnesota Statutes 1998, sections 18B.38, subdivision 2; 31A.27, subdivision 3; 32.19; 46.07; 47.66; 60A.03, subdivision 9; 60A.031, subdivision 4; 60A.135, subdivision 4; 60A.208, subdivision 7; 60A.93; 60A.968, subdivision 2; 60B.14, subdivision 3; 60C.14, subdivision 2; 60D.22; 60K.10; 62C.17, subdivision 4; 62G.20, subdivision 3; 116.075, subdivision 2; 136A.64, subdivision 2; 169.09, subdivision 13; 171.31; 171.32, subdivisions 1 and 3; 175.24; 175.27; 176.184, subdivision 5; 176.231, subdivision 8; 196.08; 254A.09; 257.56, subdivision 1; 257.70; 259.10, subdivision 2; 268A.05, subdivision 1; 297B.12; 297D.13, subdivision 1; 297E.03, subdivision 8; ~~298~~.48, subdivisions 2 and 4; 299C.065, subdivision 4; 319B.11, subdivision 6; 469.154, subdivision 2; 471.617, subdivision 5; and 626.53, subdivision 1; repealing Minnesota Statutes 1998, sections 144.58; and 297D.13, subdivisions 2 and 3.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 1998, section 18B.38, subdivision 2, is amended to read:

Subd. 2. ~~**INFORMATION REVEALED**~~ **PRIVATE OR NONPUBLIC DATA.** After consideration of the applicant's request submitted under subdivision 1, ~~the commissioner shall not make any information public~~ information that in the commissioner's judgment contains or relates to trade secrets or to commercial or financial information obtained from an applicant are private data on individuals or nonpublic data as defined in section 13.02. When necessary, information relating to formulas of products may be revealed to any state or federal agency consulted with similar protection of trade secret authority and may be revealed at a public hearing or in findings of facts issued by the commissioner.

Sec. 2. Minnesota Statutes 1998, section 31A.27, subdivision 3, is amended to read:

Subd. 3. **PENALTIES RELATED TO TESTIMONY AND RECORDS.**

(a) A person who neglects or refuses to attend and testify, to answer a lawful inquiry, or to produce documentary evidence, if it is in the person's power to do so, in obedience to the subpoena or lawful requirement of the commissioner is guilty of a misdemeanor.

(b) A person who willfully (1) makes or causes to be made a false entry or statement of fact in a report required under this chapter; (2) makes or causes to be made a false entry in an account, record, or memorandum kept by a person subject to this chapter; (3) neglects or fails to make or to cause to be made full and correct entries in the accounts, records, or memoranda, of all facts and transactions relating to the person's business; (4) leaves the jurisdiction of this state; (5) mutilates, alters, or by any other means falsifies documentary evidence of a person subject to this chapter; or (6) refuses to submit to the commissioner, for inspection and copying, any documentary evidence of a person subject to this chapter in the person's possession or control, is

guilty of a misdemeanor.

(c) A person required by this chapter to file an annual or special report who fails to do so within the time fixed by the commissioner for filing the report and continues the failure for 30 days after notice of failure to file, is guilty of a misdemeanor.

(d) ~~An officer or employee of this state who makes public information obtained by the commissioner without the commissioner's authority, unless directed by a court, is guilty of a misdemeanor~~. Information obtained by the commissioner under this section are private data on individuals or nonpublic data as defined in section 13.02 but may be released by the commissioner or under court order.

Sec. 3. Minnesota Statutes 1998, section 32.19, is amended to read:

32.19 **REPORTS; CONTENTS NOT TO BE DIVULGED, PENALTY.**

(a) Every person, owner, or operator required by section 32.18 to maintain daily records on milk, cream, butterfat and other dairy products shall, within 90 days following the close of each fiscal year and at such other times as the commissioner may fix or require, by rules adopted as required by law, make and file with the commissioner, on blank forms prepared by the commissioner, itemized and verified reports of all business transacted by the commissioner, as set out in section 32.18, during the preceding fiscal year. Such reports shall contain such further information as, from time to time, may be required by the commissioner. A duplicate copy thereof shall be retained by such person, owner, or operator in files, which shall be subject to examination by the commissioner at any time. ~~It shall be unlawful for the commissioner, or any public official or employee to divulge or otherwise make known in any manner any particulars set forth or disclosed in any report or return required by this section, or any information concerning the business transacted by any such person, owner or operator so reporting, acquired from records, officers or employees while examining or inspecting any books or records kept and maintained as required by section 32.18, except as such information is required or authorized to be disclosed in a judicial proceeding by order of the district court. Except as last stated and with the authority there required, any person violating the provision of this section establishing the confidential character of such information and the reports or returns required to be made and filed with the commissioner shall be guilty of a gross misdemeanor.~~

~~Nothing herein contained shall be construed to prohibit the commissioner from publishing statistics so classified as not to disclose the identity of particular returns or reports or any item or entry therein contained.~~

(b) Reports received by the commissioner under this section and data from records under section 32.18 are private data on individuals or nonpublic data as defined in section 13.02.

Sec. 4. Minnesota Statutes 1998, section 46.07, is amended to read:

46.07 **RECORDS.**

Subdivision 1. **DEPARTMENT RECORDS.** The commissioner of commerce shall keep all proper records and files pertaining to the duties and work of that office.

Subd. 2. **CONFIDENTIAL ~~RECORDS~~ OR PROTECTED NONPUBLIC DATA.** ~~The commissioner shall divulge facts and information~~ Data obtained in the course of examining financial institutions under the commissioner's supervision are confidential data on individuals or protected nonpublic data as defined in section 13.02 and may be disclosed only when and to the extent required or permitted by law to report upon or take special action regarding the affairs of an institution, or ordered by a court of law to testify or produce evidence in a civil or criminal

proceeding~~, except that~~. The commissioner may furnish information as to matters of mutual interest to an official or examiner of the federal reserve system, the Federal Deposit Insurance Corporation, the Federal Office of Thrift Supervision, the Federal Home Loan Bank System, the National Credit Union Administration, comptroller of the currency, other state bank supervisory agencies subject to cooperative agreements authorized by section 49.411, subdivision 7, the United States Small Business Administration, for purposes of sections 53.09, subdivision 2a, and 56.10, subdivision 1, or state and federal law enforcement agencies. ~~The commissioner shall not be required to disclose the name of a debtor of a financial institution under the commissioner's supervision, or anything relative to the private accounts, ownership, or transactions of an institution, or any fact obtained in the course of an examination thereof, except as herein provided.~~ For purposes of this subdivision, a subpoena is not an order of a court of law. ~~These records are classified confidential or protected nonpublic for purposes of the Minnesota Government Data Practices Act and their~~ The destruction of this data, as prescribed in section 46.21, is exempt from the provisions of chapter 138 and Laws 1971, chapter 529, so far as their deposit with the state archives.

Subd. 3. **COMPLAINT FILES.** Notwithstanding the provisions of subdivision 2 to the contrary, data gathered and maintained in relation to a complaint filed with the commissioner is private data on individuals or nonpublic ~~pursuant to the Minnesota Government Data Practices Act~~ data as defined in section 13.02.

Sec. 5. Minnesota Statutes 1998, section 47.66, is amended to read:

47.66 **EXAMINATION.**

An electronic financial terminal or a transmission facility may be examined by the commissioner to the extent permitted by law as to any financial transaction by, with, or involving a financial institution solely for the purpose of reconciling accounts and verifying the security and accuracy of such electronic financial terminals or transmission facilities, including any supporting equipment, structures, or systems. ~~All facts and information~~ Data obtained in the course of such examination are confidential data on individuals or protected nonpublic data as defined in section 13.02 and shall not be disclosed except as otherwise provided by law. The person examined shall pay examination fees as determined by the commissioner.

Sec. 6. Minnesota Statutes 1998, section 60A.03, subdivision 9, is amended to read:

Subd. 9. **CONFIDENTIALITY OF INFORMATION.** ~~The commissioner may not be required to divulge any~~ Except as otherwise provided in this chapter or other law, information obtained by the commissioner in the course of the supervision or examination of insurance companies, ~~or the examination of insurance companies,~~ including examination related correspondence and workpapers~~, until~~ is private data on individuals or nonpublic data as defined in section 13.02. When the examination report is finally accepted and issued by the commissioner, ~~and then only in the form of~~ the final ~~public~~ report ~~of examinations~~ is public data. Nothing contained in this subdivision prevents or shall be construed as prohibiting the commissioner from disclosing the content of this information to the insurance department of another state or the National Association of Insurance Commissioners if the recipient of the information agrees in writing to hold it as private or nonpublic data as defined in section 13.02, in a manner consistent with this subdivision. This subdivision does not apply to the extent the commissioner is required or permitted by law, or ordered by a court of law to testify or produce evidence in a civil or criminal proceeding. For purposes of this subdivision, a subpoena is not an

order of a court of law.

Sec. 7. Minnesota Statutes 1998, section 60A.031, subdivision 4, is amended to read:

Subd. 4. **EXAMINATION REPORT; FOREIGN AND DOMESTIC COMPANIES.**

(a) The commissioner shall make a full and true report of every examination conducted pursuant to this chapter, which shall include (1) a statement of findings of fact relating to the financial status and other matters ascertained from the books, papers, records, documents, and other evidence obtained by investigation and examination or ascertained from the testimony of officers, agents, or other persons examined under oath concerning the business, affairs, assets, obligations, ability to fulfill obligations, and compliance with all the provisions of the law of the company, applicant, organization, or person subject to this chapter and (2) a summary of important points noted in the report, conclusions, recommendations and suggestions as may reasonably be warranted from the facts so ascertained in the examinations. The report of examination shall be verified by the oath of the examiner in charge thereof, and shall be prima facie evidence in any action or proceedings in the name of the state against the company, applicant, organization, or person upon the facts stated therein.

(b) No later than 60 days following completion of the examination, the examiner in charge shall file with the department a verified written report of examination under oath. Upon receipt of the verified report, the department shall transmit the report to the company examined, together with a notice which provides the company examined with a reasonable opportunity of not more than 30 days to make a written submission or rebuttal with respect to matters contained in the examination report.

(c) Within 30 days of the end of the period allowed for the receipt of written submissions or rebuttals, the commissioner shall fully consider and review the report, together with the written submissions or rebuttals and the relevant portions of the examiner's workpapers and enter an order:

(1) adopting the examination report as filed or with modification or corrections. If the examination report reveals that the company is operating in violation of any law, rule, or prior order of the commissioner, the commissioner may order the company to take any action the commissioner considers necessary and appropriate to cure the violation;

(2) rejecting the examination report with directions to the examiners to reopen the examination for purposes of obtaining additional data, documentation, or information, and refiling the report as required under paragraph (b); or

(3) calling for an investigatory hearing with no less than 20 days' notice to the company for purposes of obtaining additional documentation, data, information, and testimony.

(d)(1) All orders entered under paragraph (c), clause (1), must be accompanied by findings and conclusions resulting from the commissioner's consideration and review of the examination report, relevant examiner workpapers, and any written submissions or rebuttals. The order is a final administrative decision and may be appealed as provided under chapter 14. The order must be served upon the company by certified mail, together with a copy of the adopted examination report. Within 30 days of the issuance of the adopted report, the company shall file affidavits executed by each of its directors stating under oath that they have received a copy of the adopted report and related orders.

(2) A hearing conducted under paragraph (c), clause (3), by the commissioner or authorized representative, must be conducted as a nonadversarial confidential investigatory proceeding as necessary for the resolution of inconsistencies, discrepancies, or disputed issues

apparent upon the face of the filed examination report or raised by or as a result of the commissioner's review of relevant workpapers or by the written submission or rebuttal of the company. Within 20 days of the conclusion of the hearing, the commissioner shall enter an order as required under paragraph (c), clause (1).

(3) The commissioner shall not appoint an examiner as an authorized representative to conduct the hearing. The hearing must proceed expeditiously. Discovery by the company is limited to the examiner's workpapers which tend to substantiate assertions in a written submission or rebuttal. The commissioner or the commissioner's representative may issue subpoenas for the attendance of witnesses or the production of documents considered relevant to the investigation whether under the control of the department, the company, or other persons. The documents produced must be included in the record. Testimony taken by the commissioner or the commissioner's representative must be under oath and preserved for the record.

This section does not require the department to disclose information or records which would indicate or show the existence or content of an investigation or activity of a criminal justice agency.

(4) The hearing must proceed with the commissioner or the commissioner's representative posing questions to the persons subpoenaed. Thereafter, the company and the department may present testimony relevant to the investigation. Cross-examination may be conducted only by the commissioner or the commissioner's representative. The company and the department shall be permitted to make closing statements and may be represented by counsel of their choice.

(e)(1) Notwithstanding section 60A.03, subdivision 9, upon the adoption of the examination report under paragraph (c), clause (1), ~~the commissioner shall continue to hold the content of~~ the examination report ~~as private and confidential information~~ is private data on individuals or nonpublic data as defined in section 13.02 for a period of 30 days except as otherwise provided in paragraph (b). ~~Thereafter~~ After that period, ~~the commissioner may open~~ the report ~~for public inspection if~~ is public data unless a court of competent jurisdiction ~~has not stayed~~ stays its publication.

(2) Nothing contained in this subdivision prevents or shall be construed as prohibiting the commissioner from disclosing the content of an examination report, preliminary examination report or results, or any matter relating to the reports, to the commerce department or the insurance department of another state or country, the National Association of Insurance Commissioners, or to law enforcement officials of this or another state or agency of the federal government at any time, if the agency or office receiving the report or matters relating to the report agrees in writing to hold it ~~confidential and~~ in a manner consistent with this subdivision.

(3) If the commissioner determines that regulatory action is appropriate as a result of an examination, the commissioner may initiate proceedings or actions as provided by law.

(f) All ~~working papers, recorded information, documents and copies thereof~~ data produced by, obtained by, or disclosed to the commissioner or any other person in the course of an examination made under this subdivision ~~must be given confidential treatment~~ are private data on individuals or nonpublic data and are not subject to subpoena and may not be made public ~~by the commissioner or any other person~~, except to the extent provided in paragraph (e). ~~Access may also be granted to the National Association of Insurance Commissioners. The parties must agree in writing prior to receiving the information to provide to it the same confidential treatment as required by this section, unless the prior written consent of the company to which it pertains has been obtained.~~

Sec. 8. Minnesota Statutes 1998, section 60A.135, subdivision 4, is amended to read:

Subd. 4. **CONFIDENTIALITY.** Reports filed with the commissioner pursuant to sections 60A.135 to 60A.137 ~~must be held as~~ are nonpublic data as defined in section 13.02, are not subject to subpoena, and may not be ~~made public by the commissioner, the National Association of Insurance Commissioners, or other person, except to insurance departments of other states,~~ released without the prior written consent of the insurer to which ~~it~~ a report pertains, except as provided in section 60A.03, subdivision 9. However, the commissioner may publish all or part of a report in the manner the commissioner considers appropriate if, after giving the affected insurer notice and an opportunity to be heard, the commissioner determines that the interest of policyholders, shareholders, or the public will be served by the publication.

Sec. 9. Minnesota Statutes 1998, section 60A.208, subdivision 7, is amended to read:

Subd. 7. **REPORTS AND RECOMMENDATIONS BY THE ASSOCIATION.** An association may submit reports and make recommendations to the commissioner regarding the financial condition of any eligible surplus lines insurer. ~~These~~ The reports and recommendations ~~shall not be considered to be public information~~ are nonpublic data as defined in section 13.02. There shall not be liability on the part of, or a cause of action of any nature shall not arise against, eligible surplus lines insurers, the association or its agents or employees, the directors, or the commissioner or authorized representatives of the commissioner, for statements made by them in any reports or recommendations made under this subdivision.

Sec. 10. Minnesota Statutes 1998, section 60A.93, is amended to read:

60A.93 **CONFIDENTIALITY.**

All financial analysis ratios and examination synopses concerning insurance companies that are submitted to the department by the National Association of Insurance Commissioners' Insurance Regulatory Information System are ~~confidential and may not be disclosed by the department~~ protected nonpublic data as defined in section 13.02.

Sec. 11. Minnesota Statutes 1998, section 60A.968, subdivision 2, is amended to read:

Subd. 2. **PRIVATE DATA.** ~~Names and individual identification data for all~~ Data on viators ~~is~~ are private ~~and confidential information and must not be disclosed by the commissioner, unless required by law~~ data on individuals as defined in section 13.02.

Sec. 12. Minnesota Statutes 1998, section 60B.14, subdivision 3, is amended to read:

Subd. 3. **RECORDS.** In all summary proceedings and judicial reviews thereof, all records of the company, other documents, and all department of commerce files and court records and papers, so far as they pertain to or are a part of the record of the summary proceedings, shall be and remain confidential except as is necessary to obtain compliance therewith, unless the court, after hearing arguments from the parties in chambers, shall order otherwise, or unless the insurer requests that the matter be made public. Until such court order, all papers filed with the court administrator shall be held in a confidential file. Department of commerce data relating to summary proceedings are private data on individuals or nonpublic data as defined in section 13.02.

Sec. 13. Minnesota Statutes 1998, section 60C.14, subdivision 2, is amended to read:

Subd. 2. **OPTIONAL POWERS AND DUTIES.** The commissioner may:

(a) Suspend or revoke, after notice and hearing, the certificate of authority to transact insurance or to execute surety bonds in this state of any member insurer which fails to pay an assessment when due or fails to comply with the plan of operation. As an alternative, the commissioner may levy a fine on any member insurer which fails to pay an assessment when due. The fine shall not exceed five percent of the unpaid assessment per month, except that no fine shall be less than $100 per month.

(b) Revoke the designation of any servicing facility if the commissioner finds claims are being handled unsatisfactorily.

(c) Disclose to the board of directors information regarding any member insurer, or any company seeking admission to transact insurance business in this state, whose financial condition may be hazardous to policyholders or to the public, including data that are not public data as defined in section 13.02. ~~This disclosure does not violate any data privacy requirement or any obligation to treat the information as privileged. This disclosure does not change the data privacy or privileged status of the information.~~ Board members shall not disclose the information to anyone else or use the information for any purpose other than their duties as board members.

Sec. 14. Minnesota Statutes 1998, section 60D.22, is amended to read:

60D.22 ~~**CONFIDENTIAL TREATMENT**~~ **ACCESS TO DATA.**

~~All information, documents, and copies of them~~ Data obtained by or disclosed to the commissioner or any other person in the course of an examination or investigation made pursuant to section 60D.20 and all information reported pursuant to sections 60D.18 and 60D.19~~, shall be given confidential treatment and shall not be subject to subpoena and shall not be made public by the commissioner, the National Association of Insurance Commissioners, or any other person, except to insurance departments of other states, without the prior written consent of the insurer to which it pertains unless~~ are private data on individuals or nonpublic data as defined in section 13.02 but may be released as provided in section 60A.03, subdivision 9. In addition, the data may be released if the commissioner, after giving the insurer and its affiliates who would be affected, notice and opportunity to be heard, determines that the interest of policyholders or the public will be served by the publication, in which event the commissioner may publish all or any part in the manner the commissioner considers appropriate.

Sec. 15. Minnesota Statutes 1998, section 60K.10, is amended to read:

60K.10 **TERM OF APPOINTMENTS.**

All appointments of agents by insurers pursuant to this section shall remain in force until terminated voluntarily by the appointing insurer or the license of the agent has for any reason been terminated during the appointment. The original appointing insurer, as well as any subsequent appointing insurer, may terminate the appointment of an agent at any time by giving written notice thereof to the commissioner and by sending a copy thereof to the last known address of the agent. The effective date of the termination shall be the date of receipt of the notice by the commissioner unless another date is specified by the insurer in the notice. Within 30 days after the insurer gives notice of termination to the commissioner, the insurer shall furnish the agent with a current statement of the agent's commission account.

Accompanying the notice of a termination given to the commissioner by the insurer shall be a statement of the specific reasons constituting the cause of termination. Any document, record, or statement relating to the agent which is disclosed or furnished to the commissioner

contemporaneously with, or subsequent to, the notice of termination ~~shall be deemed confidential by the commissioner and a privileged communication~~ is private data on individuals as defined in section 13.02. The document, record, or statement furnished to the commissioner is a privileged communication and shall not be admissible in whole or in part for any purpose in any action or proceeding against (1) the insurer or any of its officers, employees, or representatives submitting or providing the document, record, or statement, or (2) any person, firm, or corporation furnishing in good faith to the insurer the information upon which the reasons for termination are based.

Sec. 16. Minnesota Statutes 1998, section 62C.17, subdivision 4, is amended to read:

Subd. 4. The commissioner may at any time after a hearing pursuant to the contested case provisions of chapter 14, revoke or suspend a license if satisfied that the licensee is not qualified. An application for a new license or for reinstatement may be entertained one year after revocation or suspension, upon filing of a bond in the amount of $5,000 approved by the commissioner for protection of the public for a period of five years, or a lesser amount and period as the commissioner may prescribe. The commissioner shall revoke or suspend a license upon written request by the corporation or agent for which the licensee is licensed to act. Such a request shall include a statement of the specific facts constituting cause for termination. ~~Any such information shall be deemed~~ The request is private data on individuals or nonpublic data as defined in section 13.02. The request is a confidential and privileged communication, and shall not be admissible, in whole or in part, in any action or proceeding without the corporation's or agent's written consent.

Sec. 17. Minnesota Statutes 1998, section 62G.20, subdivision 3, is amended to read:

Subd. 3. The commissioner may at any time after a hearing pursuant to sections 14.001 to 14.69, revoke or suspend a license if satisfied that the licensee is not qualified. An application for a new license or for reinstatement may be entertained one year after revocation or suspension, upon filing of a bond in the amount of $5,000 approved by the commissioner for protection of the public for a period of five years, or a lesser amount and period as the commissioner may prescribe. The commissioner shall revoke or suspend a license upon written request by the legal service plan corporation or agent for which the licensee is licensed to act. The request shall include a statement of the specific facts constituting cause for termination. The request is private data on individuals or nonpublic data as defined in section 13.02. Information contained in a request is confidential and privileged and is not admissible, in whole or in part, in any action or proceeding without the written consent of the party submitting the request.

Sec. 18. Minnesota Statutes 1998, section 116.075, subdivision 2, is amended to read:

Subd. 2. Any records or other information obtained by the pollution control agency or furnished to the agency by the owner or operator of one or more air contaminant or water or land pollution sources which are certified by said owner or operator, and said certification, as it applies to water pollution sources, is approved in writing by the commissioner, to relate to (a) sales figures, (b) processes or methods of production unique to the owner or operator, or (c) information which would tend to affect adversely the competitive position of said owner or operator, ~~shall be only for the confidential use of the agency in discharging its statutory obligations, unless otherwise specifically authorized by said owner or operator~~ are private data on individuals or nonpublic data as defined in section 13.02. ~~Provided, however that all such~~

~~information may be used by the agency in compiling or publishing analyses or summaries relating to the general condition of the state's water, air and land resources so long as such analyses or summaries do not identify any owner or operator who has so certified. Notwithstanding the foregoing,~~ The agency may disclose any information~~, whether or not otherwise considered confidential which~~ that it is obligated to disclose in order to comply with federal law and regulations, to the extent and for the purpose of such federally required disclosure.

Sec. 19. Minnesota Statutes 1998, section 136A.64, subdivision 2, is amended to read:

Subd. 2. ~~The office shall not disclose~~ Financial records provided to ~~it~~ the office by a school pursuant to this section ~~except~~ are nonpublic data as defined in section 13.02 but may be disclosed for the purpose of defending, at hearings pursuant to chapter 14, or other appeal proceedings, ~~its~~ a decision to approve or not to approve the granting of degrees or the use of a name by the school. Section 15.17, subdivision 4, shall not apply to such records.

Sec. 20. Minnesota Statutes 1998, section 169.09, subdivision 13, is amended to read:

Subd. 13. **REPORTS CONFIDENTIAL; EVIDENCE, FEE, PENALTY, APPROPRIATION.** (a) All written reports and supplemental reports required under this section ~~shall be~~ are confidential data on individuals or protected nonpublic data as defined in section 13.02 and are only for the use of the commissioner of public safety and other appropriate state, federal, county, and municipal governmental agencies for accident analysis purposes, except:

(1) the commissioner of public safety or any law enforcement agency shall, upon written request of any person involved in an accident or upon written request of the representative of the person's estate, surviving spouse, or one or more surviving next of kin, or a trustee appointed pursuant to section 573.02, disclose to the requester, the requester's legal counsel, or a representative of the requester's insurer the report required under subdivision 8;

(2) the commissioner of public safety shall, upon written request, provide the driver filing a report under subdivision 7 with a copy of the report filed by the driver;

(3) the commissioner of public safety may verify with insurance companies vehicle insurance information to enforce sections 65B.48, 169.792, 169.793, 169.796, and 169.797;

(4) the commissioner of public safety shall provide the commissioner of transportation the information obtained for each traffic accident involving a commercial motor vehicle, for purposes of administering commercial vehicle safety regulations; and

(5) the commissioner of public safety may give to the United States Department of Transportation commercial vehicle accident information in connection with federal grant programs relating to safety.

(b) Accident reports and data contained in the reports shall not be discoverable under any provision of law or rule of court. No report shall be used as evidence in any trial, civil or criminal, arising out of an accident, except that the commissioner of public safety shall furnish upon the demand of any person who has, or claims to have, made a report, or, upon demand of any court, a certificate showing that a specified accident report has or has not been made to the commissioner solely to prove compliance or failure to comply with the requirements that the report be made to the commissioner.

(c) Nothing in this subdivision prevents any person who has made a report pursuant to this section from providing information to any persons involved in an accident or their representatives or from testifying in any trial, civil or criminal, arising out of an accident, as to

facts within the person's knowledge. It is intended by this subdivision to render privileged the reports required, but it is not intended to prohibit proof of the facts to which the reports relate.

(d) Disclosing any information contained in any accident report, except as provided in this subdivision, section 13.82, subdivision 3 or 4, or other statutes, is a misdemeanor.

(e) The commissioner of public safety may charge authorized persons a $5 fee for a copy of an accident report.

(f) The commissioner and law enforcement agencies may charge commercial users who request access to response or incident data relating to accidents a fee not to exceed 50 cents per report. "Commercial user" is a user who in one location requests access to data in more than five accident reports per month, unless the user establishes that access is not for a commercial purpose. Money collected by the commissioner under this paragraph is appropriated to the commissioner.

Sec. 21. Minnesota Statutes 1998, section 171.31, is amended to read:

171.31 **PERSON RECEIVING BENEFITS FOR BLINDNESS, DISCOVERY OF INFORMATION.**

The commissioner of public safety, in order to promote highway safety by restricting driving privileges to those persons meeting accepted visual acuity standards, ~~may request and shall receive information~~ has access to private or confidential data on individuals as defined in section 13.02, concerning the identity and whereabouts of any person who has applied for or received any type of welfare, licensing, or other benefits for the blind or nearly blind, from the records of ~~all departments, boards, bureaus, or other agencies of this state except the department of revenue, and they shall provide such information notwithstanding the provisions of section 268.19 or any other existing law or rule to the contrary~~ state agencies, except ~~that~~ when section 270B.02, subdivision 1, prohibits disclosure of information by the commissioner of revenue.

Sec. 22. Minnesota Statutes 1998, section 171.32, subdivision 1, is amended to read:

Subdivision 1. **ACTIONS BY COMMISSIONER.** The commissioner upon receipt of ~~any such~~ information under section 171.31 shall take such action as the commissioner deems necessary to insure that each such person meets the accepted visual acuity standards required of all driver's license applicants and such further action as required by law or rule. The driver's license of any person who has been classified as legally blind shall be immediately canceled.

Sec. 23. Minnesota Statutes 1998, section 171.32, subdivision 3, is amended to read:

Subd. 3. **USE OF EXAMINATION DATA.** (a) Information received by the commissioner under this section is confidential data on individuals as defined in section 13.02, except that:

(1) the results of any visual acuity examination administered because of information received pursuant to ~~this~~ section 171.31 may be communicated by the commissioner to the ~~department~~ state agency from which the person received a benefit. ~~The information received by the commissioner pursuant to this section must not be divulged or otherwise made known in any manner except in connection with the cancellation of drivers licenses, and then only to the person involved whose license is canceled, and except for statistical purposes which do not reveal the identity of the individuals involved~~; and

(2) information may be disclosed to the subject of the data if the subject's driver's license is canceled.

(b) The record of such person with respect to visual acuity shall be maintained in the same manner as all other driver's license records.

Sec. 24. Minnesota Statutes 1998, section 175.24, is amended to read:

175.24 **DUTIES OF EMPLOYERS AND OTHERS TO MAKE REPORTS; PRESERVATION OF RECORDS.**

On request of the department of labor and industry, and within the time limited therein, every employer of labor, any officer of a labor organization, or any person from whom the department of labor and industry shall find it necessary to gather information, shall make a certified report to the department, upon blanks furnished by it, of all matters covered by the request. ~~The names of persons or concerns supplying such information shall not be disclosed.~~ Every notice, order, or direction given by such department shall be in writing, signed by an officer or inspector of such department, or a person specially designated for the purpose, and be served by the signer. Except as otherwise provided by law, papers so served and ~~all records and documents of~~ data received by the department under this section are ~~hereby declared~~ public ~~documents~~ data and shall not be destroyed ~~within~~ earlier than two years after their return or receipt by such department. The identity of persons supplying the information are private data on individuals or nonpublic data as defined in section 13.02.

Sec. 25. Minnesota Statutes 1998, section 175.27, is amended to read:

175.27 ~~**DISCLOSURE OF NAMES OF PERSONS GIVING INFORMATION;**~~ **REFUSAL TO TESTIFY; DENYING ADMISSION; PENALTY.**

~~Any employee of the department of labor and industry who shall disclose the names of any~~ Data on persons supplying information at the request of such department ~~shall be guilty of a misdemeanor~~ are private data on individuals or nonpublic data as defined in section 13.02. Any person who, having been duly subpoenaed, shall refuse to attend or testify in any hearing under the direction of the department of labor and industry shall be guilty of a misdemeanor. Any owner or occupant of any place of employment who shall refuse to admit thereto any employee of the department seeking entrance in the discharge of the employee's duties, shall be guilty of a misdemeanor. Any person, firm, or corporation, or any of its officers or agents, who or which shall refuse to file with the department such reports as are required by it under the provisions of sections 175.24 to 175.27 shall be guilty of a misdemeanor.

Sec. 26. Minnesota Statutes 1998, section 176.184, subdivision 5, is amended to read:

Subd. 5. **REQUEST FOR INVESTIGATION BY EMPLOYEE.** (a) Any employee or representative of an employee who believes that their employer is uninsured against workers' compensation liability, may request an inspection by giving notice to the commissioner of the belief and grounds for the belief. Any notice shall be written, shall set forth with reasonable particularity the grounds for the notice, and shall be signed by the employee or representative of employees. A copy of the notice shall be provided the employer, representative, or agent no later than the time of inspection, except that, upon the request of a person giving the notice, the employee's name and the names of individual employees referred to in the notice are private data on individuals as defined in section 13.02, subdivision 2, and shall not appear in the copy or on any record published, released, or made available. If upon receipt of the notification the commissioner determines that reasonable grounds exist to believe that the employer is uninsured against workers' compensation liability, the commissioner shall make an inspection in

accordance with this section as soon as practicable. If the commissioner determines that there are not reasonable grounds to believe that a violation exists, the commissioner shall so notify the employee or representative of employees in writing. Upon notification, the employee or the employee representative may request the commissioner to reconsider the determination. Upon receiving the request, the commissioner shall review the determination.

(b) The commissioner, upon receipt of a report of violation of the mandatory insurance provisions of section 176.181 or 176.185 verified by review of the department's insurance registration records and other relevant information, shall initiate a preliminary investigation to determine if reasonable grounds exist to believe that the employer is uninsured against workers' compensation liability, and upon certification of reasonable belief that the employer is uninsured the commissioner shall make an inspection in accordance with paragraph (a).

Sec. 27. Minnesota Statutes 1998, section 176.231, subdivision 8, is amended to read:

Subd. 8. **NO PUBLIC INSPECTION OF REPORTS.** Subject to subdivision 9, a report ~~or its copy which has been~~ filed with the commissioner of the department of labor and industry under this section is ~~not available to public inspection~~ private data on individuals or nonpublic data as defined in section 13.02. Any person who has access to such a report shall not disclose its contents to anyone in any manner.

A person who unauthorizedly discloses a report or its contents to another is guilty of a misdemeanor.

Sec. 28. Minnesota Statutes 1998, section 196.08, is amended to read:

196.08 **FILES AND RECORDS CONFIDENTIAL.**

~~The contents of, and all files, records, reports, papers and documents~~ Data pertaining to, any claim for the benefits of Laws 1943, chapter 420, whether pending or adjudicated, ~~shall be deemed confidential and privileged~~ are private data on individuals as defined in section 13.02 and no disclosure ~~thereof~~ shall be made, without the consent in writing of the claimant who has not been adjudicated incompetent, except as follows:

(a) To said claimant personally, a duly appointed guardian, an attorney in fact, or a duly authorized representative, and as to personal matters, when, in the judgment of the commissioner, such disclosure would not be injurious to the physical or mental health of the claimant.

(b) To the representatives of veterans' organizations recognized by the United States government, not exceeding five from each such veterans' organizations, and when such representatives have been duly certified as such by the state department of any such veterans' organizations in the state of Minnesota.

(c) In any court in the state of Minnesota which has jurisdiction of the parties to, and subject matter of, an action or proceeding therein pending, as found by said court, when required to be produced by the process of such court, and then only in open court, as evidence, in such action or proceeding after a judge thereof shall have ruled the same to be relevant and competent evidence in such action or proceeding according to the laws and statutes of said state.

Sec. 29. Minnesota Statutes 1998, section 254A.09, is amended to read:

254A.09 **CONFIDENTIALITY OF RECORDS.**

The department of human services shall assure confidentiality to individuals who are the subject of research by the state authority or are recipients of alcohol or drug abuse information,

assessment, or treatment from a licensed or approved program. ~~The commissioner shall withhold from all~~ Data on those individuals are private data on individuals as defined in section 13.02 and may not be released to persons not connected with the conduct of the research ~~the names or other identifying characteristics of a subject of research~~ unless the individual gives written permission that information relative to treatment and recovery may be released. Persons authorized to protect the privacy of subjects of research may not be compelled in any federal, state or local, civil, criminal, administrative or other proceeding to identify or disclose other confidential information about the individuals. Identifying information and other confidential information related to alcohol or drug abuse information, assessment, treatment, or aftercare services may be ordered to be released by the court for the purpose of civil or criminal investigations or proceedings if, after review of the records considered for disclosure, the court determines that the information is relevant to the purpose for which disclosure is requested. The court shall order disclosure of only that information which is determined relevant. In determining whether to compel disclosure, the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the treatment relationship in the program affected and in other programs similarly situated, and the actual or potential harm to the ability of programs to attract and retain patients if disclosure occurs. This section does not exempt any person from the reporting obligations under section 626.556, nor limit the use of information reported in any proceeding arising out of the abuse or neglect of a child. Identifying information and other confidential information related to alcohol or drug abuse information, assessment, treatment, or aftercare services may be ordered to be released by the court for the purpose of civil or criminal investigations or proceedings. No information may be released pursuant to this section that would not be released pursuant to section 595.02, subdivision 2.

Sec. 30. Minnesota Statutes 1998, section 257.56, subdivision 1, is amended to read:

Subdivision 1. If, under the supervision of a licensed physician and with the consent of her husband, a wife is inseminated artificially with semen donated by a man not her husband, the husband is treated in law as if he were the biological father of a child thereby conceived. The husband's consent must be in writing and signed by him and his wife. The consent must be retained by the physician for at least four years after the confirmation of a pregnancy that occurs during the process of artificial insemination.

All papers and records pertaining to the insemination, whether part of the permanent record of a court or of a file held by the supervising physician ~~or elsewhere~~, are subject to inspection only upon an order of the court for good cause shown. Government data pertaining to the insemination are confidential data on individuals as defined in section 13.02.

Sec. 31. Minnesota Statutes 1998, section 257.70, is amended to read:

257.70 **HEARINGS AND RECORDS; CONFIDENTIALITY.**

(a) Notwithstanding any other law concerning public hearings and records, any hearing or trial held under sections 257.51 to 257.74 shall be held in closed court without admittance of any person other than those necessary to the action or proceeding. All papers and records, other than the final judgment, pertaining to the action or proceeding~~, whether~~ that are part of the permanent record of the court ~~or of a file in the state department of human services or elsewhere,~~ are subject to inspection only upon consent of the court and all interested persons, or in exceptional cases only upon an order of the court for good cause shown. Government data pertaining to the action or proceeding are confidential data on individuals as defined in section 13.02.

(b) In all actions under this chapter in which public assistance is assigned under section 256.741 or the public authority provides services to a party or parties to the action, notwithstanding statutory or other authorization for the public authority to release private data on the location of a party to the action, information on the location of one party may not be released by the public authority to the other party if:

(1) the public authority has knowledge that a protective order with respect to the other party has been entered; or

(2) the public authority has reason to believe that the release of the information may result in physical or emotional harm to the other party.

Sec. 32. Minnesota Statutes 1998, section 259.10, subdivision 2, is amended to read:

Subd. 2. **WITNESS AND VICTIM PROTECTION NAME CHANGES; PRIVATE DATA.** If the court determines that the name change for an individual is made in connection with the individual's participation in a witness and victim protection program, the court shall order that the court records of the name change are not accessible to the public; except that they may be released, upon request, to a law enforcement agency, probation officer, or corrections agent conducting a lawful investigation. The existence of an application for a name change described in this subdivision may not be disclosed except to a law enforcement agency conducting a lawful investigation. Government data relating to an application for a name change are confidential data on individuals as defined in section 13.02.

Sec. 33. Minnesota Statutes 1998, section 268A.05, subdivision 1, is amended to read:

Subdivision 1. **PUBLIC RECORDS; ACCESS.** The employees of the department specifically authorized by the commissioner shall have the right to receive from any ~~public~~ government records the names, addresses and information pertinent to ~~their~~ the vocational rehabilitation of persons injured or otherwise disabled. ~~Except as provided in subdivision 2, no information obtained from these reports, nor any copy of the same, nor any of the contents thereof, nor other confidential information as defined by the commissioner shall be open to the public, nor shall be disclosed in any manner by any official or clerk or other employee of the state having access thereto, but the same may be used, except as provided in subdivision 2,~~ Data related to the vocational rehabilitation are private data on individuals as defined in section 13.02 and may be used solely to enable the department to offer the benefits of vocational rehabilitation to the persons injured or otherwise disabled.

Sec. 34. Minnesota Statutes 1998, section 297B.12, is amended to read:

297B.12 **PRIVATE NATURE OF INFORMATION.**

~~It shall be unlawful for the motor vehicle registrar, deputy registrars or any other public official or employee to divulge or otherwise make known in any manner any particulars disclosed~~ Data in any purchaser's certificate or any information concerning affairs of any person making such certificate acquired from the purchaser's records, officers or employees are private data on individuals or nonpublic data as defined in section 13.02 and may not be disclosed, except in connection with state or federal tax proceedings ~~or upon request of the person named on the certificate. Nothing herein contained should be construed to prohibit the publishing of statistics so classified as not to disclose the identity of particular purchasers' certificates and the contents thereof. Any person violating the provisions of this section shall be guilty of a gross misdemeanor.~~

Sec. 35. Minnesota Statutes 1998, section 297D.13, subdivision 1, is amended to read:

Subdivision 1. **DISCLOSURE PROHIBITED.** ~~Notwithstanding any law to the contrary, neither the commissioner nor a public employee may reveal facts~~ Data contained in a report or return required by this chapter ~~or~~ and any information obtained from a tax obligor~~; nor can any~~ are private data on individuals as defined in section 13.02. Information contained in such a report or return or obtained from a tax obligor may not be used against the tax obligor in any criminal proceeding, unless independently obtained, except in connection with a proceeding involving taxes due under this chapter from the tax obligor making the return.

Sec. 36. Minnesota Statutes 1998, section 297E.03, subdivision 8, is amended to read:

Subd. 8. **DISCLOSURE PROHIBITED.** ~~(a) Notwithstanding any law to the contrary, neither the commissioner nor a public employee may reveal facts~~ Data contained in a sports bookmaking tax return filed with the commissioner of revenue ~~as required by~~ under this section~~; nor can any~~ are private data on individuals as defined in section 13.02. Information contained in the report or return may not be used against the tax obligor in any criminal proceeding, unless independently obtained, except in connection with a proceeding involving taxes due under this section, or as provided in section 270.064.

~~(b) Any person violating this section is guilty of a gross misdemeanor.~~

~~(c) This section does not prohibit the commissioner from publishing statistics that do not disclose the identity of tax obligors or the contents of particular returns or reports.~~

Sec. 37. Minnesota Statutes 1998, section 298.48, subdivision 2, is amended to read:

Subd. 2. **USE OF ~~DATE~~ DATA.** Notwithstanding any other law to the contrary, the commissioner of revenue may use any data filed pursuant to subdivision 1 and any similar data otherwise obtained to the extent and in the manner the commissioner deems necessary to project the future availability, value, and utilization of the metallic mineral resources of this state. In making such projections the commissioner of revenue may consult with, and provide data as deemed appropriate to, the commissioner of natural resources.

Sec. 38. Minnesota Statutes 1998, section 298.48, subdivision 4, is amended to read:

Subd. 4. **CONFIDENTIAL NATURE OF INFORMATION.** The data filed pursuant to subdivision 1 ~~shall be considered~~ are confidential data on individuals or protected nonpublic data as defined in section 13.02 for three years from the date ~~it is~~ the data are filed with the commissioner. ~~Nothing herein contained shall be construed to prohibit the commissioner from disclosing information or publishing statistics so classified as not to disclose the identity of particular data.~~

Notwithstanding the other provisions of this subdivision, the commissioner may furnish any information supplied under this section to the commissioner of natural resources, the commissioner of trade and economic development, or a county assessor. ~~Any person violating the provisions of this section shall be guilty of a gross misdemeanor.~~

Sec. 39. Minnesota Statutes 1998, section 299C.065, subdivision 4, is amended to read:

Subd. 4. **DATA CLASSIFICATION.** ~~An~~ Data in an application ~~to the commissioner~~ for ~~money is~~ a grant under this section are confidential ~~record~~ data on individuals or protected nonpublic data as defined in section 13.02. Information within investigative files that identifies or could reasonably be used to ascertain the identity of assisted witnesses, sources, or undercover

investigators is a confidential ~~record~~ data on individuals. A report at the conclusion of an investigation is a public ~~record~~ data, except that ~~information~~ data in a report ~~pertaining to~~ on the identity or location of an assisted witness ~~is~~ are private data.

Sec. 40. Minnesota Statutes 1998, section 319B.11, subdivision 6, is amended to read:

Subd. 6. **EXAMINATION BY BOARD.** (a) A board, or an employee or agent designated by a board, may inspect at all reasonable times all books and records of a professional firm and may summon and examine under oath the owners, directors, governors, officers, managers, persons occupying a position with governance authority, and employees of the firm in all matters concerning the operations of the professional firm that are governed by sections 319B.01 to 319B.12, the rules of the board, or the professional firm's generally applicable governing law. This subdivision does not authorize anyone to have access to or to compel anyone to testify with respect to books, records, or information of any type subject to a privilege recognized by law.

(b) Any information obtained by a board as a result of an examination authorized by paragraph (a) is ~~confidential~~ private data on individuals or nonpublic data as defined in section 13.02, immune from subpoena, and inadmissible as evidence at a trial, hearing, or proceeding before a court, board, or commissioner except a proceeding under subdivision 8.

(c) A professional firm subject to an examination under paragraph (a) may request in writing that the board under whose authority the examination is being or has been conducted provide the professional firm with a copy of all or any specified parts of the sworn testimony taken or received during the examination as well as all or any specified exhibits provided as part of that testimony. The board must comply promptly with the request and may charge the requesting firm the reasonable cost of making and providing the copies.

Sec. 41. Minnesota Statutes 1998, section 469.154, subdivision 2, is amended to read:

Subd. 2. **LOCAL REQUEST FOR ASSISTANCE.** Any municipality or redevelopment agency contemplating the exercise of the powers granted by sections 469.152 to 469.165 may apply to the commissioner for information, advice, and assistance. The commissioner may ~~handle such~~ treat the preliminary information ~~in a confidential manner~~, as nonpublic data as defined in section 13.02 to the extent requested by the municipality.

Sec. 42. Minnesota Statutes 1998, section 471.617, subdivision 5, is amended to read:

Subd. 5. **NONDISCLOSURE OF CLAIMS; EXCEPTION.** ~~No political subdivision or its employee or agent shall disclose any information about~~ Data on individual claims or total claims of an individual ~~without the consent of the individual~~ are private data on individuals as defined in section 13.02, except that the information may be disclosed to officers, employees, or agents of the political subdivision to the extent necessary to enable them to perform their duties in administering the health benefit program. ~~This provision shall not prevent the disclosure of aggregate claims for the group without identification of any individual.~~

~~A parent or legal guardian of a minor is authorized to act on behalf of the minor in the disclosure of a record.~~

Sec. 43. Minnesota Statutes 1998, section 626.53, subdivision 1, is amended to read:

Subdivision 1. **REPORTS TO SHERIFFS AND POLICE CHIEFS.** The report required by section 626.52, subdivision 2, shall be made forthwith by telephone or in person, and

shall be promptly supplemented by letter, enclosed in a securely sealed, postpaid envelope, addressed to the sheriff of the county in which the wound is examined, dressed, or otherwise treated; except that, if the place in which the patient is treated for such injury or the patient's wound dressed or bandaged be in a city of the first, second, or third class, such report shall be made and transmitted as herein provided to the chief of police of such city instead of the sheriff. Except as otherwise provided in subdivision 2, the report is confidential data on individuals as defined in section 13.02, and the office of any such sheriff and of any such chief of police shall keep the report as a confidential communication and shall not disclose the name of the person making the same, and the party making the report shall not by reason thereof be subpoenaed, examined, or forced to testify in court as a consequence of having made such a report.

Sec. 44. **REPEALER.**

Minnesota Statutes 1998, sections 144.58; and 297D.13, subdivisions 2 and 3, are repealed.

ARTICLE 2

TERMINOLOGY CHANGES

Section 1. Minnesota Statutes 1998, section 3.97, subdivision 11, is amended to read:

Subd. 11. "Audit" as used in this subdivision means a financial audit, a program evaluation, a best practices review, or an investigation. Data relating to an audit are ~~not public or with respect to data on individuals are~~ confidential until the final report of the audit has been published or the audit is no longer being actively pursued. Data that support the conclusions of the report and that the legislative auditor reasonably believes will result in litigation are ~~not public and with respect to data on individuals are~~ confidential until the litigation has been completed or is no longer being actively pursued. Data on individuals that could reasonably be used to determine the identity of an individual supplying data for an audit are private if the data supplied by the individual were needed for an audit and the individual would not have provided the data to the legislative auditor without an assurance that the individual's identity would remain private, or the legislative auditor reasonably believes that the subject would not have provided the data. The definitions of terms provided in section 13.02 apply for purposes of this subdivision.

Sec. 2. Minnesota Statutes 1998, section 6.715,

subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION.] Data relating to an audit are ~~protected nonpublic data or~~ confidential data ~~on individuals~~, until the final report of the audit has been published or the audit is no longer being actively pursued. Data that support the conclusions of the report and that the state auditor reasonably believes will result in litigation are ~~protected nonpublic data or~~ confidential data ~~on individuals~~, until the litigation has been completed or is no longer being actively pursued. Data on individuals that could reasonably be used to determine the identity of an individual supplying data for an audit are private data if the data supplied by the individual were needed for an audit and the individual would not have provided the data to the state auditor without an assurance that the individual's identity would remain private, or the state auditor reasonably believes that the subject would not have provided the data. Data that could reasonably be used to determine the identity of an individual supplying data pursuant to section 609.456 are private data. "Confidential data" and "private data" as used in this subdivision have the meanings given in section 13.02.

Sec. 3. Minnesota Statutes 1998, section 10A.02, subdivision 12, is amended to read:

Subd. 12. [ADVISORY OPINIONS.] (a) The board may issue and publish advisory opinions on the requirements of this chapter based upon real or hypothetical situations. An application for an advisory opinion may be made only by an individual or association who wishes to use the opinion to guide the individual's or the association's own conduct. The board shall issue written opinions on all such questions submitted to it within 30 days after receipt of written application, unless a majority of the board agrees to extend the time limit.

(b) A written advisory opinion issued by the board is binding on the board in any subsequent board proceeding concerning the person making or covered by the request and is a defense in a judicial proceeding that involves the subject

matter of the opinion and is brought against the person making or covered by the request unless:

(1) the board has amended or revoked the opinion before the initiation of the board or judicial proceeding, has notified the person making or covered by the request of its action, and has allowed at least 30 days for the person to do anything that might be necessary to comply with the amended or revoked opinion;

(2) the request has omitted or misstated material facts; or

(3) the person making or covered by the request has not acted in good faith in reliance on the opinion.

(c) A request for an opinion and the opinion itself are ~~nonpublic~~ private data, as defined in section 13.02, subdivision 12. The board, however, may publish an opinion or a summary of an opinion, but may not include in the publication the name of the requester, the name of a person covered by a request from an agency or political subdivision, or any other information that might identify the requester unless the person consents to the inclusion.

Sec. 4. Minnesota Statutes 1998, section 13.02, subdivision 3, is amended to read:

Subd. 3. [CONFIDENTIAL DATA ~~ON INDIVIDUALS~~.] "Confidential data ~~on individuals~~" means data, whether on individuals or not on individuals, ~~which~~ that is made ~~not public~~, by statute or federal law applicable to the data ~~and is~~, inaccessible to the ~~individual~~ public and to the subject of ~~that~~ the data.

Sec. 5. Minnesota Statutes 1998, section 13.02, is amended by adding a subdivision to read:

Subd. 7a. [GOVERNMENT ENTITY.] "Government entity" means a state agency, statewide system, or political subdivision.

Sec. 6. Minnesota Statutes 1998, section 13.02, subdivision 12, is amended to read:

Subd. 12. [PRIVATE DATA ~~ON INDIVIDUALS~~.] "Private data ~~on individuals~~" means data ~~which~~, whether on individuals or not on individuals, that is made, by statute or federal law applicable to the data ~~: (a) not public; and (b)~~, inaccessible to the

public but accessible to the ~~individual~~ subject of ~~that~~ the data.

Sec. 7. Minnesota Statutes 1998, section 13.02, subdivision 14, is amended to read:

Subd. 14. [PUBLIC DATA ~~NOT ON INDIVIDUALS~~.] "Public data ~~not on individuals~~" means data ~~which~~, whether on individuals or not on individuals, that is accessible to the public pursuant to section 13.03.

Sec. 8. Minnesota Statutes 1998, section 13.02, is amended by adding a subdivision to read:

Subd. 15a. "Representative of the decedent" means the personal representative of the estate of the decedent during the period of administration; or if no personal representative has been appointed or after discharge of the personal representative, the surviving spouse, a child of the decedent, or, if there is no surviving spouse or child, the parents of the decedent.

Sec. 9. Minnesota Statutes 1998, section 13.03, is amended to read:

13.03 [ACCESS TO GOVERNMENT DATA.]

Subdivision 1. [PUBLIC DATA.] All government data collected, created, received, maintained or disseminated by a ~~state agency, political subdivision, or statewide system shall~~ ~~be~~ government entity is public unless classified by statute, ~~or~~ temporary classification ~~pursuant to~~ under section 13.06, or federal law, as ~~nonpublic or protected nonpublic, or with respect to data on individuals,~~ as private or confidential. The responsible authority in every ~~state agency, political subdivision and statewide system~~ government entity shall keep records containing government data in ~~such~~ an arrangement and condition ~~as to make~~ that makes them easily accessible for convenient use. Photographic, photostatic, microphotographic, or microfilmed records ~~shall be~~ are considered ~~as~~ accessible for convenient use regardless of the size of ~~such~~ the records.

Subd. 2. [PROCEDURES.] The responsible authority in every ~~state agency, political subdivision, and statewide~~

~~system~~ government entity shall establish procedures, consistent with this chapter, to insure that requests for government data are received and complied with in an appropriate and prompt manner. 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.

A responsible authority may designate one or more designees.

Subd. 3. [REQUEST FOR ACCESS TO DATA.] Upon request to a responsible authority or designee, a person shall be permitted to inspect and copy public government data at reasonable times and places, and, upon request, shall be informed of the data's meaning. If a person requests access for the purpose of inspection, the responsible authority may not assess a charge or require the requesting person to pay a fee to inspect data. The responsible authority or designee shall provide copies of public data upon request. If a person requests copies or electronic transmittal of the data to the person, the responsible authority may require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from ~~not-public~~ private or confidential data. If the responsible authority or designee is not able to provide copies at the time a request is made, copies shall be supplied as soon as reasonably possible.

When a request under this subdivision involves ~~any~~ a person's receipt of copies of public government data that has commercial value and is a substantial and discrete portion of or an entire formula, pattern, compilation, program, device, method, technique, process, database, or system developed with a significant expenditure of public funds by the ~~agency~~ government entity, the responsible authority may charge a reasonable fee for the information in addition to the costs of making, certifying, and compiling the copies. Any fee charged must be

clearly demonstrated by the ~~ageney~~ government entity to relate to the actual development costs of the information. The responsible authority, upon the request of ~~any~~ a person, shall provide sufficient documentation to explain and justify the fee being charged.

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 inform the requesting person of the determination either orally at the time of the request, or in writing as soon after that time as possible, and shall cite the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based. Upon the request of ~~any~~ a person denied access to data, the responsible authority or designee shall certify in writing that the request has been denied and cite the specific statutory section, temporary classification, or specific provision of federal law upon which the denial was based.

Subd. 4. [CHANGE IN CLASSIFICATION OF DATA; EFFECT OF DISSEMINATION AMONG ~~AGENCIES~~ GOVERNMENT ENTITIES.] (a) The classification of data in the possession of ~~an agency~~ a government entity 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~~ government entity.

(b) If data on individuals is classified as both private and confidential by this chapter, or any other statute or federal law, the data is private.

(c) To the extent that government data is disseminated to ~~state agencies, political subdivisions, or statewide systems~~ a government entity by another ~~state agency, political subdivision, or statewide system~~ government entity , the data disseminated shall have the same classification in the hands of the ~~agency~~ government entity receiving it as it had in the hands of the government entity providing it.

(d) If a ~~state agency, statewide system, or political subdivision~~ government entity disseminates data to another ~~state agency, statewide system, or political subdivision~~ government entity, a classification provided for by law in the hands of the government entity receiving the data does not affect the classification of the data in the hands of the government entity that disseminates the data.

Subd. 5. [COPYRIGHT OR PATENT OF COMPUTER PROGRAM.] ~~Nothing in~~ Neither this chapter ~~or~~ nor any other statute ~~shall be construed to prevent a state agency, statewide system, or political subdivision~~ prevents a government entity from acquiring a copyright or patent for a computer software program or components of a program created by ~~that~~ the government ~~agency~~ entity. ~~In the event that~~ If a government ~~agency~~ entity does acquire a patent or copyright to a computer software program or component of a program, the data shall be treated as trade secret information pursuant to section 13.37.

Subd. 6. [DISCOVERABILITY OF ~~NOT-PUBLIC~~ PRIVATE OR CONFIDENTIAL DATA.] If a ~~state agency, political subdivision, or statewide system~~ government entity opposes discovery of government data or release of data pursuant to court order on the grounds that the data are classified as ~~not public~~ private or confidential, the party that seeks access to the data may bring before the appropriate presiding judicial officer, arbitrator, or administrative law judge an action to compel discovery or an action in the nature of an action to compel discovery.

The presiding officer shall first decide whether the data are discoverable or releasable pursuant to the rules of evidence and of criminal, civil, or administrative procedure appropriate to the action.

If the data are discoverable the presiding officer shall decide whether the benefit to the party seeking access to the data outweighs any harm to the confidentiality interests of the ~~agency~~ government entity maintaining the data, or of any person who has provided the data or who is the subject of the data, or

to the privacy interest of an individual identified in the data. In making the decision, the presiding officer shall consider whether notice to the subject of the data is warranted and, if warranted, what type of notice must be given. The presiding officer may fashion and issue any protective orders necessary to assure proper handling of the data by the parties. If the data are a videotape of a child victim or alleged victim alleging, explaining, denying, or describing an act of physical or sexual abuse, the presiding officer shall consider the provisions of section 611A.90, subdivision 2, paragraph (b).

Subd. 7. [DATA TRANSFERRED TO ARCHIVES.] When government data that is classified as ~~not public~~ private or confidential by this chapter or any other statute~~, including private data on deceedents and confidential data on deceedents,~~ is physically transferred to the state archives, the data ~~shall~~ are no longer ~~be~~ classified as ~~not public~~ private or confidential and access to and use of the data ~~shall be~~ are governed by section 138.17.

Subd. 8. [CHANGE TO CLASSIFICATION OF DATA NOT ON INDIVIDUALS.] Except for security information, ~~nonpublic~~ private and ~~protected nonpublic~~ confidential data not on individuals ~~shall become~~ becomes public either ten years after the creation of the data by the government ~~agency~~ entity or ten years after the data was received or collected by ~~any governmental agency~~ a government entity unless the responsible authority for the originating or custodial ~~agency~~ government entity for the data reasonably determines that, if the data were made available to the public or to the data subject, the harm to the public or to a data subject would outweigh the benefit to the public or to the data subject. If the responsible authority denies access to the data, the person denied access may challenge the denial by bringing an action in district court seeking release of the data. The action shall be brought in the district court located in the county where the data are being maintained, or, in the case of data maintained by a ~~state agency~~ government entity, in any county. The data in dispute shall be examined by the court in camera. In deciding whether or not to release the data, the

court shall consider the benefits and harms in the same manner as set forth above. The court shall make a written statement of findings in support of its decision.

Subd. 9. [EFFECT OF CHANGES IN CLASSIFICATION OF DATA.] Unless otherwise expressly provided by a particular statute, the classification of data is determined by the law applicable to the data at the time a request for access to the data is made, regardless of the data's classification at the time it was collected, created, or received.

Subd. 10. [COSTS FOR PROVIDING COPIES OF DATA.] Money collected by a responsible authority in a state agency for the actual cost to the agency of providing copies or electronic transmittal of government data is appropriated to the agency and added to the appropriations from which the costs were paid.

Subd. 11. [TREATMENT OF PRIVATE OR CONFIDENTIAL DATA ~~CLASSIFIED AS NOT PUBLIC~~; PUBLIC MEETINGS.] ~~Not-public~~ Private or confidential data may be discussed at a meeting open to the public to the extent provided in section 471.705, subdivision 1d.

Sec. 10. Minnesota Statutes 1998, section 13.04, is amended to read:

13.04 [RIGHTS OF INDIVIDUAL SUBJECTS OF DATA.]

Subdivision 1. [TYPE OF DATA.] The rights of individuals on whom ~~the~~ data is stored or to be stored ~~shall be as~~ are set forth in this section.

Subd. 2. [INFORMATION REQUIRED TO BE GIVEN INDIVIDUAL.] An individual asked to supply private or confidential data concerning the individual shall be informed of: (a) the purpose and intended use of the requested data within the collecting ~~state agency, political subdivision, or statewide system~~ government entity; (b) whether the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from 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. This requirement ~~shall~~ does not apply when an individual is asked to supply investigative data, pursuant to

section 13.82, subdivision 5, to a law enforcement officer.

Subd. 3. [ACCESS TO DATA BY INDIVIDUAL.] Upon request to a responsible authority, an individual shall be informed whether the individual is the subject of stored data on individuals, and whether ~~it~~ the data is classified as public, private or confidential. Upon further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge and, if desired, 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 that individual for six months thereafter unless a dispute or action ~~pursuant to~~ under 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 unable to comply with the request within that time, the responsible authority 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.

Subd. 4. [PROCEDURE WHEN DATA IS NOT ACCURATE OR COMPLETE.] (a) An individual subject of ~~the~~ data may contest the accuracy or completeness of public or private data. 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: (1) 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 (2) notify the individual that the authority believes the data to be correct. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

The determination of the responsible authority may be appealed ~~pursuant to~~ under the provisions of the Administrative Procedure Act relating to contested cases. Upon receipt of an appeal by an individual, the commissioner shall, before issuing the order and notice of a contested case hearing required by chapter 14, try to resolve the dispute through education, conference, conciliation, or persuasion. If the parties consent, the commissioner may refer the matter to mediation. Following these efforts, the commissioner shall dismiss the appeal or issue the order and notice of hearing.

(b) Data on ~~individuals~~ an individual that have been successfully challenged by ~~an~~ the individual must be completed, corrected, or destroyed by a ~~state agency, political subdivision, or statewide system~~ government entity without regard to the requirements of section 138.17.

After completing, correcting, or destroying successfully challenged data, a ~~state agency, political subdivision, or statewide system~~ government entity may retain a copy of the commissioner of administration's order issued under chapter 14 or, if no order ~~were~~ was issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data.

Subd. 5. [EDUCATION RECORDS; CHILD WITH A DISABILITY.] ~~Nothing in this chapter shall be construed as limiting~~ This chapter does not limit the frequency of inspection of the educational records of a child with a disability by the child's parent or guardian or by the child upon the ~~child~~ child's reaching the age of majority. ~~An agency~~ A government entity or institution may not charge a fee to search for or to retrieve the educational records. ~~An agency~~ A government entity or institution that receives a request for copies of the educational records of a child with a disability may charge a

fee that reflects the costs of reproducing the records except when to do so would impair the ability of the child's parent or guardian, or the child who has reached the age of majority, to exercise their right to inspect and review those records.

Sec. 11. Minnesota Statutes 1998, section 13.05, subdivision 1, is amended to read:

13.05 [DUTIES OF RESPONSIBLE AUTHORITY.]

Subdivision 1. [PUBLIC DOCUMENT OF DATA CATEGORIES.] The responsible authority of each government entity shall prepare a public document containing the authority's name, title and address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the ~~authority's state agency, statewide system, or political subdivision~~ government entity. Forms used to collect private and confidential data on individuals shall be included in the public document. ~~Beginning August 1, 1977 and annually thereafter,~~ The responsible authority shall annually update the public document and make any changes necessary to maintain the accuracy of the document. The document shall be available to the public from the responsible authority ~~to the public~~ in accordance with the provisions of sections 13.03 and 15.17.

Sec. 12. Minnesota Statutes 1998, section 13.05, subdivision 4, is amended to read:

Subd. 4. [LIMITATIONS ON COLLECTION AND USE OF DATA.] Private or confidential data on an individual shall not be collected, stored, used, or disseminated by ~~political subdivisions, statewide systems, or state agencies~~ government entities for any purposes other than those stated to the individual at the time of collection in accordance with section 13.04, except as provided in this subdivision.

(a) Data on individuals 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.

(b) Private or confidential data on individuals may be used and disseminated to individuals or ~~agencies~~ government entities specifically authorized access to ~~that~~ the data by state, local, or federal law enacted or promulgated after the collection of the data.

(c) Private or confidential data on individuals may be used and disseminated to individuals or ~~agencies~~ government entities subsequent to the collection of the data ~~when~~ if 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.

(d) Private data on individuals may be used by and disseminated to ~~any~~ a person ~~or agency~~, government entity, or federal 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~~ a statement authorizing ~~any~~ a person or ~~agency~~ government entity to disclose information about the individual 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 the data subject;

(4) specific as to the nature of the information the subject is authorizing to be disclosed;

(5) specific as to the persons or agencies to whom the subject is authorizing information to be disclosed;

(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, the expiration date may be two years after the date of the policy.

The responsible authority may require a person requesting copies of data under this paragraph to pay the actual costs of making, certifying, and compiling the copies.

(e) Private or confidential data on an individual may be discussed at a meeting open to the public to the extent provided in section 471.705, subdivision 1d.

Sec. 13. Minnesota Statutes 1998, section 13.05, subdivision 6, is amended to read:

Subd. 6. [CONTRACTS.] Except as provided in section 13.46, subdivision 5, in any contract between a ~~governmental unit~~ government entity subject to this chapter and any person, when the contract requires that data on individuals be made available to the contracting parties by the ~~governmental unit~~ government entity, that data shall be administered consistent with this chapter. A contracting party shall maintain the data on individuals which it received according to the statutory provisions applicable to the data.

Sec. 14. Minnesota Statutes 1998, section 13.05, subdivision 8, is amended to read:

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~~ under section 13.04 and the specific procedures in effect in the ~~state agency, statewide system or political subdivision~~ government entity for access by the data subject to public or private data on individuals.

Sec. 15. Minnesota Statutes 1998, section 13.05, subdivision 9, is amended to read:

Subd. 9. [INTERGOVERNMENTAL ACCESS OF DATA.] A responsible authority shall allow another responsible authority access to

data classified as ~~not-public~~ private or confidential only when the access is authorized or required by statute or federal law. ~~An agency~~ A government entity that supplies government data under this subdivision may require the requesting ~~agency~~ entity to pay the actual cost of supplying the data.

Sec. 16. Minnesota Statutes 1998, section 13.06, is amended to read:

13.06 [TEMPORARY CLASSIFICATION.]

Subdivision 1. [APPLICATION TO COMMISSIONER.] Notwithstanding the provisions of section 13.03, the responsible authority of a ~~state agency, political subdivision, or statewide system~~ government entity 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 nonpublic or protected nonpublic,~~ for its own use and for the use of other similar ~~agencies, political subdivisions, or statewide systems~~ government entities on a temporary basis 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~~ that 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, rejected, or granted by the commissioner, whichever is earlier.

If the commissioner determines that an application has been submitted for purposes not consistent with this section, the commissioner may immediately reject the application, give notice of that rejection to the applicant, and return the application. When the applicant receives the notice of rejection from the commissioner, the data ~~which~~ that was the subject of the application shall have the classification it had before the application was submitted to the commissioner.

Subd. 2. [CONTENTS OF APPLICATION FOR PRIVATE OR CONFIDENTIAL DATA ON INDIVIDUALS.] An application for temporary classification of data on individuals ~~shall include~~ must state,

and the applicant shall have the burden of clearly establishing, that no statute currently exists which either allows or forbids classification of the data as private or confidential; and ~~either~~

~~(a)~~ (1) 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)~~ (2) 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 individual data subject.

Subd. 3. [CONTENTS OF APPLICATION FOR ~~NONPUBLIC OR NONPUBLIC-PROTECTED~~ DATA NOT ON INDIVIDUALS.] An application for temporary classification of government data not on individuals ~~shall include~~ must state, and the applicant shall have the burden of clearly establishing, that no statute currently exists which either allows or forbids classification as ~~nonpublic~~ private or ~~protected nonpublic~~ confidential; and ~~either~~ that:

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

(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.

Subd. 4. [PROCEDURE WHEN CLASSIFICATION AFFECTS OTHERS.] If the commissioner determines that an application for temporary classification involves data ~~which~~ that would reasonably be classified in the same manner by all ~~agencies, political subdivisions, or statewide systems~~ government entities similar to the one ~~which~~ that made the application, the commissioner may approve or disapprove the classification for data of the kind ~~which~~ that is the subject of the application for the use of

all ~~agencies, political subdivisions, or statewide systems~~ government entities similar to the applicant. On deeming this approach advisable, the commissioner shall provide notice of the proposed action 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,~~ government entity or 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~~ that is the subject of the application, for the use of all ~~agencies, political subdivisions, or statewide systems~~ government entities 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~~ that 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~~ government entities similar to the applicant until the application is disapproved or granted by the commissioner, whichever is earlier. Proceedings after the grant or disapproval shall be governed by the provisions of subdivision 5.

Subd. 5. [DETERMINATION.] The commissioner shall either grant or disapprove the application for temporary classification within 45 days after it is filed. On disapproving an application, the commissioner shall set forth in detail reasons

for the disapproval, and shall include a statement of belief as to what classification is appropriate for the data ~~which~~ that is the subject of the application. Twenty days after the date of the commissioner's disapproval of an application, the data ~~which~~ that is the subject of the application ~~shall become~~ becomes public data, unless the responsible authority submits an amended application for temporary classification which requests the classification deemed appropriate by the commissioner in the 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~~ that 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 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~~ that is the subject of the application ~~shall become~~ becomes 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~~ becomes 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~~ that is the subject of the classification ~~shall become~~ becomes public data five working days after the date of the attorney general's disapproval.

Subd. 7. [LEGISLATIVE CONSIDERATION OF TEMPORARY CLASSIFICATIONS; EXPIRATION.] 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. ~~The~~ A temporary classification expires June 1 of the year following its submission to the legislature.

Sec. 17. Minnesota Statutes 1998, section 13.072, subdivision , is amended to read:

13.072 [OPINIONS BY THE COMMISSIONER.]

Subdivision 1. [OPINION; WHEN REQUIRED.] (a) Upon request of a ~~state agency, statewide system, or political subdivision~~ government entity, the commissioner may give a written opinion on ~~any~~ a question relating to public access to government data, rights of subjects of data, or classification of data under this chapter or other Minnesota statutes governing government data practices. Upon request of ~~any~~ a person who disagrees with a determination regarding data practices made by a ~~state agency, statewide system, or political subdivision~~ government entity, the commissioner may give a written opinion regarding the person's rights as a subject of government data or right to have access to government data. If the commissioner determines that no opinion will be issued, the commissioner shall give the ~~state agency, statewide system, political subdivision,~~ government entity or person requesting the opinion notice of the decision not to issue the opinion within five days of receipt of the request. If this notice is not given, the commissioner shall issue an opinion within 20 days of receipt of the request. For good cause and upon written notice to the person requesting the opinion, the commissioner may extend this deadline for one additional 30-day period. The notice must state the reason for extending the deadline. The ~~state agency, statewide system, or political subdivision~~ government entity must be provided a reasonable opportunity to explain the reasons for its decision regarding the data. The commissioner or the ~~state agency, statewide system, or political subdivision~~ government entity may choose to give notice to the subject of the data concerning the dispute ~~regarding~~ about the data.

(b) This section does not apply to a determination made by the commissioner of health under section 13.38, subdivision 2, paragraph (c), or 144.6581.

(c) A written opinion issued by the attorney general ~~shall take~~ takes precedence over an opinion issued by the commissioner under this section.

Subd. 2. [EFFECT.] Opinions issued by the commissioner under this section are not binding on the ~~state agency, statewide system, or political subdivision~~ government entity whose data is the subject of the opinion, but must be given deference by a court in a proceeding involving the data. The commissioner shall arrange for public dissemination of opinions issued under this section. This section does not preclude a person from bringing any other action under this chapter or other law in addition to or instead of requesting a written opinion. A ~~state agency, statewide system, political subdivision,~~ government entity or person that acts in conformity with a written opinion of the commissioner is not liable for compensatory or exemplary damages or awards of attorneys fees in actions under section 13.08 or for a penalty under section 13.09.

Subd. 4. [DATA SUBMITTED TO COMMISSIONER.] A ~~state agency, statewide system, or political subdivision~~ government entity may submit ~~not public~~ private or confidential data to the commissioner for the purpose of requesting or responding to a person's request for an opinion. Government data submitted to the commissioner by a ~~state agency, statewide system, or political subdivision~~ government entity or copies of government data submitted by other persons have the same classification as the data have when held by the ~~state agency, statewide system, or political subdivision~~ submitting government entity. If the nature of the opinion is such that the release of the opinion would reveal ~~not public~~ private or confidential data, the commissioner may issue an opinion using pseudonyms for individuals. Data maintained by the commissioner, in the record of an opinion issued using pseudonyms that would reveal the identities of individuals protected by the use of the

pseudonyms, are private data on individuals.

Sec. 18. Minnesota Statutes 1998, section 13.073, subdivision 3, is amended to read:

Subd. 3. [BASIC TRAINING.] The basic training component should be designed to meet the basic information policy needs of all government employees and public officials with a focus on key data practices laws and procedures that apply to all government entities. The commissioner should design the basic training component in a manner that minimizes duplication of the effort and cost for government entities to provide basic training. The commissioner may develop general programs and materials for basic training such as video presentations, data practices booklets, and training guides. The commissioner may assist ~~state and local government agencies~~ government entities in developing training expertise ~~within their own agencies~~ and offer assistance for periodic training sessions for this purpose.

Sec. 19. Minnesota Statutes 1998, section 13.073, subdivision 4, is amended to read:

Subd. 4. [SECTOR-SPECIFIC TRAINING.] (a) The sector-specific training component should be designed to provide for the development of specific expertise needed to deal with information policy issues within a particular service area. Service areas may include government entities ~~such as state agencies, counties, cities, or school districts,~~ or functional areas such as education, human services, child protection, or law enforcement. This component should focus on training individuals who implement or administer data practices and other information policy laws within their government entity.

(b) The commissioner may provide technical assistance and support and help coordinate efforts to develop sector-specific training within different sectors. Elements of sector-specific training should include:

(1) designation, training, and coordination of data practices specialists with responsibility for clarification and resolution of sector-specific information policy issues;

(2) development of telephone hot lines within different

sectors for handling information policy inquiries;

(3) development of forums under which individuals with ongoing information policy administrative responsibilities may meet to discuss issues arising within their sectors;

(4) availability of expertise for coaching and consultation on specific issues; and

(5) preparation of publications, including reference guides to materials and resource persons.

Sec. 20. Minnesota Statutes 1998, section 13.08, is amended to read:

13.08 [CIVIL REMEDIES.]

Subdivision 1. [ACTION FOR DAMAGES.] Notwithstanding section 466.03, a ~~political subdivision, responsible authority, statewide system, or state agency which~~ government entity that violates ~~any~~ a provision of this chapter is liable to a person or representative of a decedent who suffers ~~any~~ damage as a result of the violation~~, and~~. The person damaged or a representative of the decedent in the case of private ~~data on deceedents~~ or confidential data on decedents may bring an action against the ~~political subdivision, responsible authority, statewide system or state agency to cover~~ government entity for any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the ~~political subdivision, statewide system or state agency~~ government entity shall, in addition, be liable ~~to~~ for 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 this chapter.

Subd. 2. [INJUNCTION.] A ~~political subdivision, responsible authority, statewide system or state agency which~~ government entity that violates or proposes to violate this chapter 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~~ that violate this chapter.

Subd. 3. [VENUE.] An action filed ~~pursuant to~~ under this

section may be commented in the county ~~in-which~~ where the individual alleging damage or seeking relief resides, or in the county ~~wherein~~ where the political subdivision exists, or, in the case of the state, any county.

Subd. 4. [ACTION TO COMPEL COMPLIANCE.] In addition to the remedies provided in subdivisions 1 to 3 or any other law, ~~any~~ an aggrieved person may bring an action in district court to compel compliance with this chapter and may recover costs and disbursements, 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. In an action involving a request for government data under section 13.03 or 13.04, 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~~ private or confidential.

Subd. 5. [IMMUNITY FROM LIABILITY.] A ~~state-agency, statewide-system, political-subdivision,~~ government entity or a person that releases ~~not-public~~ private or confidential data pursuant to an order under section 13.03, subdivision 6, is immune from civil and criminal liability for the release.

Subd. 6. [IMMUNITY FROM LIABILITY; PERSONNEL SETTLEMENT.] No cause of action ~~may-arise~~ arises as a result of the release of data contained in a termination or personnel settlement agreement if the data were ~~not-public~~ private or confidential data as defined in section 13.02, at the time the agreement was executed but become public data under a law enacted after execution.

Sec. 21. Minnesota Statutes 1998, section 13.10, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION OF DATA ON DECEDENTS.] Upon the death of ~~the~~ a data subject, private data and confidential data ~~shall~~ become, respectively, private data on decedents and

confidential data on decedents. Private data on decedents and confidential data on decedents ~~shall~~ become public when ten years have elapsed from the actual or presumed death of the individual and 30 years have elapsed from the creation of the data. For purposes of this subdivision, an individual is presumed to be dead if either 90 years elapsed since the creation of the data or 90 years have elapsed since the individual's birth, whichever is earlier, except that an individual is not presumed to be dead if readily available data indicate that the individual is still living.

Sec. 22. Minnesota Statutes 1998, section 13.10, subdivision 3, is amended to read:

Subd. 3. [RIGHTS.] Rights conferred by this chapter on individuals who are the subjects of private or confidential data shall, ~~in-the-case-of-private-data-on-decedents-or-confidential-data-on-decedents~~ upon the death of the data subject, be exercised by the representative of the decedent. ~~Nonpublic~~ Private data concerning a decedent, created or collected after death, are accessible by the representative of the decedent. ~~Nothing-in~~ This section ~~may-be-construed-to~~ does not prevent access to appropriate data by a trustee appointed in a wrongful death action.

Sec. 23. Minnesota Statutes 1998, section 13.30, is amended to read:

13.30 [ATTORNEYS.]

Notwithstanding the provisions of this chapter and section 15.17, the use, collection, storage, and dissemination of data by an attorney acting in a professional capacity for the ~~state, a-state-agency-or-a-political-subdivision~~ government entity ~~shall-be~~ are governed by statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility; ~~provided-that~~. However, this section ~~shall-not-be-construed-to~~ does not affect the applicability of any statute, other than this chapter and section 15.17, ~~which~~ that specifically requires or prohibits disclosure of specific information by the attorney,

nor ~~shall~~ does this section ~~be construed to~~ relieve ~~any~~ a responsible authority, other than the attorney, from duties and responsibilities ~~pursuant to~~ under this chapter and section 15.17.

Sec. 24. Minnesota Statutes 1998, section 13.31, is amended to read:

13.31 [BENEFIT DATA.]

Subdivision 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, rehabilitation and community action agency, Head Start, and food assistance programs administered by ~~state agencies, political subdivisions, or statewide systems~~ government entities. Benefit data does not include welfare data, which shall be administered in accordance with section 13.46.

Subd. 2. [PUBLIC DATA.] The names and addresses of applicants for and recipients of benefits, aid, or assistance through programs administered by ~~any political subdivision, state agency, or statewide system~~ a government entity that are intended to assist with the purchase of housing or other real property 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, and shall not be disclosed except ~~pursuant to~~ by court order or to an agent of the ~~state agency, political subdivision, or statewide system~~ government entity, including appropriate law enforcement personnel, ~~who are~~ acting in an investigation or prosecution of a criminal or civil proceeding relating to the administration of a program described in subdivision 1.

Sec. 25. Minnesota Statutes 1998, section 13.32, subdivision 1, is amended to read:

Subdivision 1. [DEFINITIONS.] As used in this section:

(a) "Educational data" means data ~~on individuals~~ that relates to a student and is maintained by a public educational

agency or institution or by a person acting for the agency or institution ~~which relates to a student~~.

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

~~Records~~ Data of a law enforcement unit of a public educational agency or institution ~~which~~ that are maintained apart from ~~education~~ educational data ~~and~~, are maintained solely for law enforcement purposes, and are not disclosed to individuals other than law enforcement officials of the jurisdiction are not educational data; ~~provided, that education records~~ however, education data maintained by the educational agency or institution that are ~~not~~ disclosed to the personnel of the law enforcement unit remain educational data. The University of Minnesota police department is a law enforcement agency for purposes of section 13.82 and other sections of Minnesota Statutes dealing with law enforcement records. Records of organizations providing security services to a public educational agency or institution must be administered consistent with section 13.861.

~~Records relating to~~ Data on a student who is employed by a public educational agency or institution ~~which~~ are classified under section 13.43 if the data 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 13.43~~.

(b) "Juvenile justice system" includes criminal justice agencies and the judiciary when involved in juvenile justice activities.

(c) "Student" means an individual currently or formerly enrolled or registered, applicants for enrollment or registration at a public educational agency or institution, or

individuals who receive shared time educational services from a public agency or institution.

(d) "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 to the position of the maker of the record.

Sec. 26. Minnesota Statutes 1998, section 13.34, is amended to read:

13.34 [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~~ private data not on individuals, except pursuant to court order. Completed versions of personnel, licensing, or academic examinations ~~shall be~~ are 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 13.04, the responsible authority shall not be required to provide copies of completed examinations or answer keys to ~~any~~ an individual who has completed an examination.

Sec. 27. Minnesota Statutes 1998, section 13.35, is amended to read:

13.35 [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~~ the state agency or political subdivision 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~~.

Sec. 28. Minnesota Statutes 1998, section 13.36, is amended to read:

13.36 [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~~ government entities pursuant to sections 624.712 to 624.719 are classified as private~~, pursuant to section 13.02, subdivision 12~~ data on individuals.

Sec. 29. Minnesota Statutes 1998, section 13.37, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION.] The following government data is classified as ~~nonpublic data with regard to data not on individuals, pursuant to section 13.02, subdivision 9, and as~~ private data ~~with regard to data on individuals, pursuant to section 13.02, subdivision 12~~: Security information; trade secret information; sealed absentee ballots prior to opening by an election judge; sealed bids, including the number of bids received, prior to the opening of the bids; internal competitive proposals prior to the time specified by a political subdivision for the receipt of private sector proposals for the services; parking space leasing data; and labor relations information, ~~provided~~ except that specific labor relations information ~~which~~ that relates to a specific labor organization is classified as ~~protected nonpublic~~ confidential data ~~pursuant to section 13.02, subdivision 13~~.

Sec. 30. Minnesota Statutes 1998, section 13.39, is amended to read:

13.39 [CIVIL INVESTIGATION.]

Subdivision 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~~ government entity.

Subd. 2. [CIVIL ACTIONS.] (a) Except as provided in

paragraph (b), data collected by ~~state agencies, political subdivisions, or statewide systems~~ government entities 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~~ confidential data ~~pursuant to section 13.02, subdivision 13, in the case of data not on individuals and confidential pursuant to section 13.02, subdivision 3, in the case of data on individuals. Any agency, political subdivision, or statewide system~~ A government entity may make any data classified as confidential ~~or protected nonpublic~~ pursuant to this subdivision accessible to any person, agency or the public if the ~~agency, political subdivision, or statewide system~~ government entity determines that the access will aid the law enforcement process, promote public health or safety or dispel widespread rumor or unrest.

(b) A complainant has access to a statement provided by the complainant to a ~~state agency, statewide system, or political subdivision~~ government entity under paragraph (a).

Subd. 2a. [DISCLOSURE OF DATA.] During the time when a civil legal action is determined to be pending under subdivision 1, ~~any~~ a person may bring an action in the district court in the county where the data is maintained to obtain disclosure of data classified as confidential ~~or protected nonpublic~~ under subdivision 2. The court may order that all or part of the data be released to the public or to the person bringing the action. In making the determination whether 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, the agency, or any person identified in the data. The data in dispute shall be examined by the court in camera.

Subd. 3. [INACTIVE INVESTIGATIVE DATA.] Inactive civil investigative data are public, unless the release of the data would jeopardize another pending civil legal action, and except for those portions of a civil investigative file that are classified as ~~not public~~ private or confidential data by this

chapter or other law. ~~Any~~ Civil investigative data presented as evidence in court or made part of a court record ~~shall be~~ are public. Civil investigative data become inactive upon the occurrence of any of the following events:

(1) a decision by the ~~state agency, political subdivision, or statewide system~~ government entity or by the chief attorney acting for the ~~state agency, political subdivision, or statewide system~~ government entity not to pursue the civil action;

(2) expiration of the time to file a complaint under the statute of limitations or agreement applicable to the civil action; or

(3) exhaustion of or expiration of rights of appeal by either party to the civil action.

Data determined to be inactive under clause (1) may become active if the ~~state agency, political subdivision, statewide system,~~ government entity or its attorney decides to renew the civil action.

Sec. 31. Minnesota Statutes 1998, section 13.392, subdivision 1, is amended to read:

Subdivision 1. [CONFIDENTIAL DATA ~~OR PROTECTED NONPUBLIC DATA~~.] Data, notes, and preliminary drafts of reports created, collected, and maintained by the internal audit offices of state agencies and political subdivisions, or persons performing audits for state agencies and political subdivisions, and relating to an audit or investigation are confidential data ~~on individuals or protected nonpublic data~~ until the final report has been published or the audit or investigation is no longer being pursued actively, except that the data shall be disclosed as required to comply with section 6.67 or 609.456. This section does not limit in any way:

(1) the state auditor's access to government data of political subdivisions or data, notes, or preliminary drafts of reports of persons performing audits for political subdivisions; or

(2) the public or a data subject's access to data classified by section 13.43.

Sec. 32. Minnesota Statutes 1998, section 13.40, subdivision 1, is amended to read:

Subdivision 1. [RECORDS SUBJECT TO THIS CHAPTER.] (a) For purposes of this section, "historical records repository" means an archives or manuscript repository operated by ~~any state agency, statewide system, or political subdivision~~ a government entity whose purpose is to collect and maintain data to further the history of a geographic or subject area. The term does not include the state archives as defined in section 138.17, subdivision 1, clause (5).

(b) Data collected, maintained, used, or disseminated by a library or historical records repository operated by ~~any state agency, political subdivision, or statewide system~~ a government entity shall be administered in accordance with the provisions of this chapter.

Sec. 33. Minnesota Statutes 1998, section 13.40, subdivision 3, is amended to read:

Subd. 3. [NONGOVERNMENTAL DATA.] Data held in the custody of a historical records repository that were not originally created, received, maintained, or disseminated by a ~~state agency, statewide system, or political subdivision~~ government entity are not government data. These data are accessible to the public unless:

(1) the data are contributed by private persons under an agreement that restricts access, to the extent of any lawful limitation; or

(2) access would significantly endanger the physical or organizational integrity of the data.

Sec. 34. Minnesota Statutes 1998, section 13.41, subdivision 2, is amended to read:

Subd. 2. [PRIVATE DATA; DESIGNATED ADDRESSES AND TELEPHONE NUMBERS.] (a) The following data collected, created or maintained by ~~any~~ a licensing agency are classified as private, ~~pursuant to section 13.02, subdivision 12~~ data on individuals: data, other than their names and designated addresses, submitted by 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 the disclosure; 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~~ a health licensing agency for purposes of review or in anticipation of a 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.

(b) An applicant for a license shall designate on the application a residence or business address and telephone number at which the applicant can be contacted in connection with the license application. A licensee who is subject to a health-related licensing board, as defined in section 214.01, subdivision 2, shall designate a residence or business address and telephone number at which the licensee can be contacted in connection with the license.

Sec. 35. Minnesota Statutes 1998, section 13.41, subdivision 2a, is amended to read:

Subd. 2a. [BOARD OF PEACE OFFICER STANDARDS AND TRAINING.] The following government data of the board of peace officer standards and training are private data:

(1) home addresses of licensees and applicants for licenses; and

(2) data that identify the ~~state agency, statewide system, or political subdivision~~ government entity that employs a licensed peace officer.

The board may disseminate private data on applicants and licensees as ~~is~~ necessary to administer law enforcement licensure or to provide data under section 626.845, subdivision 1, to law enforcement agencies ~~who are~~ conducting employment background investigations.

Sec. 36. Minnesota Statutes 1998, section 13.41, subdivision 3, is amended to read:

Subd. 3. [CONFIDENTIAL DATA.] The following data

collected, created or maintained by ~~any~~ a licensing agency are classified as confidential~~, pursuant to section 13.02, subdivision 3~~: active investigative data relating to the investigation of complaints against ~~any~~ a licensee.

Sec. 37. Minnesota Statutes 1998, section 13.41, subdivision 4, is amended to read:

Subd. 4. [PUBLIC DATA.] Licensing agency minutes, application data on licensees, orders for hearing, findings 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 13.02, subdivision 15~~. The entire record concerning the disciplinary proceeding is public data ~~pursuant to section 13.02, subdivision 15~~, in those instances where there is a public hearing concerning the disciplinary action. If the licensee and the licensing agency agree to resolve a complaint without a hearing, the agreement and the specific reasons for the agreement are public data. The license numbers, the license status, and continuing education records issued or maintained by the board of peace officer standards and training are ~~classified as~~ public data~~, pursuant to section 13.02, subdivision 15~~.

Sec. 38. Minnesota Statutes 1998, section 13.42, subdivision 2, is amended to read:

Subd. 2. [PUBLIC HOSPITALS; DIRECTORY INFORMATION.] (a) During the time that ~~a person~~ an individual is a patient in a hospital operated by a state agency or political subdivision under legal commitment, directory information is public data. After the ~~person~~ individual is released by termination of the ~~person's~~ individual's legal commitment, the directory information is private data on individuals.

(b) If ~~a person~~ an individual is a patient other than pursuant to 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.

~~(c) Directory information about~~ If an emergency patient ~~who~~

is unable to communicate ~~which is public~~ under this subdivision, directory information 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.

Sec. 39. Minnesota Statutes 1998, section 13.43, is amended to read:

13.43 [PERSONNEL DATA.]

Subdivision 1. [DEFINITION.] 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~~ government entity or is a member of or an applicant for a position on an advisory board or commission.

Subd. 2. [PUBLIC DATA.] (a) Except for employees described in subdivision 5, the following personnel data on current and former employees, volunteers, and independent contractors of a ~~state agency, statewide system, or political subdivision~~ government entity and members of advisory boards or commissions is public:

(1) name; actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary;

(2) job title; job description; education and training background; and previous work experience;

(3) date of first and last employment;

(4) the existence and status of ~~any~~ complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action;

(5) the final disposition of any disciplinary action

together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the ~~public body~~ government entity;

(6) the terms of ~~any~~ an agreement settling ~~any~~ a dispute arising out of an employment relationship, including a buyout agreement as defined in section 123B.143, subdivision 2, paragraph (a); except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money;

(7) work location; a work telephone number; badge number; and honors and awards received; ~~and~~

(8) payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other ~~not public~~ private or confidential data; and

(9) city and county of residence.

(b) For purposes of this subdivision, a final disposition occurs when the ~~state agency, statewide system, or political subdivision~~ government entity makes its final decision about the disciplinary action, regardless of the possibility of ~~any~~ later proceedings or court proceedings. In the case of arbitration proceedings arising under collective bargaining agreements, a final disposition occurs at the conclusion of the arbitration proceedings, or upon the failure of the employee to elect arbitration within the time provided by the collective bargaining agreement. Final disposition includes a resignation by an individual when the resignation occurs after the final decision of the ~~state agency, statewide system, political subdivision,~~ government entity or arbitrator.

(c) The ~~state agency, statewide system, or political subdivision~~ government entity may display a photograph of a current or former employee to a prospective witness as part of the ~~state agency's, statewide system's, or political~~

~~subdivision's~~ government entity's investigation of ~~any~~ a complaint or charge against the employee.

(d) A complainant has access to a statement provided by the complainant to a ~~state agency, statewide system, or political subdivision~~ government entity in connection with a complaint or charge against an employee.

(e) Notwithstanding paragraph (a), clause (5), upon completion of an investigation of a complaint or charge against a public official, or if a public official resigns or is terminated from employment while the complaint or charge is pending, all data relating to the complaint or charge are public, unless access to the data would jeopardize an active investigation or reveal confidential sources. For purposes of this paragraph, "public official" means:

(1) the head of a state agency and deputy and assistant state agency heads;

(2) members of boards or commissions required by law to be appointed by the governor or other elective officers; and

(3) executive or administrative heads of departments, bureaus, divisions, or institutions.

Subd. 2a. [DATA DISCLOSURE BY STATEWIDE PENSION PLANS.] Notwithstanding any law to the contrary, with respect to data collected and maintained on members, survivors, and beneficiaries by statewide retirement systems that is classified as public data in accordance with subdivision 2, those retirement systems may be only required to disclose name, gross pension, and type of benefit awarded, except as required by sections 13.03, subdivisions 4 and 6; and 13.05, subdivisions 4 and 9.

Subd. 3. [APPLICANT DATA.] Except for applicants described in subdivision 5, the following personnel data on current and former applicants for employment by a ~~state agency, statewide system or political subdivision~~ government entity or appointment to an advisory board or commission is public: veteran status; relevant test scores; rank on eligible list; job history; education and training; and work availability. Names of

applicants ~~shall be~~ are 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. Names and home addresses of applicants for appointment to and members of an advisory board or commission are public.

Subd. 4. [OTHER DATA.] All other personnel data is private data on individuals but may be released pursuant to a court order.

Subd. 5. [UNDERCOVER LAW ENFORCEMENT OFFICER.] All personnel data maintained by ~~any state agency, statewide system or political subdivision~~ a government entity relating to an individual employed as, or an applicant for employment as, an undercover law enforcement officer are private data on individuals. When the individual is no longer assigned to an undercover position, the data described in subdivisions 2 and 3 become public unless the law enforcement agency determines that revealing the data would threaten the personal safety of the officer or jeopardize an active investigation.

Subd. 6. [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 chapters 179 and 179A. 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 commissioner of the bureau of mediation services.

Subd. 7. [EMPLOYEE ASSISTANCE DATA.] All data created, collected or maintained by ~~any~~ a state agency or political subdivision to administer employee assistance programs similar to the one authorized by section 16B.39, subdivision 2, are classified as private~~, pursuant to section 13.02, subdivision 12~~ data on individuals. This section ~~shall~~ does not ~~be interpreted~~

~~to~~ authorize the establishment of employee assistance programs.

Subd. 8. [HARASSMENT DATA.] When allegations of sexual or other types of harassment are made against an employee, the employee does not have access to data that would identify the complainant or other witnesses if the responsible authority determines that the employee's access to that data would:

(1) threaten the personal safety of the complainant or a witness; or

(2) subject the complainant or witness to harassment.

If a disciplinary proceeding is initiated against the employee, data on the complainant or witness shall be available to the employee as ~~may be~~ necessary for the employee to prepare for the proceeding.

Subd. 9. [PEER COUNSELING DEBRIEFING DATA.] (a) Data acquired by a peer group member in a public safety peer counseling debriefing is private data on the person being debriefed.

(b) For purposes of this subdivision, "public safety peer counseling debriefing" means a group process oriented debriefing session held for peace officers, firefighters, medical emergency persons, dispatchers, or other persons involved with public safety emergency services, that is established by ~~any~~ a agency providing public safety emergency services and is designed to help a person who has suffered an occupation-related traumatic event begin the process of healing and effectively dealing with posttraumatic stress.

Subd. 10. [PROHIBITION ON AGREEMENTS LIMITING DISCLOSURE OR DISCUSSION OF PERSONNEL DATA.] (a) A ~~state agency, statewide system, or political subdivision~~ government entity may not enter into an agreement settling a dispute arising out of the employment relationship with the purpose or effect of limiting access to or disclosure of personnel data or limiting the discussion of information or opinions related to personnel data. An agreement or portion of an agreement that violates this paragraph is void and unenforceable.

(b) Paragraph (a) applies to the following, but only to the

extent that the data or information could otherwise be made accessible to the public:

(1) an agreement not to discuss, publicize, or comment on personnel data or information;

(2) an agreement that limits the ability of the subject of personnel data to release or consent to the release of data; or

(3) any other provision of an agreement that has the effect of limiting the disclosure or discussion of information that could otherwise be made accessible to the public, except a provision that limits the ability of an employee to release or discuss private data that identifies other employees.

(c) Paragraph (a) also applies to a court order that contains terms or conditions prohibited by paragraph (a).

Subd. 11. [PROTECTION OF EMPLOYEE OR OTHERS.] (a) If the responsible authority or designee of a ~~state agency, statewide system, or political subdivision~~ government entity reasonably determines that the release of personnel data is necessary to protect an employee from harm to self or to protect ~~another~~ a person who may be harmed by the employee, data that are relevant to the concerns for safety may be released as provided in this subdivision.

(b) The data may be released:

(1) to the person who may be harmed and to an attorney representing the person when the data are relevant to obtaining a restraining order;

(2) to a prepetition screening team conducting an investigation of the employee under section 253B.07, subdivision 1; or

(3) to a court, law enforcement agency, or prosecuting authority.

(c) Section 13.03, subdivision 4, paragraph (c), applies to data released under this subdivision, except to the extent that the data have a more restrictive classification in the possession of the agency or authority that receives the data. If the person who may be harmed or the person's attorney receives data under this subdivision, the data may be used or

released further only to the extent necessary to protect the person from harm.

Subd. 12. [SHARING OF LAW ENFORCEMENT PERSONNEL BACKGROUND INVESTIGATION DATA.] A law enforcement agency shall share data from a background investigation done under section 626.87 with the peace officer standards and training board or with a law enforcement agency doing an investigation of the subject of the data under section 626.87.

Sec. 40. Minnesota Statutes 1998, section 13.44, is amended to read:

13.44 [PROPERTY COMPLAINT DATA.]

The identities of individuals who register complaints with state agencies or political subdivisions concerning violations of state laws or local ordinances concerning the use of real property are classified as confidential data~~,-pursuant-to section-13.02,-subdivision-3~~ on individuals.

Sec. 41. Minnesota Statutes 1998, section 13.45, is amended to read:

13.45 [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, and which is maintained by ~~state agencies,-political-subdivisions-or-statewide-systems~~ are government entities is classified as ~~nonpublic-pursuant-to section-13.02,-subdivision-9~~ private data not on individuals.

Sec. 42. Minnesota Statutes 1998, section 13.46, subdivision 2, is amended to read:

Subd. 2. [GENERAL.] (a) 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:

(1) according to section 13.05;

(2) according to court order;

(3) according to a statute specifically authorizing access

to the private data;

(4) to an agent of the welfare system, including a law enforcement person, attorney, or investigator acting for it in the investigation or prosecution of a criminal or civil proceeding relating to the administration of a program;

(5) 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;

(6) to administer federal funds or programs;

(7) between personnel of the welfare system working in the same program;

(8) the amounts of cash public assistance and relief paid to welfare recipients in this state, including their names, social security numbers, income, addresses, and other data as required, upon request by the department of revenue to administer the property tax refund law, supplemental housing allowance, early refund of refundable tax credits, and the income tax. "Refundable tax credits" means the dependent care credit under section 290.067, the Minnesota working family credit under section 290.0671, the property tax refund under section 290A.04, and, if the required federal waiver or waivers are granted, the federal earned income tax credit under section 32 of the Internal Revenue Code;

(9) between the department of human services and the Minnesota department of economic security for the purpose of monitoring the eligibility of the data subject for reemployment insurance, for any employment or training program administered, supervised, or certified by that agency, for the purpose of administering any rehabilitation program, whether alone or in conjunction with the welfare system, or to monitor and evaluate the statewide Minnesota family investment program by exchanging data on recipients and former recipients of food stamps, cash assistance under chapter 256, 256D, 256J, or 256K, child care assistance under chapter 119B, or medical programs under chapter 256B, 256D, or 256L;

(10) to appropriate parties in connection with an emergency

if knowledge of the information is necessary to protect the health or safety of the individual or other individuals or persons;

(11) data maintained by residential programs as defined in section 245A.02 may be disclosed to the protection and advocacy system established in this state according to Part C of Public Law Number 98-527 to protect the legal and human rights of persons with mental retardation or other related conditions who live in residential facilities for these persons if the protection and advocacy system receives a complaint by or on behalf of that person and the person does not have a legal guardian or the state or a designee of the state is the legal guardian of the person;

(12) to the county medical examiner or the county coroner for identifying or locating relatives or friends of a deceased person;

(13) data on a child support obligor who makes payments to the public agency may be disclosed to the higher education services office to the extent necessary to determine eligibility under section 136A.121, subdivision 2, clause (5);

(14) participant social security numbers and names collected by the telephone assistance program may be disclosed to the department of revenue to conduct an electronic data match with the property tax refund database to determine eligibility under section 237.70, subdivision 4a;

(15) the current address of a recipient of aid to families with dependent children or Minnesota family investment program-statewide may be disclosed to law enforcement officers who provide the name of the recipient and notify the agency that:

(i) the recipient:

(A) is a fugitive felon fleeing to avoid prosecution, or custody or confinement after conviction, for a crime or attempt to commit a crime that is a felony under the laws of the jurisdiction from which the individual is fleeing; or

(B) is violating a condition of probation or parole imposed under state or federal law;

(ii) the location or apprehension of the felon is within the law enforcement officer's official duties; and

(iii) the request is made in writing and in the proper exercise of those duties;

(16) the current address of a recipient of general assistance or general assistance medical care may be disclosed to probation officers and corrections agents who are supervising the recipient and to law enforcement officers who are investigating the recipient in connection with a felony level offense;

(17) information obtained from food stamp applicant or recipient households may be disclosed to local, state, or federal law enforcement officials, upon their written request, for the purpose of investigating an alleged violation of the Food Stamp Act, according to Code of Federal Regulations, title 7, section 272.1(c);

(18) the address, social security number, and, if available, photograph of any member of a household receiving food stamps shall be made available, on request, to a local, state, or federal law enforcement officer if the officer furnishes the agency with the name of the member and notifies the agency that:

(i) the member:

(A) is fleeing to avoid prosecution, or custody or confinement after conviction, for a crime or attempt to commit a crime that is a felony in the jurisdiction the member is fleeing;

(B) is violating a condition of probation or parole imposed under state or federal law; or

(C) has information that is necessary for the officer to conduct an official duty related to conduct described in subitem (A) or (B);

(ii) locating or apprehending the member is within the officer's official duties; and

(iii) the request is made in writing and in the proper exercise of the officer's official duty;

(19) certain information regarding child support obligors who are in arrears may be made public according to section 518.575;

(20) data on child support payments made by a child support obligor and data on the distribution of those payments excluding identifying information on obligees may be disclosed to all obligees to whom the obligor owes support, and data on the enforcement actions undertaken by the public authority, the status of those actions, and data on the income of the obligor or obligee may be disclosed to the other party;

(21) data in the work reporting system may be disclosed under section 256.998, subdivision 7;

(22) to the department of children, families, and learning for the purpose of matching department of children, families, and learning student data with public assistance data to determine students eligible for free and reduced price meals, meal supplements, and free milk according to United States Code, title 42, sections 1758, 1761, 1766, 1766a, 1772, and 1773; to produce accurate numbers of students receiving aid to families with dependent children or Minnesota family investment program-statewide as required by section 126C.06; to allocate federal and state funds that are distributed based on income of the student's family; and to verify receipt of energy assistance for the telephone assistance plan;

(23) the current address and telephone number of program recipients and emergency contacts may be released to the commissioner of health or a local board of health as defined in section 145A.02, subdivision 2, when the commissioner or local board of health has reason to believe that a program recipient is a disease case, carrier, suspect case, or at risk of illness, and the data are necessary to locate the person;

(24) to other state agencies, statewide systems, and political subdivisions of this state, including the attorney general, and agencies of other states, interstate information networks, federal agencies, and other entities as required by federal regulation or law for the administration of the child

support enforcement program;

(25) to personnel of public assistance programs as defined in section 256.741, for access to the child support system database for the purpose of administration, including monitoring and evaluation of those public assistance programs; or

(26) to monitor and evaluate the statewide Minnesota family investment program by exchanging data between the departments of human services and children, families, and learning, on recipients and former recipients of food stamps, cash assistance under chapter 256, 256D, 256J, or 256K, child care assistance under chapter 119B, or medical programs under chapter 256B, 256D, or 256L.

(b) Information on persons who have been treated for drug or alcohol abuse may only be disclosed according to the requirements of Code of Federal Regulations, title 42, sections 2.1 to 2.67.

(c) Data provided to law enforcement agencies under paragraph (a), clause (15), (16), (17), or (18), or paragraph (b), are investigative data and are confidential ~~or protected nonpublic~~ while the investigation is active. The data are private after the investigation becomes inactive under section 13.82, subdivision 5, paragraph (a) or (b).

(d) Mental health data shall be treated as provided in subdivisions 7, 8, and 9, but is not subject to the access provisions of subdivision 10, paragraph (b).

Sec. 43. Minnesota Statutes 1998, section 13.46, subdivision 3, is amended to read:

Subd. 3. [INVESTIGATIVE DATA.] Data on persons, including data on vendors of services and data on licensees, that 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 data ~~on individuals pursuant to section 13.02, subdivision 3, or protected nonpublic data not on individuals pursuant to section 13.02, subdivision 13~~, and shall not be disclosed except:

(a) pursuant to section 13.05;

(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; or

(d) to provide notices required or permitted by statute.

The data referred to in this subdivision ~~shall be classified as~~ becomes public data upon its submission to an administrative law judge or court in an administrative or judicial proceeding. Inactive welfare investigative data shall be treated as provided in section 13.39, subdivision 3.

Sec. 44. Minnesota Statutes 1998, section 13.46, subdivision 4, is amended to read:

Subd. 4. [LICENSING DATA.] (a) As used in this subdivision:

(1) "licensing data" means all data collected, maintained, used, or disseminated by the welfare system pertaining to persons licensed or registered or who apply for licensure or registration or who formerly were licensed or registered under the authority of the commissioner of human services;

(2) "client" means a person who is receiving services from a licensee or from an applicant for licensure; and

(3) "personal and personal financial data" means social security numbers, identity of and letters of reference, insurance information, reports from the bureau of criminal apprehension, health examination reports, and social/home studies.

(b) Except as provided in paragraph (c), the following data on current and former licensees are public: name, address, telephone number of licensees, licensed capacity, type of client preferred, variances granted, type of dwelling, name and relationship of other family members, previous license history, class of license, and the existence and status of complaints. When disciplinary action has been taken against a licensee or the complaint is resolved, the following data are public: the substance of the complaint, the findings of the investigation of the complaint, the record of informal resolution of a licensing violation, orders of hearing, findings of fact, conclusions of law, and specifications of the final disciplinary action

contained in the record of disciplinary action.

The following data on persons subject to disqualification under section 245A.04 in connection with a license to provide family day care for children, child care center services, foster care for children in the provider's home, or foster care or day care services for adults in the provider's home, are public: the nature of any disqualification set aside under section 245A.04, subdivision 3b, and the reasons for setting aside the disqualification; and the reasons for granting any variance under section 245A.04, subdivision 9.

(c) The following are private data ~~on individuals under section 13.02, subdivision 12, or nonpublic data under section 13.02, subdivision 9~~: personal and personal financial data on family day care program and family foster care program applicants and licensees and their family members who provide services under the license.

(d) The following are private data on individuals: the identity of persons who have made reports concerning licensees or applicants that appear in inactive investigative data, and the records of clients or employees of the licensee or applicant for licensure whose records are received by the licensing agency for purposes of review or in anticipation of a contested matter. The names of reporters under sections 626.556 and 626.557 may be disclosed only as provided in section 626.556, subdivision 11, or 626.557, subdivision 12b.

(e) Data classified as private, or confidential, ~~nonpublic, or protected nonpublic~~ under this subdivision become public data if submitted to a court or administrative law judge as part of a disciplinary proceeding in which there is a public hearing concerning the disciplinary action.

(f) Data generated in the course of licensing investigations that relate to an alleged violation of law are investigative data under subdivision 3.

(g) Data that are ~~not public~~ private or confidential data collected, maintained, used, or disseminated under this subdivision and that relate to or are derived from a report as

defined in section 626.556, subdivision 2, are subject to the destruction provisions of section 626.556, subdivision 11.

Sec. 45. Minnesota Statutes 1998, section 13.46, subdivision 8, is amended to read:

Subd. 8. [ACCESS FOR AUDITING.] To the extent required by state or federal law for the purpose of auditing, representatives of federal, state, or local agencies shall have access to data maintained by public or private community mental health centers, mental health divisions of counties, and other providers under contract to deliver mental health services ~~which is necessary to achieve the purpose of auditing~~. Public or private community mental health centers, mental health divisions of counties, and other providers under contract to deliver mental health services shall not permit this data to identify any particular patient or client by name or contain any other unique personal identifier, except data provided to the legislative auditor. Notwithstanding any statute or rule to the contrary, and solely for the purposes of conducting an audit approved by the legislative audit commission in 1988, the legislative auditor shall be given access to all data, records, and files classified as ~~not public~~ private or confidential. The legislative auditor shall maintain all data collected under this subdivision in accordance with chapter 13 and may not disclose data that identify a patient or client by name or that contain any other personal identifier.

Sec. 46. Minnesota Statutes 1998, section 13.46, subdivision 10, is amended to read:

Subd. 10. [RESPONSIBLE AUTHORITY.] (a) Notwithstanding any other provision of this chapter to the contrary, the responsible authority for each component of the welfare system listed in subdivision 1, clause (c), ~~shall be~~ is as follows:

(1) the responsible authority for the department of human services, state hospitals, and nursing homes is the commissioner of the department of human services;

(2) the responsible authority of a county welfare agency is the director of the county welfare agency;

(3) the responsible authority for a local social services agency, human services board, or community mental health center board is the chair of the board;

(4) the responsible authority of any person, agency, institution, organization, or other entity under contract to any of the components of the welfare system listed in subdivision 1, clause (c), is the person specified in the contract; and

(5) the responsible authority of the public authority for child support enforcement is the head of the public authority for child support enforcement.

(b) A responsible authority shall allow another responsible authority in the welfare system access to data classified as ~~not public~~ private or confidential data when access is necessary for the administration and management of programs, or as authorized or required by statute or federal law.

Sec. 47. Minnesota Statutes 1998, section 13.46, subdivision 11, is amended to read:

Subd. 11. [NURSING HOME APPRAISALS.] Names, addresses, and other data that could identify nursing homes selected as part of a random sample to be appraised by the department of human services in its rate setting process are classified as ~~protected nonpublic~~ confidential data not on individuals until the sample has been completed.

Sec. 48. Minnesota Statutes 1998, section 13.48, is amended to read:

13.48 [AWARD DATA.]

Financial data on business entities submitted to a ~~state agency, statewide system, or political subdivision~~ government entity for the purpose of presenting awards to business entities for achievements in business development or performance are private data ~~on individuals or nonpublic data~~.

Sec. 49. Minnesota Statutes 1998, section 13.50 , is amended to read:

13.50 [APPRAISAL DATA.]

Subdivision 1. [CONFIDENTIAL ~~OR PROTECTED NONPUBLIC~~ DATA.] Estimated or appraised values of individual parcels of real

property which are made by personnel of the state, its agencies and departments, or a political subdivision or by independent appraisers acting for the state, its agencies and departments, or a political subdivision for the purpose of selling or acquiring land through purchase or condemnation are classified as confidential data ~~on individuals or protected nonpublic data~~.

Subd. 2. [PUBLIC DATA.] The data made confidential ~~or protected nonpublic~~ by the provisions of subdivision 1 shall become public upon the occurrence of any of the following:

(a) The negotiating parties exchange appraisals;

(b) The data are submitted to a court appointed condemnation commissioner;

(c) The data are presented in court in condemnation proceedings; or

(d) The negotiating parties enter into an agreement for the purchase and sale of the property.

Sec. 50. Minnesota Statutes 1998, section 13.51, is amended to read:

13.51 [ASSESSOR'S DATA.]

Subdivision 1. [GENERALLY.] The following data collected, created and maintained by political subdivisions are classified as private~~, pursuant to section 13.02, subdivision 12, 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 individuals or business entities concerning income properties are classified as private ~~or nonpublic~~ data ~~pursuant to section 13.02, subdivisions 9 and 12~~:

(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;

(d) anticipated income and expenses for the current year;

(e) projected vacancy factor for the current year; and

(f) lease information.

Subd. 3. [DATA ON INCOME OF INDIVIDUALS.] Income information on individuals collected and maintained by political subdivisions to determine eligibility of property for classification 4c under section 273.13, subdivision 25, paragraph (c), is private data on individuals ~~as defined in section 13.02, subdivision 12~~.

Sec. 51. Minnesota Statutes 1998, section 13.511, is amended to read:

13.511 [LODGING TAX DATA.]

Data, other than basic taxpayer identification data, collected from taxpayers under a lodging tax ordinance are ~~nonpublic~~ private.

Sec. 52. Minnesota Statutes 1998, section 13.52, is amended to read:

13.52 [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 13.02, subdivision 12~~ on individuals.

13.521 [TRANSPORTATION SERVICE DATA.]

Personal, medical, financial, familial, or locational information data pertaining to applicants for or users of services providing transportation for the disabled or elderly, with the exception of the name of the applicant or user of the service, are private data on individuals.

Sec. 53. Minnesota Statutes 1998, section 13.53, is amended to read:

13.53 [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 13.02, subdivision 3~~ on individuals: names of persons interviewed; foster care placement plans obtained from other public and private agencies; and all information gathered during interviews with study participants.

Sec. 54. Minnesota Statutes 1998, section 13.531, is amended to read:

13.531 [FARM ASSISTANCE DATA.]

The following data collected and maintained by counties that provide assistance to individual farmers who are experiencing economic or emotional distress are classified as private data on individuals: financial history, including listings of assets and debts, and personal and emotional status information.

Sec. 55. Minnesota Statutes 1998, section 13.54, subdivision 2, is amended to read:

Subd. 2. [CONFIDENTIAL DATA.] (a) The following data on individuals maintained by the housing agency are classified as confidential data~~, pursuant to section 13.02, subdivision 3~~: 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.

(b) The following data not on individuals maintained by the housing agency are classified as confidential: 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 bodies or agencies for possible prosecution for fraud and commencement of

actions against independent contractors of the agency.

Sec. 56. Minnesota Statutes 1998, section 13.54, subdivision 4, is amended to read:

Subd. 4. [~~NONPUBLIC~~ PRIVATE DATA.] (a) The following data not on individuals maintained by the housing agency are classified as ~~nonpublic data, pursuant to section 13.02, subdivision 9~~ private: 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.

(b) Income information on individuals collected and maintained by a housing agency to determine eligibility of property for classification 4c under section 273.13, subdivision 25, paragraph (c), is private data on individuals. The data may be disclosed to the county and local assessors responsible for determining eligibility of the property for classification 4c.

Sec. 57. Minnesota Statutes 1998, section 13.55, subdivision 1, is amended to read:

Subdivision 1. [~~NOT-PUBLIC-CLASSIFICATION~~ PRIVATE DATA.] The following data received, created, or maintained by or for publicly owned and operated convention facilities, civic center authorities, or the metropolitan sports facilities commission are classified as ~~nonpublic~~ private data ~~pursuant to section 13.02, subdivision 9, or private data on individuals pursuant to section 13.02, subdivision 12~~:

(a) a letter or other documentation from any person who makes inquiry to or who is contacted by the facility regarding the availability of the facility for staging events;

(b) identity of firms and corporations which contact the facility;

(c) type of event which they wish to stage in the facility;

(d) suggested terms of rentals; and

(e) responses of authority staff to these inquiries.

Sec. 58. Minnesota Statutes 1998, section 13.55, subdivision 2, is amended to read:

Subd. 2. [PUBLIC DATA.] The data made ~~not-public~~ private by the provisions of subdivision 1 ~~shall~~ become public upon the occurrence of any of the following:

(a) five years elapse from the date on which the lease or contract is entered into between the facility and the inquiring party or parties or the event which was the subject of inquiry occurs at the facility, whichever occurs earlier;

(b) the event which was the subject of inquiry does not occur; or

(c) the event which was the subject of inquiry occurs elsewhere.

Sec. 59. Minnesota Statutes 1998, section 13.551, is amended to read:

13.551 [PORT AUTHORITY DATA.]

Subdivision 1. [SAINT PAUL PORT AUTHORITY.] The following data not on individuals collected and maintained by the Saint Paul port authority are classified as ~~protected nonpublic~~ confidential, until 30 days before the date of a hearing on a proposed sale pursuant to section 469.065: financial studies and reports that are part of appraisers' estimates of value of or concerning projects as defined in chapter 474, prepared by personnel of the port authority or independent accountants, consultants, and appraisers for the purpose of marketing by sale or lease a project which the port authority has acquired or repossessed as the result of the default under and the termination of a revenue agreement as defined in chapter 474.

Subd. 2. [RED WING PORT AUTHORITY.] Data maintained by the Red Wing port authority that pertain to negotiations with property owners regarding the purchase of property are ~~nonpublic~~ confidential data not on individuals. With the exception of the authority's evaluation of properties not purchased, all other negotiation data become public at the time of the closing of the property sale.

Sec. 60. Minnesota Statutes 1998, section 13.57, is amended to read:

13.57 [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-13.02,-subdivision-12~~ data on individuals: the name, address, telephone number, any other data that identifies the individual, and any 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.

Sec. 61. Minnesota Statutes 1998, section 13.59, is amended to read:

13.59 [REDEVELOPMENT DATA.]

Subdivision 1. [PRIVATE DATA.] The following data collected in surveys of individuals conducted by cities and housing and redevelopment authorities for the purposes of planning, development, and redevelopment, are classified as private data ~~pursuant-to-section-13.02,-subdivision-12~~ on individuals: the names and addresses of individuals and the legal descriptions of property owned by individuals.

Subd. 2. [NONPUBLIC DATA.] The following data collected in surveys of businesses conducted by cities and housing and redevelopment authorities, for the purposes of planning, development, and redevelopment, are classified as ~~nonpublic~~ private data ~~pursuant-to-section-13.02,-subdivision-9~~ not on individuals: the names, addresses, and legal descriptions of business properties and the commercial use of the property to the extent disclosure of the use would identify a particular business.

Sec. 62. Minnesota Statutes 1998, section 13.61, is amended to read:

13.61 [INSURANCE TRUST DATA; PRIVATE AND NONPUBLIC DATA.]

The following data collected or created by the league of Minnesota cities insurance trust, association of Minnesota counties insurance trust, or by the Minnesota school board

association insurance trust in order to process claims for workers' compensation are classified as ~~either~~ private data ~~in regard to claims when the insured worker is living, or nonpublic data in regard to claims when the insured worker is deceased~~ on individuals or on decedents: name, address, phone number, and social security account number of the claimant if the claimant is not a public employee; claim number, date of claimed injury, employee's social security number, home phone number, home address, date of birth, sex, and marital status; whether claimed injury caused loss of time from work; whether the employee lost time from work on the day of the claimed injury and the number of hours lost; whether the employee has returned to work; whether full or partial wages were paid for the first day of lost time and the amount paid, time of day, and location where injury occurred; whether the injury occurred on employer's premises; the name, address, and phone number of the treating physician or practitioner; identification of the hospital where treated; nature of the claimed injury or occupational illness; part of body affected; name or type of object involved in causing the injury; nature of injury; type of accident; description of actions taken to prevent recurrence; names of coworker witnesses; and all data collected or created as a result of the investigation of the claim including, but not limited to, physicians' reports; other data on the medical condition of the claimant; data collected from the claimant's physicians; and data collected in interviews of the claimant's employer, coworkers, family members, and neighbors.

Sec. 63. Minnesota Statutes 1998, section 13.62, is amended to read:

13.62 [ECONOMIC ASSISTANCE DATA.]

The following data collected by cities in their administration of the city economic development assistance program are classified as ~~nonpublic~~ private data not on individuals:

(1) application data, except company names, addresses, and other data that identify the applicant, until the application is

approved by the city;

(2) application data, except company names, addresses, and other data that identify the applicant, that pertain to companies whose applications have been disapproved;

(3) attachments to applications including but, not limited to, business and personal financial records, until the application is approved;

(4) income tax returns, either personal or corporate, that are filed by applicants; and

(5) correspondence between the program administrators and the applicant until the application has been approved or disapproved.

Sec. 64. Minnesota Statutes 1998, section 13.621, is amended to read:

13.621 [TWO HARBORS DEVELOPMENT COMMISSION DATA.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] The following data ~~that are~~ submitted to the Two Harbors development commission by businesses that are requesting financial assistance are ~~nonpublic~~ private data not on individuals: financial statements, business plans, income and expense projections, customer lists, balance sheets, net worth calculations, and market data, including feasibility studies not paid for with public funds.

Subd. 2. [PUBLIC DATA.] Data submitted to the commission under subdivision 1 become public data if the commission provides financial assistance to the business except that the following data remain ~~nonpublic~~ private data not on individuals: business plans, income and expense projections, customer lists, and market data, including feasibility studies not paid for with public funds.

Sec. 65. Minnesota Statutes 1998, section 13.622, is amended to read:

13.622 [MOORHEAD ECONOMIC DEVELOPMENT AUTHORITY DATA.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] The following data submitted to the city of Moorhead and to the Moorhead economic development authority by businesses that are requesting

financial assistance are ~~nonpublic~~ private data not on individuals: financial statements, business plans, income and expense projections, customer lists, balance sheets, and market and feasibility studies not paid for with public funds.

Subd. 2. [PUBLIC DATA.] Data submitted to the city and the city's economic development authority under subdivision 1 become public data if the city provides financial assistance to the business except that the following data remain ~~nonpublic~~ private data not on individuals: business plans, income and expense projections, customer lists, and market and feasibility studies not paid for with public funds.

Sec. 66. Minnesota Statutes 1998, section 13.64, is amended to read:

13.64 [DEPARTMENT OF ADMINISTRATION DATA.]

Notes and preliminary drafts of reports created, collected, or maintained by the management analysis division, department of administration, and prepared during management studies, audits, reviews, consultations, or investigations are classified as confidential ~~or protected nonpublic~~ data until the final report has been published or preparation of the report is no longer being actively pursued. Data that support the conclusions of the report and that the commissioner of administration reasonably believes will result in litigation are confidential ~~or protected nonpublic~~ until the litigation has been completed or until the litigation is no longer being actively pursued. Data on individuals that could reasonably be used to determine the identity of an individual supplying data for a report are private if (a) the data supplied by the individual were needed for a report and (b) the data would not have been provided to the management analysis division without an assurance to the individual that the individual's identity would remain private.

Sec. 67. Minnesota Statutes 1998, section 13.643, subdivision 1, is amended to read:

Subdivision 1. [LOAN AND GRANT APPLICANT DATA.] The following data on applicants, collected by the department of agriculture in its sustainable agriculture revolving loan and

grant programs under sections 17.115 and 17.116, are private ~~or nonpublic~~: nonfarm income; credit history; insurance coverage; machinery and equipment list; financial information; and credit information requests.

Sec. 68. Minnesota Statutes 1998, section 13.645, is amended to read:

13.645 [AQUACULTURE PERMIT DATA.]

The following data collected and maintained by an agency issuing aquaculture permits under sections 17.47 to 17.498 are classified as private ~~or nonpublic~~: the names and addresses of customers provided in the permit application.

Sec. 69. Minnesota Statutes 1998, section 13.646, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATIONS.] Legislative and budget proposals, including preliminary drafts, that are created, collected, or maintained by the state administration are ~~protected nonpublic~~ confidential data not on individuals. After the budget is presented to the legislature by the state administration, supporting data, including agency requests, are public data. Supporting data do not include preliminary drafts. The state administration may disclose any of the data within the state administration and to the public at any time if disclosure would aid the administration in considering and preparing its proposals.

Sec. 70. Minnesota Statutes 1998, section 13.65, subdivision 2, is amended to read:

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 13.02, subdivision 3~~ data on individuals: 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.

Sec. 71. Minnesota Statutes 1998, section 13.65, subdivision 3, is amended to read:

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 13.02, subdivision 15~~.

Sec. 72. Minnesota Statutes 1998, section 13.66, is amended to read:

13.66 [CORRECTIONS OMBUDSMAN DATA.]

Subdivision 1. [PRIVATE DATA.] The following data maintained by the ombudsman for corrections are classified as private~~, pursuant to section 13.02, subdivision 12~~ data on individuals:

(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~~ individuals 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 13.02, subdivision 3~~ data on individuals: the written summary of the investigation to the extent it identifies individuals.

Subd. 3. [PUBLIC DATA.] The following data maintained by the ombudsman are ~~classified as~~ public~~, pursuant to section 13.02, subdivision 15~~: client name, client location~~,~~ and the inmate identification number assigned by the department of corrections.

Sec. 73. Minnesota Statutes 1998, section 13.67, is amended to read:

13.67 [EMPLOYEE RELATIONS DATA.]

The following data collected, created, or maintained by the department of employee relations are classified as ~~nonpublic~~ private data ~~pursuant to section 13.02, subdivision 9~~ not on individuals:

(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;

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

(d) The managerial plan prepared by the department pursuant to section 43A.18 that governs the compensation and terms and conditions of employment for employees in managerial positions, as specified in section 43A.18, subdivision 3, until the plan is submitted to the legislative commission on employee relations; and

(e) Claims experience and all related information received from carriers and claims administrators participating in either the state group insurance plan, the Minnesota employee insurance program, the state workers' compensation program, or the public employees insurance program as defined in chapter 43A, and survey information collected from employees and employers participating in these plans and programs, except when the department determines that release of the data will not be detrimental to the plan or program.

Sec. 74. Minnesota Statutes 1998, section 13.671, is amended to read:

13.671 [IRON RANGE RESOURCES AND REHABILITATION BOARD DATA.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] The following data that are submitted to the commissioner of the iron range resources and rehabilitation board by businesses that are requesting financial assistance are ~~nonpublic~~ private data not on individuals: the identity of the business and financial information about the business including, but not limited to,

credit reports, financial statements, net worth calculations, business plans, income and expense projections, customer lists, and market and feasibility studies not paid for with public funds.

Subd. 2. [PUBLIC DATA.] Data submitted to the commissioner under subdivision 1 become public data upon submission of the request for financial assistance to the iron range resources and rehabilitation board except that the following data remain ~~nonpublic~~ private data not on individuals: business plans, income and expense projections, customer lists, and market and feasibility studies not paid for with public funds.

Sec. 75. Minnesota Statutes 1998, section 13.68, is amended to read:

13.68 [ENERGY AND FINANCIAL DATA AND STATISTICS.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] Energy and financial data, statistics, and information furnished to the commissioner of public service development by a coal supplier or petroleum supplier, or information on individual business customers of a public utility pursuant to section 216C.16 or 216C.17, either directly or through a federal department or agency are classified as ~~nonpublic~~ private data ~~as defined by section 13.02, subdivision 9~~ not on individuals.

Subd. 2. [ENERGY AUDIT DATA.] Data contained in copies of bids, contracts, letters of agreement between utility companies and third party auditors and firms, and in utility statements or documents showing costs for employee performance of energy audits which are received by the commissioner of public service in order to arbitrate disputes arising from complaints concerning the award of contracts to perform energy conservation audits are classified as ~~protected nonpublic~~ confidential data not on individuals ~~as defined by section 13.02, subdivision 13~~.

Sec. 76. Minnesota Statutes 1998, section 13.69, subdivision 1, is amended to read:

Subdivision 1. [CLASSIFICATIONS.] (a) The following government data of the department of public safety are private data on individuals:

(1) medical data on driving instructors, licensed drivers, and applicants for parking certificates and special license plates issued to physically handicapped persons;

(2) other data on holders of a disability certificate under section 169.345, except that data that are not medical data may be released to law enforcement agencies;

(3) social security numbers in driver's license and motor vehicle registration records, except that social security numbers must be provided to the department of revenue for purposes of tax administration and the department of labor and industry for purposes of workers' compensation administration and enforcement; and

(4) data on persons listed as designated caregivers under section 171.07, subdivision 11, except that the data must be released to:

(i) law enforcement agencies for the purpose of verifying that an individual is a designated caregiver; or

(ii) law enforcement agencies who state that the license holder is unable to communicate at that time and that the information is necessary for notifying the designated caregiver of the need to care for a child of the license holder.

(b) The following government data of the department of public safety are confidential data on individuals: data concerning an individual's driving ability when ~~that~~ the data ~~is~~ are received from a member of the individual's family.

Sec. 77. Minnesota Statutes 1998, section 13.71, is amended to read:

13.71 [DEPARTMENT OF COMMERCE DATA.]

Subdivision 1. [SURPLUS LINE INSURANCE DATA.] All data appearing on copies of surplus line insurance policies collected by the department of commerce pursuant to sections 60A.195 to 60A.209 are classified as private data on individuals.

Subd. 2. [GROUP WORKERS' COMPENSATION SELF-INSURANCE DATA.] Financial data relating to nonpublic companies that are submitted to the commissioner of commerce for the purpose of obtaining approval to self-insure workers' compensation

liability as a group are classified as ~~nonpublic~~ private data not on individuals.

Subd. 3. [WORKERS' COMPENSATION SELF-INSURANCE DATA.] Financial documents, including income statements, balance sheets, statements of changes in financial positions, and supporting financial information, submitted by nonpublic companies seeking to self-insure their workers' compensation liability or to be licensed as self-insurance plan administrators are classified as ~~nonpublic~~ private data not on individuals.

Subd. 4. [POLLUTION LIABILITY INSURANCE SURVEY DATA.] Data that could identify a company that responded to a pollution liability insurance survey taken by the department of commerce are classified as ~~nonpublic~~ private data not on individuals.

Subd. 5. [DATA ON INSURANCE COMPANIES AND TOWNSHIP MUTUAL COMPANIES.] The following data collected and maintained by the department of commerce are classified as ~~nonpublic~~ private data not on individuals:

(a) that portion of any of the following data which would identify the affected insurance company or township mutual company: (1) any order issued pursuant to section 60A.031, subdivision 5, or 67A.241, subdivision 4, and based in whole or in part upon a determination or allegation by the commerce department or commissioner that an insurance company or township mutual company is in an unsound, impaired, or potentially unsound or impaired condition; or (2) any stipulation, consent agreement, letter agreement, or similar document evidencing the settlement of any proceeding commenced pursuant to an order of a type described in clause (1), or an agreement between the department and an insurance company or township mutual company entered in lieu of the issuance of an order of the type described in clause (1);

(b) any correspondence or attachments relating to the data listed in this subdivision.

Subd. 6. [COMPREHENSIVE HEALTH INSURANCE DATA.] The following data on eligible ~~persons~~ individuals and enrollees of

the state comprehensive health insurance plan are classified as private: all data collected or maintained by the Minnesota comprehensive health association, the writing carrier, and the department of commerce.

The Minnesota comprehensive health association is considered a state agency for purposes of this chapter.

The Minnesota comprehensive health association may disclose data on eligible ~~persons~~ individuals and enrollees of the state comprehensive health insurance plan to conduct actuarial and research studies, notwithstanding the classification of this data, if:

(1) the board authorizes the disclosure;

(2) no individual may be identified in the actuarial or research report;

(3) materials allowing an individual to be identified are returned or destroyed as soon as they are no longer needed; and

(4) the actuarial or research organization agrees not to disclose the information unless the disclosure would be permitted under this chapter if made by the association.

Subd. 7. [CLASSIFICATION OF PPO AGREEMENT DATA.] Data described in section 62E.13, subdivision 11, are ~~nonpublic~~ private data not on individuals.

Subd. 8. [RELEASE OF COMPLAINT TO RESPONDENT.] The commissioner may provide a copy of a complaint to the subject of the complaint when the commissioner determines that the access is necessary in order to effectively conduct the investigation.

Sec. 78. Minnesota Statutes 1998, section 13.72, is amended to read:

13.72 [TRANSPORTATION DEPARTMENT DATA.]

Subdivision 1. [ESTIMATES FOR CONSTRUCTION PROJECTS.] An estimate of the cost of a construction project of the Minnesota department of transportation prepared by department employees is ~~nonpublic~~ private data not on individuals and is not available to the public from the time of final design until the project is awarded.

Subd. 2. [RIDESHARE DATA.] The following data on

participants, collected by the department of transportation for the purpose of administering the rideshare program, are classified as private ~~pursuant to section 13.02, subdivision 12~~ data on individuals: residential address and phone number; beginning and ending work hours; current mode of commuting to and from work; and type of rideshare service information requested.

Subd. 4. [MOTOR CARRIER ACCIDENT DATA.] All data submitted to the department of transportation in the form of motor vehicle carrier accident reports, except the portions of the report forms in which the carrier and the driver provide their version of the accident, are classified as ~~nonpublic data with regard to data not on individuals, and private data with regard to data on individuals~~ private data.

Subd. 5. [MOTOR CARRIER ACCIDENT VERSION DATA.] Those portions of the motor vehicle carrier accident report forms, that motor vehicle carriers are required to submit to the department of transportation, that contain the carrier's and driver's version of the accident are classified as ~~protected nonpublic data with regard to data not on individuals, and~~ confidential data ~~with regard to data on individuals~~.

Subd. 6. [COMPLAINT DATA.] Names of complainants, complaint letters, and other unsolicited data furnished to the department of transportation by a person other than the data subject or department employee, which provide information that a person who is subject to chapter 221 or rules adopted under that chapter may not be in compliance with those requirements, are classified as confidential data ~~or protected nonpublic data~~.

Subd. 7. [PUBLIC INVESTIGATIVE DATA.] The following data created, collected, or maintained about persons subject to chapter 221 and rules adopted under that chapter are public: data contained in inspection and compliance forms and data contained in audit reports that are not prepared under contract to the federal highway administration.

Subd. 8. [MOTOR CARRIER OPERATING DATA.] The following data submitted by Minnesota intrastate motor carriers to the

department of transportation are ~~nonpublic~~ private data: all payroll reports including wages, hours or miles worked, hours earned, employee benefit data, and terminal and route-specific operating data including percentage of revenues paid to agent operated terminals, line-haul load factors, pickup and delivery (PUD) activity, and peddle driver activity.

Sec. 79. Minnesota Statutes 1998, section 13.74, is amended to read:

13.74 [ENVIRONMENTAL QUALITY DATA.]

The following data collected and maintained by the environmental quality board are classified as private data ~~pursuant to section 13.02, subdivision 12~~: the names and addresses of individuals who submitted information and letters concerning personal health problems associated with transmission lines.

Sec. 80. Minnesota Statutes 1998, section 13.75, is amended to read:

13.75 [BUREAU OF MEDIATION SERVICES DATA.]

Subdivision 1. [REPRESENTATION DATA.] Authorization signatures or cards furnished in support of a petition filed or election conducted under sections 179.16, 179.18 to 179.25, and 179A.12, and all ballots, prior to the time of tabulation, are classified as ~~protected nonpublic~~ confidential data ~~with regard to data not on individuals pursuant to section 13.02, subdivision 13, and as confidential data on individuals with regard to data on individuals pursuant to section 13.02, subdivision 3~~.

Subd. 2. [MEDIATION DATA.] All data received or maintained by the commissioner or staff of the bureau of mediation services during the course of providing mediation services to the parties to a labor dispute under the provisions of chapter 179 are classified as ~~protected nonpublic~~ confidential data ~~with regard to data not on individuals, pursuant to section 13.02, subdivision 13, and as confidential data on individuals pursuant to section 13.02, subdivision 3~~, except to the extent the commissioner of the bureau of mediation services determines such

data are necessary to fulfill the requirements of section 179A.16, or to identify the general nature of or parties to a labor dispute.

Sec. 81. Minnesota Statutes 1998, section 13.76, subdivision 1, is amended to read:

13.76 [DEPARTMENT OF TRADE AND ECONOMIC DEVELOPMENT DATA.]

Subdivision 1. [DEVELOPMENT LOAN DATA.] All financial information on individuals and business entities including, but not limited to, credit reports, financial statements, and net worth calculations, that are contained in an application received by the department of trade and economic development in its administration of the certified state development loan program are classified as private data ~~with-regard-to-data-on individuals,-and-as-nonpublic-data-with-regard-to-data-not-on individuals~~ until the application is approved.

Sec. 82. Minnesota Statutes 1998, section 13.76, subdivision 2, is amended to read:

Subd. 2. [FINANCIAL INCENTIVE DATA.] Data collected by the department of trade and economic development relating to financial incentives offered by private businesses and organizations, other than state government, to companies for locating their proposed business operations in Minnesota are classified as ~~nonpublic~~ private data not on individuals.

Sec. 83. Minnesota Statutes 1998, section 13.761, is amended to read:

13.761 [INDIAN AFFAIRS COUNCIL DATA.]

All financial information on individuals and business entities including, but not limited to, credit reports, financial statements, and net worth calculations, that are contained in applications received by the Indian affairs council in its administration of the Indian business development loan program are classified as private data ~~with-regard-to-data-on individuals-and-as-nonpublic-data-with-regard-to-data-not-on individuals~~.

Sec. 84. Minnesota Statutes 1998, section 13.77, subdivision 1, is amended to read:

13.77 [AGRICULTURAL RESOURCE LOAN BOARD DATA.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] Financial information concerning individuals or business persons received or prepared by the agriculture resource loan guaranty board in connection with applications for loan guarantees pursuant to Laws 1984, chapter 502, article 10, sections 1 to 12, including, but not limited to, credit reports, financial statements, and net worth calculations, is classified as ~~nonpublic~~ private data.

Sec. 85. Minnesota Statutes 1998, section 13.78, is amended to read:

13.78 [MINNESOTA EXPORT AUTHORITY DATA.]

Financial information concerning individuals or business persons received or prepared by the export authority in connection with applications for financial assistance pursuant to section 116J.9673, including, but not limited to, credit reports, financial statements, net worth calculations, income and expense projections, and proposed terms of trade and foreign risk coverage, is classified as ~~nonpublic data if it is data not on an individual and as~~ private data ~~if it is data on an individual~~.

Sec. 86. Minnesota Statutes 1998, section 13.79, is amended to read:

13.79 [DEPARTMENT OF LABOR AND INDUSTRY DATA.]

Data that identify complaining employees and that appear on complaint forms received by the department of labor and industry concerning alleged violations of the Fair Labor Standards Act, section 181.75 or 181.9641 are classified as private data on individuals.

Sec. 87. Minnesota Statutes 1998, section 13.793, is amended to read:

13.793 [NATURAL RESOURCES MINERAL DATA.]

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA.] Except as provided in subdivision 2, the following data received and maintained by the commissioner of natural resources are ~~nonpublic~~ private data not on individuals:

(1) a letter or other documentation from a person that is

supplied to the commissioner before a public lease sale of metallic or other minerals for the purpose of making suggestions or recommendations about which state lands may be offered for public lease sale;

(2) a written report or other documentation of private analyses of a state-owned or controlled drill core that is public data and is under the custody of the commissioner; or

(3) exploration data received by the commissioner under the terms of a state mineral lease.

Subd. 2. [DATA BECOME PUBLIC.] (a) Data under subdivision 1, clause (1), become public data three years after the date the lease sale was held or, if not held, within three years after the date the lease sale was scheduled to be held. Except as provided in paragraph (b), data under subdivision 1, clause (2), become public data one year after receipt by the commissioner. Except as provided in paragraph (c) or as otherwise provided for by law, data under subdivision 1, clause (3), become public data upon termination of the state mineral lease under which the data were gathered.

(b) If data under subdivision 1, clause (2), relate to private land that is under mineral lease to the person submitting the data, and the mineral lease is in force at the time the data are submitted, the data become public data only after the mineral lease is no longer in force. The person submitting the data that relate to private land that is under mineral lease shall provide to the commissioner at the time the data are submitted and annually thereafter, in a format designated by the commissioner, satisfactory evidence that the mineral lease is in effect. If, in a given year, satisfactory evidence that the mineral lease is still in effect is not provided to the commissioner before the anniversary date of receipt of the data by the commissioner, the data immediately become public data.

(c) If data under subdivision 1, clause (3), are ~~nonpublic~~ private data not on individuals under the provisions of section 103I.605, subdivision 4, clause (c), the data become public data

pursuant to the provisions of section 103I.605, subdivision 4, clauses (c) and (d).

Sec. 88. Minnesota Statutes 1998, section 13.80, is amended to read:

13.80 [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 13.02, subdivision 3,~~ until a temporary court order made pursuant to subdivision 5 or 7 of section 518B.01 is executed or served upon the data subject who is the respondent to the action.

Sec. 89. Minnesota Statutes 1998, section 13.82, subdivision 5, is amended to read:

Subd. 5. [CRIMINAL INVESTIGATIVE DATA.] Except for the data defined in subdivisions 2, 3, and 4, investigative data 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 other offense for which the agency has primary investigative responsibility is confidential ~~or protected nonpublic~~ 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 10. Photographs ~~which~~ that are part of inactive investigative files and ~~which~~ that are clearly offensive to common sensibilities are classified as private ~~or nonpublic~~ data, ~~provided~~ except 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 30

years after the commission of the offense, whichever comes earliest; or

(c) exhaustion of or expiration of all rights of appeal by a person 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) may become active if the agency or appropriate prosecutorial authority decides to renew the investigation.

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.

Sec. 90. Minnesota Statutes 1998, section 13.82, subdivision 5b, is amended to read:

Subd. 5b. [INACTIVE CHILD ABUSE DATA.] Investigative data that become inactive under subdivision 5, clause (a) or (b), and that relate to the alleged abuse or neglect of a child by a person responsible for the child's care, as defined in section 626.556, subdivision 2, are private data on individuals.

Sec. 91. Minnesota Statutes 1998, section 13.82, subdivision 5d, is amended to read:

Subd. 5d. [INACTIVE VULNERABLE ADULT MALTREATMENT DATA.] Investigative data that ~~becomes~~ become inactive under subdivision 5, paragraph (a) or (b), and that relate to the alleged maltreatment of a vulnerable adult by a caregiver or facility are private data on individuals.

Sec. 92. Minnesota Statutes 1998, section 13.82, subdivision 5e, is amended to read:

Subd. 5e. [NAME CHANGE DATA.] Data ~~on~~ in court records relating to name changes under section 259.10, subdivision 2, which is held by a law enforcement agency is confidential data on an individual while an investigation is active and is private data on an individual when the investigation becomes inactive.

Sec. 93. Minnesota Statutes 1998, section 13.82, subdivision 8, is amended to read:

Subd. 8. [PUBLIC BENEFIT DATA.] ~~Any~~ A law enforcement agency may make ~~any~~ data classified as confidential ~~or protected nonpublic 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.

Sec. 94. Minnesota Statutes 1998, section 13.82, subdivision 12, is amended to read:

Subd. 12. [DATA IN ARREST WARRANT INDICES.] Data in arrest warrant indices are classified as confidential data on individuals 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.

Sec. 95. Minnesota Statutes 1998, section 13.82, subdivision 13, is amended to read:

Subd. 13. [PROPERTY DATA.] Data that uniquely describe stolen, lost, confiscated, or recovered property are classified as ~~either~~ private data ~~on individuals or nonpublic data depending on the content of the not public data~~.

Sec. 96. Minnesota Statutes 1998, section 13.82, subdivision 14, is amended to read:

Subd. 14. [REWARD PROGRAM DATA.] 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 that pays rewards to informants are ~~protected nonpublic data in the case of data not on individuals or~~ confidential data ~~in the case of data on individuals~~.

Sec. 97. Minnesota Statutes 1998, section 13.82, subdivision 15, is amended to read:

Subd. 15. [EXCHANGES OF INFORMATION.] ~~Nothing in~~ This chapter ~~prohibits~~ does not prohibit the exchange of information other than private or confidential personnel data by law enforcement agencies ~~provided~~ if the exchanged information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation~~, except not public personnel data~~.

Sec. 98. Minnesota Statutes 1998, section 13.82, subdivision 16, is amended to read:

Subd. 16. [DELIBERATIVE PROCESSES.] Data that reflect deliberative processes or investigative techniques of law enforcement agencies are confidential data ~~on individuals or protected nonpublic data~~; ~~provided~~ except that information, reports, or memoranda that have been adopted as the final opinion or justification for a decision of a law enforcement agency are public data.

Sec. 99. Minnesota Statutes 1998, section 13.83, subdivision 4, is amended to read:

Subd. 4. [INVESTIGATIVE DATA.] Data created or collected by a county coroner or medical examiner which is part of an active investigation mandated by chapter 390, or any other general or local law relating to coroners or medical examiners is confidential data ~~or protected nonpublic data~~, until the completion of the coroner's or medical examiner's final summary of findings, but may be disclosed to a state or federal agency charged by law with investigating the death of the deceased individual about whom the medical examiner or coroner has medical examiner data. Upon completion of the coroner's or medical examiner's final summary of findings, the data collected in the investigation and the final summary of it are private ~~or nonpublic~~ data. However, if the final summary and the death certificate indicate the manner of death is homicide, undetermined, or pending investigation and there is an active law enforcement investigation, within the meaning of section

13.82, subdivision 5, relating to the death of the deceased individual, the data remain confidential ~~or protected nonpublic~~. Upon review by the county attorney of the jurisdiction in which the law enforcement investigation is active, the data may be released to persons described in subdivision 8 if the county attorney determines release would not impede the ongoing investigation. When the law enforcement investigation becomes inactive, the data are private ~~or nonpublic data~~. ~~Nothing in~~ This subdivision ~~shall be construed~~ ~~to~~ does not make ~~not public~~ private or confidential the data elements identified in subdivision 2 at any point in the investigation or thereafter.

Sec. 100. Minnesota Statutes 1998, section 13.83, subdivision 7, is amended to read:

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 ~~nonpublic, protected nonpublic,~~ 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.

Sec. 101. Minnesota Statutes 1998, section 13.83, subdivision 8, is amended to read:

Subd. 8. [ACCESS TO ~~NONPUBLIC~~ PRIVATE DATA.] The data made ~~nonpublic~~ private by this section are accessible to the physician who attended the decedent at the time of death, the legal representative of the decedent's estate and to the decedent's surviving spouse, parents, children, and siblings and their legal representatives.

Sec. 102. Minnesota Statutes 1998, section 13.83, subdivision 9, is amended to read:

Subd. 9. [CHANGE IN CLASSIFICATION.] Data classified as

~~nonpublic,-protected-nonpublic,~~ private or confidential by this section ~~shall-be-classified-as~~ becomes public 30 years after the date of death of the decedent.

Sec. 103. Minnesota Statutes 1998, section 13.84, subdivision 2, is amended to read:

Subd. 2. [GENERAL.] Unless the data is summary data or a statute, including sections 609.115 and 257.70, specifically provides a different classification, the following court services data are classified as private ~~pursuant-to-section 13.02,-subdivision-12~~ data on individuals:

(a) Court services data on individuals gathered at the request of a municipal, district or county court to determine the need for any treatment, rehabilitation, counseling, or any other need of a defendant, parolee, probationer, or participant in a diversion program, and used by the court to assist in assigning an appropriate sentence or other disposition in a case;

(b) Court services data on petitioners or respondents to a family court gathered at the request of the court for purposes of, but not limited to, individual, family, marriage, chemical dependency and marriage dissolution adjustment counseling, including recommendations to the court as to the custody of minor children in marriage dissolution cases;

(c) Court services data on individuals gathered by psychologists in the course of providing the court or its staff with psychological evaluations or in the course of counseling individual clients referred by the court for the purpose of assisting them with personal conflicts or difficulties.

Sec. 104. Minnesota Statutes 1998, section 13.84, subdivision 3, is amended to read;

Subd. 3. [THIRD PARTY INFORMATION.] Whenever, in the course of gathering the private data specified above, a psychologist, probation officer or other agent of the court is directed by the court to obtain data on individual defendants, parolees, probationers, or petitioners or respondents in a family court, and the source of that data provides the data only

upon the condition of its being held confidential, that data and the identity of the source shall be confidential data on individuals~~,-pursuant-to-section-13.02,-subdivision-3~~.

Sec. 105. Minnesota Statutes 1998, section 13.85, subdivision 2, is amended to read:

Subd. 2. [PRIVATE DATA.] Unless the data are summary data or arrest data, or a statute specifically provides a different classification, corrections and detention data on individuals are classified as private ~~pursuant-to-section-13.02,-subdivision-2~~ data on individuals, to the extent that the release of the data would either (a) disclose medical, psychological, or financial information, or personal information not related to their lawful confinement or detainment or (b) endanger an individual's life.

Sec. 106. Minnesota Statutes 1998, section 13.85, subdivision 3, is amended to read:

Subd. 3. [CONFIDENTIAL DATA.] Corrections and detention data are confidential data on individuals, ~~pursuant-to-section-13.02,-subdivision-3,~~ to the extent that release of the data would: (a) endanger an individual's life, (b) endanger the effectiveness of an investigation authorized by statute and relating to the enforcement of rules or law, (c) identify a confidential informant, or (d) clearly endanger the security of any institution or its population.

Sec. 107. Minnesota Statutes 1998, section 13.86, subdivision 2, is amended to read:

Subd. 2. [GENERAL.] Investigative detention data is confidential data on individuals and shall not be disclosed except:

(a) Pursuant to section 13.05 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.

Sec. 108. Minnesota Statutes 1998, section 13.87, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION.] Criminal history data maintained by ~~agencies, political subdivisions and statewide systems~~ government entities are classified as private~~, pursuant to section 13.02, subdivision 12~~ data on individuals, except that data created, collected, or maintained by the bureau of criminal apprehension that identify an individual who was convicted of a crime and the offense of which the individual was convicted are public data for 15 years following the discharge of the sentence imposed for the offense.

The bureau of criminal apprehension shall provide to the public at the central office of the bureau the ability to inspect in person, at no charge, through a computer monitor the criminal conviction data ~~classified as~~ accessible to the public under this subdivision.

Sec. 109. Minnesota Statutes 1998, section 13.88, is amended to read:

13.88 [COMMUNITY DISPUTE RESOLUTION CENTER DATA.]

The guidelines shall provide that all files relating to a case in a community dispute resolution program are to be classified as private data on individuals~~, pursuant to section 13.02, subdivision 12~~, with the following exceptions:

(1) When a party to the case has been formally charged with a criminal offense, the data are ~~to be classified as~~ public data on individuals~~, pursuant to section 13.02, subdivision 15~~.

(2) Data relating to suspected neglect or physical or sexual abuse of children or maltreatment of vulnerable adults are ~~to be~~ subject to the reporting requirements of sections 626.556 and 626.557.

Sec. 110. Minnesota Statutes 1998, section 16A.672, subdivision 11, is amended to read:

Subd. 11. [REGISTRATION NOT PUBLIC INFORMATION.] Information in any register of ownership of bonds or certificates is ~~nonpublic data under section 13.02, subdivision 9, or~~ private data ~~on individuals~~ under section 13.02, subdivision 12. The information is open only to the subject of it, except as disclosure:

(1) is necessary for the registrar, the commissioner, the treasurer, or the legislative auditor to perform a duty; or

(2) is requested by an authorized representative of the state commissioner of revenue, the state attorney general, or the United States commissioner of internal revenue to determine the application of a tax; or

(3) is required under section 13.03, subdivision 4.

Sec. 111. Minnesota Statutes 1998, section 16D.06, subdivision 2, is amended to read:

Subd. 2. [DISCLOSURE OF DATA.] Data received, collected, created, or maintained by the commissioner or the attorney general to collect debts are classified as private data ~~on individuals~~ under section 13.02, subdivision 12, ~~or nonpublic data under section 13.02, subdivision~~ 9. The commissioner or the attorney general may disclose ~~not public~~ data that is not public:

(1) under section 13.05;

(2) under court order;

(3) under a statute specifically authorizing access to the not public data;

(4) to provide notices required or permitted by statute;

(5) to an agent of the commissioner or the attorney general, including a law enforcement person, attorney, or investigator acting for the commissioner or the attorney general in the investigation or prosecution of a criminal or civil proceeding relating to collection of a debt;

(6) to report names of debtors, amount of debt, date of debt, and the agency to whom debt is owed to credit bureaus;

(7) to locate the debtor, locate the assets of the debtor, or to enforce or implement the collection of a debt, provided that the commissioner or the attorney general may disclose only the data that are necessary to enforce or implement collection of the debt; and

(8) to the commissioner of revenue for tax administration purposes.

The commissioner and the attorney general may not disclose

data that is not public to a private collection agency or other entity with whom the commissioner has contracted under section 16D.04, subdivision 4, unless disclosure is otherwise authorized by law.

Sec. 112. Minnesota Statutes 1998, section 17.117, subdivision 12, is amended to read:

Subd. 12. [DATA PRIVACY.] The following data on applicants or borrowers collected by the commissioner under this section are private ~~for~~ data ~~on individuals~~ as provided in section 13.02, subdivision 12~~, or nonpublic for data not on individuals as provided in section 13.02, subdivision 9~~: financial information, including, but not limited to, credit reports, financial statements, tax returns and net worth calculations received or prepared by the commissioner.

Sec. 113. Minnesota Statutes 1998, section 17.498, is amended to read:

17.498 [RULES; FINANCIAL ASSURANCE.]

(a) The commissioner of the pollution control agency, after consultation and cooperation with the commissioners of agriculture and natural resources, shall present proposed rules to the pollution control agency board prescribing water quality permit requirements for aquaculture facilities by May 1, 1992. The rules must consider:

(1) best available proven technology, best management practices, and water treatment practices that prevent and minimize degradation of waters of the state considering economic factors, availability, technical feasibility, effectiveness, and environmental impacts;

(2) classes, types, sizes, and categories of aquaculture facilities;

(3) temporary reversible impacts versus long-term impacts on water quality;

(4) effects on drinking water supplies that cause adverse human health concerns; and

(5) aquaculture therapeutics, which shall be regulated by the pollution control agency.

(b) Net pen aquaculture and other aquaculture facilities with similar effects must submit an annual report to the commissioner of the pollution control agency analyzing changes in water quality trends from previous years, documentation of best management practices, documentation of costs to restore the waters used for aquaculture to the trophic state existing before aquatic farming was initiated, and documentation of financial assurance in an amount adequate to pay for restoration costs. The trophic state, which is the productivity of the waters measured by total phosphorus, dissolved oxygen, algae abundance as chlorophyll-a, and secchi disk depth of light penetration, and the condition of the waters measured by raw drinking water parameters, shall be determined to the extent possible before aquatic farming is initiated. The financial assurance may be a trust fund, letter of credit, escrow account, surety bond, or other financial assurance payable to the commissioner for restoration of the waters if the permittee cannot or will not restore the waters after termination of aquatic farming operations or revocation of the permit.

(c) The commissioner of the pollution control agency shall submit a draft of the proposed rules to the legislative water commission by September 1, 1991. By January 15, 1992, the commissioner of the pollution control agency shall submit a report to the legislative water commission about aquaculture facilities permitted by the pollution control agency. The report must include concerns of permittees as well as concerns of the agency about permitted aquaculture facilities and how those concerns will be addressed in the proposed rules.

(d) Information received as part of a permit application or as otherwise requested must be classified according to chapter 13. Information about processes, aquatic farming procedures, feed and therapeutic formulas and rates, and tests on aquatic farming products that have economic value is ~~nonpublic data~~ trade secret information under ~~chapter 13~~ section 13.37, subdivision 1, if requested by the applicant or permittee.

Sec. 114. Minnesota Statutes 1998, section 17.694,

subdivision 1, is amended to read:

Subdivision 1. [PROCEDURES.] Any association accredited under this section may engage in bargaining as provided for under sections 17.691 to 17.703.

(1) An association desiring accreditation shall file with the commissioner in the form required by the commissioner. The request shall contain properly certified evidence that the association meets the standards for accreditation and shall be accompanied by a report of the names and addresses of member producers, the name of each handler to whom the member producer delivered or contracted to deliver the agricultural commodity during the previous two calendar years. A fee to cover the costs of the commissioner in processing the request shall be established pursuant to chapter 14, and paid by the association when the request is filed.

(2) The commissioner shall notify all handlers named in the request for accreditation of an association of producers. The notice must be sent to the handlers named in the request by first class mail within ten days of the commissioner receiving the request for accreditation. The commissioner shall maintain records indicating the date of mailing.

(3) The commissioner may require all handlers of an agricultural commodity produced in a bargaining unit area as individuals to file within 30 days following a request, a report, properly certified, showing the correct names and addresses of all producers of the agricultural commodity who have delivered the agricultural commodity to the handler during the two calendar years preceding the filing of the report.

(4) Data submitted to the commissioner by producer associations under clause (1) and by commodity handlers under clause (3) are private data ~~on individuals or nonpublic data~~, as defined in section 13.02, subdivision 9 ~~or~~ 12.

Sec. 115. Minnesota Statutes 1998, section 27.04, subdivision 2, is amended to read:

Subd. 2. [APPLICATION CONTENTS.] (a) The application must be in writing, accompanied by the prescribed fee, and state:

(1) the place or places where the applicant intends to carry on the business for which the license is desired;

(2) the estimated amount of business to be done monthly;

(3) the amount of business done during the preceding year, if any;

(4) the full names of the persons constituting the firm for a partnership, and for a corporation the names of the officers of the corporation and where incorporated;

(5) a financial statement showing the value and character of the assets and the amount of liabilities of the applicant;

(6) the income and expenses for the most recent year;

(7) the names and addresses of all shareholders who own at least five percent of a corporate applicant's shares of stock;

(8) whether the applicant or any of its officers, partners, or agents have been involved in any litigation relating to the business of a wholesale produce dealer in the previous five years; and

(9) any other information relevant to the conduct of its business as a wholesale produce dealer in the previous five years, as the commissioner may require.

(b) If a contract is used in a transaction, a copy of the contract must also be filed with the commissioner.

(c) Financial data required of an applicant under this section is classified as private data ~~with-regard-to-data-on individuals-and-as-nonpublic-data-with-regard-to-data-not-on individuals~~ under section 13.02, subdivision 12.

Sec. 116. Minnesota Statutes 1998, section 32.71, subdivision 2, is amended to read:

Subd. 2. [DATA PRIVACY.] Financial and production information received by the commissioner on processors, wholesalers, or retailers including, but not limited to, financial statements, fee reports, price schedules, cost documentation, books, papers, records, or other documentation for the purpose of administration and enforcement of this chapter shall be classified as private data ~~or-nonpublic-data pursuant-to-chapter-13~~ as defined in section 13.02, subdivision

12. That classification shall not limit the use of the information in the preparation, institution, or conduct of a legal proceeding by the commissioner in enforcing this chapter.

Sec. 117. Minnesota Statutes 1998, section 41B.211, subdivision 2, is amended to read:

Subd. 2. [DATA NOT ON INDIVIDUALS.] The following data submitted to the authority by businesses that are requesting financial assistance are ~~nonpublic~~ data as defined in section 13.02, subdivision 12: financial information about the applicant, including credit reports, financial statements, net worth calculations, business plans, income and expense projections, customer lists, market and feasibility studies not paid for with public funds, tax returns, and financial reports provided to the authority after closing of the financial assistance.

Sec. 118. Minnesota Statutes 1998, section 44A.08, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION OF DATA.] For purposes of this subdivision, "business transaction" means a transaction between parties other than the board. The following data received or developed by the board is private ~~with respect to data on individuals and nonpublic with respect to data not on individuals~~ as defined in section 13.02, subdivision 12:

(1) Data relating to the financial condition of individuals or businesses receiving or performing services by or on behalf of the board.

(2) At the request of either party to the transaction data on business transactions.

(3) At the request of the person or business seeking the information, the identities of persons or businesses requesting business or trade information from the board, and the nature of the trade information.

Sec. 119. Minnesota Statutes 1998, section 45.012, is amended to read:

45.012 [COMMISSIONER.]

(a) The department of commerce is under the supervision and

control of the commissioner of commerce. The commissioner is appointed by the governor in the manner provided by section 15.06.

(b) Data that is received by the commissioner or the commissioner's designee by virtue of membership or participation in an association, group, or organization that is not otherwise subject to chapter 13 is confidential ~~or protected nonpublic~~ data as defined in section 13.02, subdivision 3, but may be shared with the department employees as the commissioner considers appropriate. The commissioner may release the data to any person, agency, or the public if the commissioner determines that the access will aid the law enforcement process, promote public health or safety, or dispel widespread rumor or unrest.

(c) It is part of the department's mission that within the department's resources the commissioner shall endeavor to:

(1) prevent the waste or unnecessary spending of public money;

(2) use innovative fiscal and human resource practices to manage the state's resources and operate the department as efficiently as possible;

(3) coordinate the department's activities wherever appropriate with the activities of other governmental agencies;

(4) use technology where appropriate to increase agency productivity, improve customer service, increase public access to information about government, and increase public participation in the business of government;

(5) utilize constructive and cooperative labor-management practices to the extent otherwise required by chapters 43A and 179A;

(6) report to the legislature on the performance of agency operations and the accomplishment of agency goals in the agency's biennial budget according to section 16A.10, subdivision 1; and

(7) recommend to the legislature appropriate changes in law necessary to carry out the mission and improve the performance of the department.

Sec. 120. Minnesota Statutes 1998, section 46.041, subdivision 1, is amended to read:

Subdivision 1. [FILING; FEE; PUBLIC INSPECTION.] The incorporators of a bank proposed to be organized under the laws of this state shall execute and acknowledge a written application in the form prescribed by the commissioner of commerce. The application must be signed by two or more of the incorporators and request a certificate authorizing the proposed bank to transact business at the place and in the name stated in the application. The applicant shall file the application with the department with a $1,000 filing fee and a $500 investigation fee. The fees must be turned over by the commissioner to the state treasurer and credited to the general fund. The application file must be public, with the exception of financial data on individuals which is private ~~under the Minnesota Government Data Practices Act~~ as defined in section 13.02, subdivision 12, and data defined as trade secret information under section 13.37, subdivision 1, paragraph (b), which must be ~~given nonpublic classification~~ classified as private upon written request by the applicant.

Sec. 121. Minnesota Statutes 1998, section 46.07, subdivision 2, is amended to read:

Subd. 2. [CONFIDENTIAL RECORDS.] The commissioner shall divulge facts and information obtained in the course of examining financial institutions under the commissioner's supervision only when and to the extent required or permitted by law to report upon or take special action regarding the affairs of an institution, or ordered by a court of law to testify or produce evidence in a civil or criminal proceeding, except that the commissioner may furnish information as to matters of mutual interest to an official or examiner of the federal reserve system, the Federal Deposit Insurance Corporation, the Federal Office of Thrift Supervision, the Federal Home Loan Bank System, the National Credit Union Administration, comptroller of the currency, other state bank supervisory agencies subject to cooperative agreements authorized by section 49.411, subdivision

7, the United States Small Business Administration, for purposes of sections 53.09, subdivision 2a, and 56.10, subdivision 1, or state and federal law enforcement agencies. The commissioner shall not be required to disclose the name of a debtor of a financial institution under the commissioner's supervision, or anything relative to the private accounts, ownership, or transactions of an institution, or any fact obtained in the course of an examination thereof, except as herein provided. For purposes of this subdivision, a subpoena is not an order of a court of law. These records are classified as confidential ~~or protected nonpublic for purposes of the Minnesota Government Data Practices Act~~ data under section 13.02, subdivision 3, and their destruction, as prescribed in section 46.21, is exempt from the provisions of chapter 138 and Laws 1971, chapter 529, so far as their deposit with the state archives.

Sec. 122. Minnesota Statutes 1998, section 46.07, subdivision 3, is amended to read:

Subd. 3. [COMPLAINT FILES.] Notwithstanding the provisions of subdivision 2 to the contrary, data gathered and maintained in relation to a complaint filed with the commissioner is private ~~or nonpublic pursuant to the Minnesota Government Data Practices Act~~ data as defined in section 13.02, subdivision 12.

Sec. 123. Minnesota Statutes 1998, section 53A.081, subdivision 4, is amended to read:

Subd. 4. [CLASSIFICATION OF DATA.] Financial information on individuals and businesses that is submitted to the commissioner in the annual report under subdivision 1 are private data ~~on individuals or nonpublic data~~ as defined in section 13.02, subdivision 12.

Sec. 124. Minnesota Statutes 1998, section 60A.03, subdivision 9, is amended to read:

Subd. 9. [CONFIDENTIALITY OF INFORMATION.] The commissioner may not be required to divulge any information obtained in the course of the supervision of insurance companies, or the examination of insurance companies, including examination related correspondence and workpapers, until the

examination report is finally accepted and issued by the commissioner, and then only in the form of the final public report of examinations. Nothing contained in this subdivision prevents or shall be construed as prohibiting the commissioner from disclosing the content of this information to the insurance department of another state or the National Association of Insurance Commissioners if the recipient of the information agrees in writing to hold it as ~~nonpublic~~ private data not on individuals as defined in section 13.02, in a manner consistent with this subdivision. This subdivision does not apply to the extent the commissioner is required or permitted by law, or ordered by a court of law to testify or produce evidence in a civil or criminal proceeding. For purposes of this subdivision, a subpoena is not an order of a court of law.

Sec. 125. Minnesota Statutes 1998, section 60A.135, subdivision 4, is amended to read:

Subd. 4. [CONFIDENTIALITY.] Reports filed with the commissioner pursuant to sections 60A.135 to 60A.137 must be held as ~~nonpublic~~ private data not on individuals as defined in section 13.02, are not subject to subpoena, and may not be made public by the commissioner, the National Association of Insurance Commissioners, or other person, except to insurance departments of other states, without the prior written consent of the insurer to which it pertains. However, the commissioner may publish all or part of a report in the manner the commissioner considers appropriate if, after giving the affected insurer notice and an opportunity to be heard, the commissioner determines that the interest of policyholders, shareholders, or the public will be served by the publication.

Sec. 126. Minnesota Statutes 1998, section 60A.67, subdivision 1, is amended to read:

Subdivision 1. [GENERALLY.] All risk-based capital reports, to the extent the information in them is not required to be set forth in a publicly available annual statement schedule, and risk-based capital plans, including the results or report of an examination or analysis of an insurer performed

pursuant to sections 60A.60 to 60A.696, and any corrective order issued by the commissioner pursuant to an examination or analysis, with respect to a domestic insurer or foreign insurer that are filed with the commissioner constitute information that might be damaging to the insurer if made available to its competitors, and shall be maintained by the commissioner as ~~nonpublic~~ private data not on individuals as defined in section 13.02, subdivision 9 12. This information is not subject to subpoena, other than by the commissioner and then only for the purpose of enforcement actions taken by the commissioner pursuant to sections 60A.60 to 60A.696 or other provision of the insurance laws of this state.

Sec. 127. Minnesota Statutes 1998, section 60A.968, subdivision 2, is amended to read:

Subd. 2. [PRIVATE DATA.] Names and individual identification data for all viators is private ~~and confidential information~~ data on individuals as defined in section 13.02, subdivision 12, and must not be disclosed by the commissioner, unless required by law.

Sec. 128. Minnesota Statutes 1998, section 60D.22, is amended to read:

60D.22 [CONFIDENTIAL TREATMENT.]

All information, documents, and copies of them obtained by or disclosed to the commissioner or any other person in the course of an examination or investigation made pursuant to section 60D.20 and all information reported pursuant to sections 60D.18 and 60D.19, ~~shall be given confidential treatment~~ are private data not on individuals and shall not be subject to subpoena and shall not be made public by the commissioner, the National Association of Insurance Commissioners, or any other person, except to insurance departments of other states, without the prior written consent of the insurer to which it pertains unless the commissioner, after giving the insurer and its affiliates who would be affected, notice and opportunity to be heard, determines that the interest of policyholders or the public will be served by the publication, in which event the

commissioner may publish all or any part in the manner the commissioner considers appropriate.

Sec. 129. Minnesota Statutes 1998, section 62J.152, subdivision 7, is amended to read:

Subd. 7. [DATA GATHERING.] In evaluating a specific technology, the health technology advisory committee may seek the use of data collected by manufacturers, health plans, professional and trade associations, nonprofit organizations, academic institutions, or any other organization or association that may have data relevant to the committee's technology evaluation. All information obtained under this subdivision shall be considered ~~nonpublic~~ private data not on individuals under section 13.02, ~~subdivision 9,~~ unless the data is already available to the public generally or upon request.

Sec. 130. Minnesota Statutes 1998, section 62J.23, subdivision 2, is amended to read:

Subd. 2. [INTERIM RESTRICTIONS.] From July 1, 1992, until rules are adopted by the commissioner under this section, the restrictions in the federal Medicare antikickback statutes in section 1128B(b) of the Social Security Act, United States Code, title 42, section 1320a-7b(b), and rules adopted under the federal statutes, apply to all persons in the state, regardless of whether the person participates in any state health care program. The commissioner shall approve a transition plan submitted to the commissioner by January 1, 1993, by a person who is in violation of this section that provides a reasonable time for the person to modify prohibited practices or divest financial interests in other persons in order to come into compliance with this section. Transition plans ~~that identify individuals~~ are private data as defined in section 13.02, subdivision 12. ~~Transition plans that do not identify individuals are nonpublic data.~~

Sec. 131. Minnesota Statutes 1998, section 62J.321, subdivision 5, is amended to read:

Subd. 5. [DATA CLASSIFICATION.] (a) Data collected to fulfill the data and research initiatives authorized by sections

62J.301 to 62J.42 that identify individual patients or providers are private data ~~on individuals~~ as defined in section 13.02, subdivision 12. ~~Data not on individuals are nonpublic data.~~ The commissioner shall establish procedures and safeguards to ensure that data released by the commissioner is in a form that does not identify specific patients, providers, employers, individual or group purchasers, or other specific individuals and organizations, except with the permission of the affected individual or organization, or as permitted elsewhere in this chapter.

(b) Raw unaggregated data collected from household and employer surveys used by the commissioner to monitor the number of uninsured individuals, reasons for lack of insurance coverage, and to evaluate the effectiveness of health care reform, are subject to the same data classifications as data collected pursuant to sections 62J.301 to 62J.42.

(c) Notwithstanding sections 13.03, subdivisions 6 to 8; 13.10, subdivisions 1 to 4; and 138.17, data received by the commissioner pursuant to sections 62J.301 to 62J.42, ~~shall retain~~ retains the classification designated under this section and shall not be disclosed other than pursuant to this section.

(d) Summary data collected to fulfill the data and research initiatives authorized by sections 62J.301 to 62J.42 may be disseminated under section 13.05, subdivision 7. For the purposes of this section, summary data includes ~~nonpublic~~ private data not on individuals.

(e) Notwithstanding paragraph (a), the commissioner may publish ~~nonpublic or~~ private data collected pursuant to sections 62J.301 to 62J.42 on health care costs and spending, quality and outcomes, and utilization for health care institutions, individual health care professionals and groups of health care professionals, and group purchasers, with a description of the methodology used for analysis. The commissioner may not make public any patient identifying information except as specified in law. The commissioner shall not reveal the name of an institution, group of professionals, individual health care

professional, or group purchaser until after the institution, group of professionals, individual health care professional, or group purchaser has had 21 days to review the data and comment. The commissioner shall include comments received in the release of the data.

(f) A provider or group purchaser may contest whether the data meets the criteria of section 62J.311, subdivision 2, paragraph (a), clause (2), in accordance with a contested case proceeding as set forth in sections 14.57 to 14.62, subject to appeal in accordance with sections 14.63 to 14.68. To obtain a contested case hearing, the provider or group purchaser must make a written request to the commissioner before the end of the time period for review and comment. Within ten days of the assignment of an administrative law judge, the provider or group purchaser shall make a clear showing to the administrative law judge of probable success in a hearing on the issue of whether the data are accurate and valid and were collected based on the criteria of section 62J.311, subdivision 2, paragraph (a), clause (2). If the administrative law judge determines that the provider or group purchaser has made such a showing, the data shall remain private ~~or nonpublic~~ during the contested case proceeding and appeal. If the administrative law judge determines that the provider or group purchaser has not made such a showing, the commissioner may publish the data immediately, with comments received in the release of the data. The contested case proceeding and subsequent appeal is not an exclusive remedy and any person may seek a remedy pursuant to section 13.08, subdivisions 1 to 4, or as otherwise authorized by law.

Sec. 132. Minnesota Statutes 1998, section 62J.452, subdivision 2, is amended to read:

Subd. 2. [DATA CLASSIFICATIONS.] (a) Data collected, obtained, received, or created by the health data institute ~~shall be~~ is classified as private ~~or nonpublic~~ data, as ~~applicable~~ defined in section 13.02, subdivision 12, unless given a different classification in this subdivision. Data

classified as private ~~or nonpublic~~ under this subdivision may be released or disclosed only as permitted under this subdivision and under the other subdivisions referenced in this subdivision. For purposes of this section, data that identify individual patients or industry participants are private data on individuals or ~~nonpublic data~~ not on individuals, as appropriate. ~~Data not on individuals are nonpublic data.~~ Notwithstanding sections 13.03, subdivisions 6 to 8; 13.10, subdivisions 1 to 4; and 138.17, data received by the health data institute ~~shall~~ retain the classification designated under this chapter and shall not be disclosed other than pursuant to this chapter. Nothing in this subdivision prevents patients from gaining access to their health record information pursuant to section 144.335.

(b) When industry participants, as defined in section 62J.451, are required by statute to provide, either directly or through a contractor, as defined in section 62J.451, subdivision 2, paragraph (c), patient identifying data to the commissioner pursuant to this chapter or to the health data institute pursuant to section 62J.451, the industry participant or its contractor ~~shall be able to~~ may provide the data with or without patient consent, and may not be held liable for doing so.

(c) When an industry participant submits patient identifying data to the health data institute, and the data is submitted to the health data institute in electronic form, or through other electronic means including, but not limited to, the electronic data interchange system defined in section 62J.451, the industry participant shall submit the patient identifying data in encrypted form, using an encryption method supplied or specified by the health data institute. Submission of encrypted data as provided in this paragraph satisfies the requirements of section 144.335, subdivision 3b.

(d) Patient identifying data may be disclosed only as permitted under subdivision 3.

(e) Industry participant identifying data which is not patient identifying data may be disclosed only by being made

public in an analysis as permitted under subdivisions 4 and 5 or through access to an approved researcher, industry participant, or contractor as permitted under subdivision 6 or 7.

(f) Data that is not patient identifying data and not industry participant identifying data is public data.

(g) Data that describes the finances, governance, internal operations, policies, or operating procedures of the health data institute, and that does not identify patients or industry participants or identifies them only in connection with their involvement with the health data institute, is public data.

Sec. 133. Minnesota Statutes 1998, section 62J.452, subdivision 9, is amended to read:

Subd. 9. [AUTHORIZATION OF STATE AGENCIES AND POLITICAL SUBDIVISIONS TO PROVIDE DATA.] (a) Notwithstanding any limitation in chapter 13 or section 62J.321, subdivision 5, regarding the disclosure of ~~not-public~~ private or confidential data, all state agencies and political subdivisions, including, but not limited to, municipalities, counties, and hospital districts may provide ~~not-public~~ private or confidential data relating to health care costs, quality, or outcomes to the health data institute for the purposes set forth in section 62J.451.

(b) Data provided by the commissioner pursuant to paragraph (a) may not include patient identifying data as defined in section 62J.451, subdivision 2, paragraph (m). For data provided by the commissioner of health pursuant to paragraph (a), the health data institute and anyone receiving the data from the health data institute, is prohibited from unencrypting or attempting to link the data with other patient identifying data sources.

(c) Any data provided to the health data institute pursuant to paragraph (a) ~~shall retain~~ retains the same classification that it had with the state agency or political subdivision that provided it. The authorization in this subdivision is subject to any federal law restricting or prohibiting such disclosure of the data described above.

(d) Notwithstanding any limitation in chapter 13 or this section and section 62J.451 regarding the disclosure of ~~nonpublic and~~ private data, the health data institute may provide ~~nonpublic and~~ private data to any state agency that is a member of the board of the health data institute. Any such data provided to a state agency ~~shall retain nonpublic or~~ retains private classification~~, as applicable~~.

Sec. 134. Minnesota Statutes 1998, section 62J.452, subdivision 5, is amended to read:

Subd. 5. [FAIR HEARING PROCEDURE PRIOR TO MAKING AN ANALYSIS PUBLIC.] (a) The health data institute may not make public an analysis that identifies an industry participant unless the health data institute first complies with this subdivision. A draft of the portion of the analysis that identifies an industry participant must be furnished upon an industry participant's request to that industry participant prior to making that portion of the analysis public. ~~Such~~ The draft analysis is private ~~or nonpublic~~ data, as ~~applicable~~ defined in section 13.02, subdivision 12. The industry participants so identified have the right to a hearing, at which the industry participants or their contractors, as defined in section 62J.451, subdivision 2, paragraph (c), may object to or seek modification of the analysis. The cost of the hearing shall be borne by the industry participant requesting the hearing.

(b) The health data institute shall establish the hearing procedure in writing. The hearing procedure shall include the following:

(1) the provision of reasonable notice of the health data institute's intention to make ~~such~~ the analysis public;

(2) an opportunity for the identified industry participants to submit written statements to the health data institute board of directors or its designate, to be represented by a contractor, as defined in section 62J.451, subdivision 2, paragraph (c), or other individual or entity acting on behalf of and chosen by the industry participant for this purpose, and to

append a statement to ~~such~~ the analysis to be included with it when and if the analysis is made public; and

(3) access by the identified industry participants to industry participant identifying data, but only as permitted by subdivision 6 or 7.

(c) The health data institute shall make the hearing procedure available in advance to industry participants which are identified in an analysis. The written hearing procedure is public data. The following data related to a hearing is public:

(1) the parties involved;

(2) the dates of the hearing; and

(3) a general description of the issue and the results of the hearing.

All other data relating to the hearing is private ~~or nonpublic~~.

Sec. 135. Minnesota Statutes 1998, section 62L.10, subdivision 3, is amended to read:

Subd. 3. [SUBMISSIONS TO COMMISSIONER.] Subsequent to the annual filing, the commissioner may request information and documentation from a health carrier describing its rating practices and renewal underwriting practices, including information and documentation that demonstrates that a health carrier's rating methods and practices are in accordance with sound actuarial principles and the requirements of this chapter. Except in cases of violations of this chapter or of another chapter, information received by the commissioner as provided under this subdivision is ~~nonpublic~~ private data not on individuals.

Sec. 136. Minnesota Statutes 1998, section 62Q.03, subdivision 9, is amended to read:

Subd. 9. [DATA COLLECTION AND DATA PRIVACY.] The association members shall not have access to unaggregated data on individuals or health plan companies. The association shall develop, as a part of the plan of operation, procedures for ensuring that data is collected by an appropriate entity. The commissioners of health and commerce shall have the authority to

audit and examine data collected by the association for the purposes of the development and implementation of the risk adjustment system. Data on individuals obtained for the purposes of risk adjustment development, testing, and operation are ~~designated as~~ private data as defined in section 13.02, subdivision 12. Data not on individuals which is obtained for the purposes of development, testing, and operation of risk adjustment are ~~designated as nonpublic~~ private data as defined in section 13.02, subdivision 12, except that the proposed and approved plan of operation, the risk adjustment methodologies examined, the plan for testing, the plan of the risk adjustment system, minutes of meetings, and other general operating information are classified as public data. Nothing in this section ~~is intended to prohibit~~ prohibits the preparation of summary data under section 13.05, subdivision 7. The association, state agencies, and any contractors having access to this data shall maintain it in accordance with this classification. The commissioners of health and human services have the authority to collect data from health plan companies as needed for the purpose of developing a risk adjustment mechanism for public programs.

Sec. 137. Minnesota Statutes 1998, section 62E.13, subdivision 11, is amended to read:

Subd. 11. [CLASSIFICATION OF PPO AGREEMENT DATA.] If the writing carrier uses its own provider agreements for the association's preferred provider network in lieu of agreements exclusively between the association and the providers, then the terms and conditions of those agreements are ~~nonpublic~~ private data as defined in section 13.02, subdivision 9 12.

Sec. 138. Minnesota Statutes 1998, section 62J.79, subdivision 4, is amended to read:

Subd. 4. [DATA PRIVACY.] (a) Consumer complaint data, including medical records and other documentation, provided by a patient or enrollee to the office of health care consumer assistance, advocacy, and information ~~shall be~~ is classified as private data on individuals under section 13.02, subdivision 12.

(b) Except as provided in paragraph (a), all data collected or maintained by the office in the course of assisting a patient or enrollee in resolving a complaint, including data collected or maintained for the purpose of assistance during a formal or informal dispute resolution process, shall be classified as investigative data under section 13.39, except that inactive investigative data shall be classified as private data on individuals under section 13.02, subdivision 12.

Sec. 139. Minnesota Statutes 1998, section 72A.20, subdivision 15, is amended to read:

Subd. 15. [PRACTICES NOT HELD TO BE DISCRIMINATION OR REBATES.] Nothing in subdivision 8, 9, or 10, or in section 72A.12, subdivisions 3 and 4, shall be construed as including within the definition of discrimination or rebates any of the following practices:

(1) in the case of any contract of life insurance or annuity, paying bonuses to policyholders or otherwise abating their premiums in whole or in part out of surplus accumulated from nonparticipating insurance, provided that any bonuses or abatement of premiums shall be fair and equitable to policyholders and for the best interests of the company and its policyholders;

(2) in the case of life insurance policies issued on the industrial debit plan, making allowance, to policyholders who have continuously for a specified period made premium payments directly to an office of the insurer, in an amount which fairly represents the saving in collection expense;

(3) readjustment of the rate of premium for a group insurance policy based on the loss or expense experienced thereunder, at the end of the first or any subsequent policy year of insurance thereunder, which may be made retroactive only for such policy year;

(4) in the case of an individual or group health insurance policy, the payment of differing amounts of reimbursement to insureds who elect to receive health care goods or services from providers designated by the insurer, provided that each insurer

shall on or before August 1 of each year file with the commissioner summary data regarding the financial reimbursement offered to providers so designated.

Any insurer which proposes to offer an arrangement authorized under this clause shall disclose prior to its initial offering and on or before August 1 of each year thereafter as a supplement to its annual statement submitted to the commissioner pursuant to section 60A.13, subdivision 1, the following information:

(a) the name which the arrangement intends to use and its business address;

(b) the name, address, and nature of any separate organization which administers the arrangement on the behalf of the insurers; and

(c) the names and addresses of all providers designated by the insurer under this clause and the terms of the agreements with designated health care providers.

The commissioner shall maintain a record of arrangements proposed under this clause, including a record of any complaints submitted relative to the arrangements.

If the commissioner requests copies of contracts with a provider under this clause and the provider requests a determination, all information contained in the contracts that the commissioner determines may place the provider or health care plan at a competitive disadvantage is ~~nonpublic~~ private data not on individuals as defined in section 13.02, subdivision 12.

Sec. 140. Minnesota Statutes 1998, section 79A.02, subdivision 2, is amended to read:

Subd. 2. [ADVICE TO COMMISSIONER.] At the request of the commissioner, the committee shall meet and shall advise the commissioner with respect to whether or not an applicant to become a private self-insurer in the state of Minnesota has met the statutory requirements to self-insure. The department of commerce may furnish the committee with any financial data which it has, but a member of the advisory committee who may have a

conflict of interest in reviewing the financial data shall not have access to the data nor participate in the discussions concerning the applicant. Financial data received from the commissioner is ~~nonpublic~~ private data not on individuals as defined in section 13.02, subdivision 12. The committee shall advise the commissioner if it has any information that any private self-insurer may become insolvent.

Sec. 141. Minnesota Statutes 1998, section 115A.84, subdivision 5, is amended to read:

Subd. 5. [EXCLUSION OF MATERIALS SEPARATED AT CERTAIN FACILITIES.] (a) A county or district shall exclude from the designation, subject to approval by the director, materials that the county or district determines will be separated for recycling at a transfer station located outside of the area subject to designation if:

(1) the residual materials left after separation of the recyclable materials are delivered to a facility designated by the county or district;

(2) each waste collector who would otherwise be subject to the designation ordinance and who delivers waste to the transfer station has not been found in violation of the designation ordinance in the six months prior to filing for an exclusion;

(3) the materials separated at the transfer station are delivered to a recycler and are actually recycled; and

(4) the owner or operator of the transfer station agrees to report and actually reports to the county or district the quantities of materials, by categories to be specified by the county or district, that are recycled by the facility that otherwise would have been subject to designation.

(b) In order to qualify for the exclusion in this subdivision, the owner of a transfer station shall file with the county or district a written description of the transfer station, its operation, location, and waste supply sources, the quantity of waste delivered to the transfer station by the owner of the transfer station, the market for the materials separated for recycling, where the recyclable materials are delivered for

recycling, and other information the county or district may reasonably require. Information received by the county or district is ~~nonpublic~~ private data not as individuals as defined in section 13.02, subdivision 9 12.

(c) A county or district that grants an exclusion under this subdivision may revoke the exclusion if any of the conditions of paragraph (a) are not being met.

Sec. 142. Minnesota Statutes 1998, section 115A.882, subdivision 3, is amended to read:

Subd. 3. [INSPECTION.] A person authorized by a county in which a designation ordinance is effective may, anywhere in the state:

(1) upon presentation of identification and without a search warrant, inspect or copy the records required to be kept on a waste collection vehicle under subdivision 2 and inspect the waste on the vehicle at the time of deposit of the waste at a facility;

(2) when reasonable notice under the circumstances has been given, upon presentation of identification and without a search warrant, inspect or copy the records of an owner or operator of a solid waste facility that are required to be maintained under subdivision 2;

(3) request, in writing, copies of records of a solid waste collector that indicate the type, origin, and weight or, if applicable, the volume of waste collected, the identity of the facility at which the waste was deposited, and the date of deposit at the facility; and

(4) upon presentation of identification and without a search warrant, inspect or copy that portion of the business records of a waste collector necessary to comply with clause (3) at the central record keeping location of the waste collector only if the collector fails to provide copies of the records within 15 days of receipt of a written request for them, unless the time has been extended by agreement of the parties.

Records or information received, inspected, or copied by a county under this section are classified as ~~nonpublic~~ private

data not on individuals as defined in section 13.02, subdivision 9 12, and may be used by the county solely for enforcement of a designation ordinance. A waste collector or the owner or operator of a waste facility shall maintain business records needed to comply with this section for two years.

Sec. 143. Minnesota Statutes 1998, section 115A.93, subdivision 5, is amended to read:

Subd. 5. [CUSTOMER DATA.] Customer lists provided to counties or cities by solid waste collectors are private data on ~~individuals~~ as defined in section 13.02, ~~subdivision 12, with regard to data on individuals, or nonpublic data as defined in section 13.02, subdivision 9, with regard to data not on individuals~~.

Sec. 144. Minnesota Statutes 1998, section 115B.17, subdivision 5, is amended to read:

Subd. 5. [CLASSIFICATION OF DATA.] Except as otherwise provided in this subdivision, data obtained from any person pursuant to subdivision 3 or 4 is public data as defined in section 13.02. Upon certification by the subject of the data that the data relates to sales figures, processes or methods of production unique to that person, or information which would tend to affect adversely the competitive position of that person, the commissioner shall classify the data as private ~~or nonpublic~~ data as defined in section 13.02. Notwithstanding any other law to the contrary, data classified as private ~~or nonpublic~~ under this subdivision may be disclosed when relevant in any proceeding under sections 115B.01 to 115B.18, or to other public agencies concerned with the implementation of sections 115B.01 to 115B.18.

Sec. 145. Minnesota Statutes 1998, section 115B.24, subdivision 5, is amended to read:

Subd. 5. [EXCHANGE OF INFORMATION.] Notwithstanding the provisions of section 116.075, the pollution control agency may provide the commissioner of revenue with the information necessary for the enforcement of section 115B.22 and this section. Information disclosed in a return filed pursuant to

this section is public. Information exchanged between the commissioner and the agency is public unless the information is of the type determined to be for the confidential use of the agency pursuant to section 116.075 or is trade secret information classified pursuant to section 13.37. Information obtained in the course of an audit of the taxpayer by the department of revenue ~~shall be nonpublic or~~ is private data as defined in section 13.02 to the extent that it is not directly divulged in a return of the tax.

Sec. 146. Minnesota Statutes 1998, section 115C.03, subdivision 8, is amended to read:

Subd. 8. [CLASSIFICATION OF DATA.] Except as otherwise provided in this subdivision, data obtained from a person under subdivision 6 or 7 is public data as defined in section 13.02. Upon certification by the subject of the data that the data relates to sales figures, processes or methods of production unique to that person, or information that would tend to adversely affect the competitive position of that person, the commissioner shall classify the data as private ~~or nonpublic~~ data as defined in section 13.02. Data classified as private ~~or nonpublic~~ under this subdivision may be disclosed when relevant in a proceeding under this chapter.

Sec. 147. Minnesota Statutes 1998, section 115D.09, is amended to read:

115D.09 [CONFIDENTIALITY.]

Information and techniques developed under section 115D.04, the reduction information and techniques under section 115A.0716, and the progress reports required under section 115D.08 are public data under chapter 13. The plans required under section 115D.07 are ~~nonpublic~~ private data not on individuals under ~~chapter 13~~ section 13.02.

Sec. 148. Minnesota Statutes 1998, section 116.54, is amended to read:

116.54 [INJECTION OF CERTAIN MATERIALS.]

The pollution control agency shall authorize and may monitor not less than one or more than five projects to test the

controlled injection of oxygen-bearing materials and appropriate microbiological systems into sites of water or soil contamination. An applicant for authority to conduct one of the tests shall describe to the agency plans for the test injection project including at least the following:

(1) the quantity and type of chemicals and microbes to be used in the injection project;

(2) the frequency and planned duration of the injections;

(3) test monitoring and evaluation equipment that will be maintained at the site; and

(4) procedures for recording, analyzing, and maintaining information on the injection project.

The applicant shall make available to the agency all significant test results from the injection project. Trade secret information, as defined in section 13.37, made available by an applicant is classified as ~~nonpublic~~ private data, pursuant to section 13.02, subdivision 9~~, or private data on individuals, pursuant to section 13.02, subdivision~~ 12.

Sec. 149. Minnesota Statutes 1998, section 116C.840, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION.] Except as otherwise provided in this subdivision, data obtained from any person pursuant to subdivision 1 is public data as defined in section 13.02. Upon certification by the generator that the data relates to sales figures, processes, or methods of production unique to that person, or information which would tend to affect adversely the competitive position of that person, the agency shall classify the data as ~~nonpublic~~ private data not on individuals as defined in section 13.02. The agency may disclose data classified as ~~nonpublic~~ private under this subdivision to the Interstate Commission, when relevant in any proceeding under section 116C.835, or when necessary to carry out its responsibilities under sections 116C.833 to 116C.843.

Sec. 150. Minnesota Statutes 1998, section 116O.03, subdivision 6, is amended to read:

Subd. 6. [CLOSED MEETINGS; RECORDING.] The board of

directors may by a majority vote in a public meeting decide to hold a closed meeting authorized under subdivision 5. The time and place of the closed meeting must be announced at the public meeting. A written roll of members present at the closed meeting must be made available to the public after the closed meeting. The proceedings of a closed meeting must be tape recorded at the expense of the board and must be preserved by the board for two years. The data on the tape is ~~nonpublic~~ private data not on individuals under section 13.02~~,-subdivision~~ 9.

Sec. 151. Minnesota Statutes 1998, section 116O.03, subdivision 7, is amended to read:

Subd. 7. [APPLICATION AND INVESTIGATIVE DATA.] The following data is classified as private data ~~with-regard-to-data on-individuals~~ under section 13.02~~,-subdivision-12,-or-as nonpublic-data-with-regard-to-data-not-on-individuals-under section-13.02,-subdivision-9,-whichever-is-applicable:~~

(1) financial data, statistics, and information furnished in connection with assistance or proposed assistance under section 116O.06, including credit reports, financial statements, statements of net worth, income tax returns, either personal or corporate, and any other business and personal financial records; or

(2) security information, trade secret information, or labor relations information, as defined in section 13.37, subdivision 1, disclosed to members of the corporation board or employees of the corporation under section 116O.06.

Sec. 152. Minnesota Statutes 1998, section 116R.02, subdivision 3, is amended to read:

Subd. 3. [REVIEW PROCEDURE; DATA PRACTICES.] (a) Before issuing the bonds for a project, approving financial assistance, or entering into loan, lease, or other revenue agreements for the project described in subdivisions 5 and 6, the commissioner of finance shall review the financial condition of the proposed lessee or lessees of the project or projects, and any related person. The commissioner shall exercise due diligence in the

review. The commissioner shall engage an independent, nationally recognized consultant having special expertise with the airline industry and its financing to prepare a written report on the financial condition of the lessee or lessees and any related person. A lessee and any related person shall provide all information required for the commissioner's review and the consultant's report, including information substantially equivalent to that required by an investment bank or other financial institution considering a project for debt financing.

(b) Except as otherwise provided in this subdivision, business plans, financial statements, customer lists, and market and feasibility studies required under sections 116R.01 to 116R.16 or submitted in connection with the provision of financial assistance or any agreement authorized under Laws 1991, chapter 350, are ~~nonpublic~~ private data not on individuals, as defined in section 13.02, subdivision 9 12. The commissioner or the commissioner of trade and economic development may make the data accessible to any person, agency, or public entity if the commissioner or the commissioner of trade and economic development determines that access is required under state or federal securities law or is necessary for the person, agency, or public entity to perform due diligence in connection with the provision of financial assistance to the projects described in subdivisions 5 and 6. The data may also be made available as requested by the legislative commission on planning and fiscal policy.

(c) Before the commissioner issues bonds for a project, approves financial assistance, or enters into loan, lease, or other revenue agreements for the project, the commissioner shall submit a report on the proposed transaction to the governor. The report must describe: all proposed state, metropolitan, and local government financial commitments; the financial assistance proposed to be provided; the proposed loan, lease, and revenue agreements; any other arrangements related to state and local debt, taxes, financing, and debt service; and the estimates of economic activity, air traffic, and other factors that have been

used in assessing the prospective financial condition of the lessee or lessees and any related person. The report must contain the following findings:

(1) that the commissioners of trade and economic development and finance and, for purposes of a project described in subdivision 5, the metropolitan airports commission have reviewed the current and prospective financial condition of each proposed lessee of the project or projects and any related person; and

(2) that, on the basis of their review, the commissioners and, for purposes of the project described in subdivision 5, the commission have determined that the revenues estimated to be available to the lessee or lessees for payments under the loan, lease, or other revenue agreements are at least sufficient during each year of the term of the proposed bonds to pay when due all financial obligations of the lessee or lessees under the terms of the proposed loan, lease, or other revenue agreements. Copies of the report must be filed at the legislature as provided in section 3.195 when the report is submitted to the governor.

Sec. 153. Minnesota Statutes 1998, section 116S.02, subdivision 8, is amended to read:

Subd. 8. [APPLICATION AND INVESTIGATIVE DATA.] Financial data, statistics, and information furnished to the corporation in connection with assistance or proposed assistance, including credit reports, financial statements, statements of net worth, income tax returns, either personal or corporate, and any other business and personal financial records are private data ~~with regard to data on individuals~~ under section 13.02, subdivision 12~~, or as nonpublic data with regard to data not on individuals under section 13.02, subdivision 9~~.

Sec. 154. Minnesota Statutes 1998, section 144.147, subdivision 5, is amended to read:

Subd. 5. [EVALUATION.] The commissioner shall evaluate the overall effectiveness of the grant program. The commissioner may collect, from the hospital, and communities receiving

grants, the information necessary to evaluate the grant program. Information related to the financial condition of individual hospitals shall be classified as ~~nonpublic~~ private data not on individuals under section 13.02.

Sec. 155. Minnesota Statutes 1998, section 144.225, subdivision 6, is amended to read:

Subd. 6. [GROUP PURCHASER IDENTITY; ~~NONPUBLIC~~ PRIVATE DATA; DISCLOSURE.] (a) Except as otherwise provided in this subdivision, the named identity of a group purchaser as defined in section 62J.03, subdivision 6, collected in association with birth registration is ~~nonpublic~~ private data not on individuals as defined in section 13.02, subdivision 12.

(b) The commissioner may publish, or by other means release to the public, the named identity of a group purchaser as part of an analysis of information collected from the birth registration process. Analysis means the identification of trends in prenatal care and birth outcomes associated with group purchasers. The commissioner may not reveal the named identity of the group purchaser until the group purchaser has had 21 days after receipt of the analysis to review the analysis and comment on it. In releasing data under this subdivision, the commissioner shall include comments received from the group purchaser related to the scientific soundness and statistical validity of the methods used in the analysis. This subdivision does not authorize the commissioner to make public any individual identifying data except as permitted by law.

(c) A group purchaser may contest whether an analysis made public under paragraph (b) is based on scientifically sound and statistically valid methods in a contested case proceeding under sections 14.57 to 14.62, subject to appeal under sections 14.63 to 14.68. To obtain a contested case hearing, the group purchaser must present a written request to the commissioner before the end of the time period for review and comment. Within ten days of the assignment of an administrative law judge, the group purchaser must demonstrate by clear and convincing evidence the group purchaser's likelihood of

succeeding on the merits. If the judge determines that the group purchaser has made this demonstration, the data may not be released during the contested case proceeding and through appeal. If the judge finds that the group purchaser has not made this demonstration, the commissioner may immediately publish, or otherwise make public, the ~~nonpublic~~ private group purchaser data, with comments received as set forth in paragraph (b).

(d) The contested case proceeding and subsequent appeal is not an exclusive remedy and any person may seek a remedy pursuant to section 13.08, subdivisions 1 to 4, or as otherwise authorized by law.

Sec. 156. Minnesota Statutes 1998, section 144.4186, subdivision 1, is amended to read:

Subdivision 1. [~~NONPUBLIC~~ PRIVATE AND CONFIDENTIAL DATA.] Data contained in a health directive are classified as ~~protected nonpublic~~ confidential data ~~under section 13.02, subdivision 13,~~ in the case of data not on individuals under section 13.02, subdivision 3, and private data under section 13.02, subdivision 12, in the case of data on individuals. Investigative data ~~shall have the classification accorded it~~ is classified under section 13.39.

Sec. 157. Minnesota Statutes 1998, section 144.581, subdivision 5, is amended to read:

Subd. 5. [CLOSED MEETINGS; RECORDING.] (a) Notwithstanding subdivision 4 or section 471.705, a public hospital or an organization established under this section may hold a closed meeting to discuss specific marketing activity and contracts that might be entered into pursuant to the marketing activity in cases where the hospital or organization is in competition with health care providers that offer similar goods or services, and where disclosure of information pertaining to those matters would cause harm to the competitive position of the hospital or organization, provided that the goods or services do not require a tax levy. No contracts referred to in this paragraph may be entered into earlier than 15 days after the proposed contract

has been described at a public meeting and the description entered in the minutes, except for contracts for consulting services or with individuals for personal services.

(b) A meeting may not be closed under paragraph (a) except by a majority vote of the board of directors in a public meeting. The time and place of the closed meeting must be announced at the public meeting. A written roll of members present at the closed meeting must be available to the public after the closed meeting. The proceedings of a closed meeting must be tape-recorded and preserved by the board of directors for two years. The data on the tape are ~~nonpublic~~ private data not on individuals under section 13.02, subdivision 9 12. However, the data become public data under section 13.02, subdivision 14, two years after the meeting, or when the hospital or organization takes action on matters referred to in paragraph (a), except for contracts for consulting services. In the case of personal service contracts, the data become public when the contract is signed. For entities subject to section 471.345, a contract entered into by the board is subject to the requirements of section 471.345.

(c) The board of directors may not discuss a tax levy, bond issuance, or other expenditure of money unless the expenditure is directly related to specific marketing activities and contracts described in paragraph (a) at a closed meeting.

Sec. 158. Minnesota Statutes 1998, section 145.64, subdivision 3, is amended to read:

Subd. 3. [HENNEPIN COUNTY EMERGENCY MEDICAL SERVICES DATA.] Data collected, created, or maintained by the quality committee of the Hennepin county emergency medical services advisory council when conducting a health care review activity of the emergency medical services function or services are private data ~~on individuals or nonpublic data not on individuals~~, as defined in section 13.02.

Sec. 159. Minnesota Statutes 1998, section 156.082, is amended to read:

156.082 [VETERINARY MEDICAL RECORDS.]

Veterinary records of a client that are maintained by a state agency, statewide system, or political subdivision are private data ~~on individuals or nonpublic data~~ as defined in section 13.02.

Sec. 160. Minnesota Statutes 1998, section 174.30, subdivision 9, is amended to read:

Subd. 9. [COMPLAINT DATA; CLASSIFICATION.] When information is furnished to the department of transportation that alleges a violation of this section, an operating standard adopted under this section, or section 174.315, the following data are classified as confidential data ~~or protected nonpublic data~~ as defined in section 13.02, subdivision 3:

(1) names of complainants;

(2) complaint letters; and

(3) other unsolicited data when furnished by a person who is not the subject of the data and who is not a department employee.

Sec. 161. Minnesota Statutes 1998, section 182.668, subdivision 2, is amended to read:

Subd. 2. [CLASSIFICATION OF DATA.] Information that has been registered pursuant to subdivision 1 ~~shall be~~ is classified as ~~nonpublic or~~ private data as defined in section 13.02~~, subdivisions 9 and 12~~.

All other information reported to or otherwise obtained by the commissioner or a representative in connection with any inspection or proceeding under this chapter which contains or which might reveal a trade secret ~~shall be~~ is classified as ~~nonpublic or~~ private data as defined in section 13.02~~, subdivisions 9 and 12~~. Information classified as ~~nonpublic or~~ private may be disclosed to other officers or employees concerned with carrying out this chapter or when relevant in any proceeding under this chapter or when otherwise required in order to comply with federal law or regulation but only to the extent required by the federal law or regulation.

Sec. 162. Minnesota Statutes 1998, section 214.25, subdivision 1, is amended to read:

Subdivision 1. [BOARD DATA.] (a) All data collected or maintained as part of the board's duties under sections 214.19, 214.23, and 214.24 ~~shall be~~ is classified as investigative data under section 13.39 except that inactive investigative data ~~shall be~~ is classified as private data under section 13.02, subdivision 12~~, or nonpublic data under section 13.02, subdivision 9, in the case of data not on individuals~~.

(b) Notwithstanding section 13.05, subdivision 9, data addressed in this subdivision shall not be disclosed except as provided in this subdivision or section 13.04; except that the board may disclose to the commissioner under section 214.23.

Sec. 163. Minnesota Statutes 1998, section 214.35, is amended to read:

214.35 [CLASSIFICATION OF DATA.]

All data collected and maintained and any agreements with regulated persons entered into as part of the program is classified as active investigative data under section 13.41 while the individual is in the program, except for monitoring data which is classified as private. When a regulated person successfully completes the program, the data and participation agreement become inactive investigative data which ~~shall be~~ is classified as private data under section 13.02, subdivision 12~~, or nonpublic data under section 13.02, subdivision 9, in the case of data not on individuals~~. Data and agreements shall not be forwarded to the board unless the program reports a participant to a board as described in section 214.33, subdivision 3.

Sec. 164. Minnesota Statutes 1998, section 216C.17, subdivision 4, is amended to read:

Subd. 4. [PUBLIC INSPECTION.] Reports issued pursuant to this section, other than individual corporate reports classified as ~~nonpublic~~ private data not on individuals in section 13.68, shall be available for public inspection in the office of the department during normal business hours.

Sec. 165. Minnesota Statutes 1998, section 216C.37, subdivision 3b, is amended to read:

Subd. 3b. [PUBLIC ACCESSIBILITY OF LOAN APPLICATION DATA.] Data contained in an application submitted to the commissioner for a loan to be made pursuant to this section, including supporting technical documentation, is classified as "public data not on individuals" under section 13.02, subdivision 14.

Sec. 166. Minnesota Statutes 1998, section 221.0355, subdivision 9, is amended to read:

Subd. 9. [APPLICATION DATA.] The following data submitted to the commissioner under subdivisions 4 and 5 are private data~~,~~ ~~with respect to data on individuals, and nonpublic data, with respect to data not on individuals~~ under section 13.02, subdivision 12: information contained in parts II and III of the uniform application relating to a carrier's customers and service provided to specific customers, financial balance sheet and income statement data, ownership and debt liability data, and information relating to a carrier's parent companies, affiliates, and subsidiaries. For the purpose of administering or enforcing the uniform program, the commissioner may disclose any information classified by this subdivision as private data ~~on individuals or nonpublic data by this subdivision~~ to the United States Department of Transportation, any other participating state or state agency, or to the national repository established under the uniform program.

Sec. 167. Minnesota Statutes 1998, section 223.17, subdivision 6, is amended to read:

Subd. 6. [FINANCIAL STATEMENTS.] For the purpose of fixing or changing the amount of a required bond or for any other proper reason, the commissioner shall require an annual financial statement from a licensee which has been prepared in accordance with generally accepted accounting principles and which meets the following requirements:

(a) The financial statement shall include, but not be limited to the following: (1) a balance sheet; (2) a statement of income (profit and loss); (3) a statement of retained earnings; (4) a statement of changes in financial position; and (5) a statement of the dollar amount of grain purchased in the

previous fiscal year of the grain buyer.

(b) The financial statement shall be accompanied by a compilation report of the financial statement which is prepared by a grain commission firm or a management firm approved by the commissioner or by an independent public accountant, in accordance with standards established by the American Institute of Certified Public Accountants.

(c) The financial statement shall be accompanied by a certification by the chief executive officer or the chief executive officer's designee of the licensee, under penalty of perjury, that the financial statement accurately reflects the financial condition of the licensee for the period specified in the statement.

Only one financial statement must be filed for a chain of warehouses owned or operated as a single business entity, unless otherwise required by the commissioner. Any grain buyer having a net worth in excess of $500,000,000 need not file the financial statement required by this subdivision but must provide the commissioner with a certified net worth statement. All financial statements filed with the commissioner are private ~~or nonpublic~~ data as provided in section 13.02.

Sec. 168. Minnesota Statutes 1998, section 256.01, subdivision 12, is amended to read:

Subd. 12. [CHILD MORTALITY REVIEW PANEL.] (a) The commissioner shall establish a child mortality review panel to review deaths of children in Minnesota, including deaths attributed to maltreatment or in which maltreatment may be a contributing cause and to review near fatalities as defined in section 626.556, subdivision 11d. The commissioners of health, children, families, and learning, and public safety and the attorney general shall each designate a representative to the child mortality review panel. Other panel members shall be appointed by the commissioner, including a board-certified pathologist and a physician who is a coroner or a medical examiner. The purpose of the panel shall be to make recommendations to the state and to county agencies for

improving the child protection system, including modifications in statute, rule, policy, and procedure.

(b) The commissioner may require a county agency to establish a local child mortality review panel. The commissioner may establish procedures for conducting local reviews and may require that all professionals with knowledge of a child mortality case participate in the local review. In this section, "professional" means a person licensed to perform or a person performing a specific service in the child protective service system. "Professional" includes law enforcement personnel, social service agency attorneys, educators, and social service, health care, and mental health care providers.

(c) If the commissioner of human services has reason to believe that a child's death was caused by maltreatment or that maltreatment was a contributing cause, the commissioner has access to ~~not public~~ private or confidential data under chapter 13 maintained by state agencies, statewide systems, or political subdivisions that are related to the child's death or circumstances surrounding the care of the child. The commissioner shall also have access to records of private hospitals as necessary to carry out the duties prescribed by this section. Access to data under this paragraph is limited to police investigative data; autopsy records and coroner or medical examiner investigative data; hospital, public health, or other medical records of the child; hospital and other medical records of the child's parent that relate to prenatal care; and records created by social service agencies that provided services to the child or family within three years preceding the child's death. A state agency, statewide system, or political subdivision shall provide the data upon request of the commissioner. ~~Not public~~ Private or confidential data may be shared with members of the state or local child mortality review panel in connection with an individual case.

(d) Notwithstanding the data's classification in the possession of any other agency, data acquired by a local or state child mortality review panel in the exercise of its duties

is ~~protected nonpublic or~~ confidential data as defined in section 13.02, subdivision 3, but may be disclosed as necessary to carry out the purposes of the review panel. The data is not subject to subpoena or discovery. The commissioner may disclose conclusions of the review panel, but shall not disclose data that was classified as confidential or private data on decedents, under section 13.10, ~~or~~ private, data on individuals or confidential, ~~or protected nonpublic~~ data in the disseminating agency, except that the commissioner may disclose local social service agency data as provided in section 626.556, subdivision 11d, on individual cases involving a fatality or near fatality of a person served by the local social service agency prior to the date of death.

(e) A person attending a child mortality review panel meeting shall not disclose what transpired at the meeting, except to carry out the purposes of the mortality review panel. The proceedings and records of the mortality review panel are ~~protected nonpublic~~ confidential data not on individuals as defined in section 13.02, subdivision ~~13~~ 3, and are not subject to discovery or introduction into evidence in a civil or criminal action against a professional, the state or a county agency, arising out of the matters the panel is reviewing. Information, documents, and records otherwise available from other sources are not immune from discovery or use in a civil or criminal action solely because they were presented during proceedings of the review panel. A person who presented information before the review panel or who is a member of the panel shall not be prevented from testifying about matters within the person's knowledge. However, in a civil or criminal proceeding a person shall not be questioned about the person's presentation of information to the review panel or opinions formed by the person as a result of the review meetings.

Sec. 169. Minnesota Statutes 1998, section 256.9744, subdivision 1, is amended to read:

Subdivision 1. [CLASSIFICATION.] Except as provided in this section, data maintained by the office under sections

256.974 to 256.9744 are private data ~~on individuals or nonpublic data~~ as defined in section 13.02, subdivision ~~9 or~~ 12, and must be maintained in accordance with the requirements of Public Law Number 100-75, United States Code, title 42, section 3027(a)(12)(D).

Sec. 170. Minnesota Statutes 1998, section 268.19, is amended to read:

268.19 [INFORMATION.]

(a) Except as otherwise provided by this section, data gathered from any employer or individual pursuant to the administration of sections 268.03 to 268.23 are private data ~~on individuals or nonpublic data not on individuals~~ as defined in section 13.02, ~~subdivisions~~ subdivision 9 ~~and~~ 12, and may not be disclosed except pursuant to a court order or section 13.05. These data may be disseminated to and used by the following agencies without the consent of the subject of the data:

(1) state and federal agencies specifically authorized access to the data by state or federal law;

(2) any agency of Minnesota or any other state; or any federal agency charged with the administration of an employment security law or the maintenance of a system of public employment offices;

(3) human rights agencies within Minnesota that have enforcement powers;

(4) the department of revenue must have access to department private data ~~on individuals and nonpublic data not on individuals~~ as defined in section 13.02, subdivision 12, only to the extent necessary for enforcement of Minnesota tax laws;

(5) public and private agencies responsible for administering publicly financed assistance programs for the purpose of monitoring the eligibility of the program's recipients;

(6) the department of labor and industry on an interchangeable basis with the department subject to the following limitations and notwithstanding any law to the contrary:

(i) the department must have access to private data ~~on individuals and nonpublic data not on individuals~~ as defined in section 13.02, subdivision 12, for uses consistent with the administration of its duties under sections 268.03 to 268.23; and

(ii) the department of labor and industry must have access to private data ~~on individuals and nonpublic data not on individuals~~ as defined in section 13.02, subdivision 12, for uses consistent with the administration of its duties under Minnesota law;

(7) the department of trade and economic development may have access to private data on ~~individual~~ employers ~~and nonpublic data not on individual employers~~ for its internal use only; when received by the department of trade and economic development, the data remain private data ~~on individuals or nonpublic data~~;

(8) local and state welfare agencies for monitoring the eligibility of the data subject for assistance programs, or for any employment or training program administered by those agencies, whether alone, in combination with another welfare agency, or in conjunction with the department or to monitor and evaluate the statewide Minnesota family investment program by providing data on recipients and former recipients of food stamps, cash assistance under chapter 256, 256D, 256J, or 256K, child care assistance under chapter 119B, or medical programs under chapter 256B, 256D, or 256L;

(9) local, state, and federal law enforcement agencies for the sole purpose of ascertaining the last known address and employment location of the data subject, ~~provided~~ if the data subject is the subject of a criminal investigation; and

(10) the department of health may have access to private data ~~on individuals and nonpublic data not on individuals~~ as defined in section 13.02, subdivision 12, solely for the purposes of epidemiologic investigations.

(b) Data on individuals and employers that are collected, maintained, or used by the department in an investigation

pursuant to section 268.182 are confidential ~~as to~~ data ~~on individuals and protected nonpublic data not on individuals~~ as defined in section 13.02, ~~subdivisions~~ subdivision 3 ~~and 13~~, and must not be disclosed except pursuant to statute or court order or to a party named in a criminal proceeding, administrative or judicial, for preparation of a defense.

(c) Tape recordings and transcripts of recordings of proceedings conducted in accordance with section 268.105 and exhibits received into evidence at those proceedings are private data ~~on individuals and nonpublic data not on individuals~~ as defined in section 13.02, subdivision 12, and must be disclosed only pursuant to the administration of section 268.105, or pursuant to a court order.

(d) The department may disseminate an employer's name, address, industry code, occupations employed, and the number of employees by ranges of not less than 100 for the purpose of assisting individuals using the Minnesota workforce center system in obtaining employment.

(e) The general aptitude test battery and the nonverbal aptitude test battery as administered by the department are private data ~~on individuals or nonpublic data~~ as defined in section 13.02, subdivision 12.

(f) Data gathered by the department pursuant to the administration of sections 268.03 to 268.23 must not be made the subject or the basis for any suit in any civil proceedings, administrative or judicial, unless the action is initiated by the department.

Sec. 171. Minnesota Statutes 1998, section 270B.02, is amended to read:

270B.02 [CLASSIFICATION OF DATA.]

Subdivision 1. [GENERAL RULE.] Except as otherwise provided in this chapter, returns and return information are private data ~~on individuals or nonpublic data~~ as defined in section 13.02, ~~subdivisions 9 and~~ subdivision 12. Except as authorized by this chapter, the department of revenue, the commissioner, an officer or employee or former officer or

employee of the department of revenue, a person engaged or retained by the department on an independent contract basis, or a person who, under sections 270B.05 to 270B.15, is permitted to inspect returns or return information may not disclose returns or return information.

Subd. 2. [~~PROTECTED-NONPUBLIC~~ CONFIDENTIAL DATA.] The following are ~~protected-nonpublic~~ confidential data as defined in section 13.02, subdivision ~~13~~ 3:

(1) criteria for determining which computer processed returns are selected for audit;

(2) criteria for determining which returns are selected for an in-depth audit; and

(3) criteria for determining which accounts receivable balances below a stated amount are written off or canceled.

Subd. 3. [CONFIDENTIAL DATA ~~ON-INDIVIDUALS;-PROTECTED NONPUBLIC-DATA~~.] (a) Except as provided in paragraph (b), the name or existence of an informer, informer letters, and other unsolicited data, in whatever form, given to the department of revenue by a person, other than the data subject, who informs that a specific taxpayer is not or may not be in compliance with tax laws, or nontax laws administered by the department of revenue, including laws not listed in section 270B.01, subdivision 8, are confidential data ~~on-individuals-or-protected nonpublic-data~~ as defined in section 13.02, ~~subdivisions~~ subdivision 3 ~~and-13~~.

(b) Data under paragraph (a) may be disclosed with the consent of the informer or upon a written finding by a court that the information provided by the informer was false and that there is evidence that the information was provided in bad faith. This subdivision does not alter disclosure responsibilities or obligations under the rules of criminal procedure.

Subd. 4. [PUBLIC DATA.] Information required to be filed by exempt individuals, corporations, organizations, estates, and trusts under section 290.05, subdivisions 1 and 4, is public data ~~on-individuals-or-public-data-not-on-individuals~~, as

defined in section 13.02, ~~subdivisions~~ subdivision 14 ~~and 15~~. The commissioner may publish a list of organizations exempt from taxation under section 290.05, except that the name or address of any contributor to any organization that is or was exempt, or that has applied for tax exempt status, or any other information that could not be disclosed under section 6104 of the Internal Revenue Code of 1986, as amended through December 31, 1988, is classified as private data ~~on individuals or nonpublic data~~ as defined in section 13.02, ~~subdivisions 9 and~~ subdivision 12.

Subd. 5. [MAINTAINING CLASSIFICATIONS.] Notwithstanding section 13.03, subdivision 7, returns and return information retain the classification designated under this chapter. Notwithstanding sections 13.03, subdivision 8, and 13.10, data classified under subdivision 3 and department of revenue data classified under this chapter as ~~nonpublic data, protected nonpublic data,~~ private data ~~on individuals,~~ or confidential data ~~on individuals~~ remain so classified.

Subd. 6. [CLIENT LISTS; THIRD-PARTY BULK FILERS.] Client lists required under section 290.92, subdivision 30, are classified as private data ~~on individuals or nonpublic data~~, as defined in section 13.02, ~~subdivisions 9 and~~ subdivision 12.

Sec. 172. Minnesota Statutes 1998, section 272.115, subdivision 1, is amended to read:

Subdivision 1. [REQUIREMENT.] Except as otherwise provided in subdivision 5, whenever any real estate is sold for a consideration in excess of $1,000, whether by warranty deed, quitclaim deed, contract for deed or any other method of sale, the grantor, grantee or the legal agent of either shall file a certificate of value with the county auditor in the county in which the property is located when the deed or other document is presented for recording. ~~Contract~~ Contracts for ~~deeds~~ deed are subject to recording under section 507.235, subdivision 1. Value shall, in the case of any deed not a gift, be the amount of the full actual consideration thereof, paid or to be paid, including the amount of any lien or liens assumed. The items and value of personal property transferred with the real

property must be listed and deducted from the sale price. The certificate of value shall include the classification to which the property belongs for the purpose of determining the fair market value of the property. The certificate shall include financing terms and conditions of the sale which are necessary to determine the actual, present value of the sale price for purposes of the sales ratio study. The commissioner of revenue shall promulgate administrative rules specifying the financing terms and conditions which must be included on the certificate. Pursuant to the authority of the commissioner of revenue in section 270.066, the certificate of value must include the social security number or the federal employer identification number of the grantors and grantees. The identification numbers of the grantors and grantees are private data ~~on individuals or nonpublic data~~ as defined in section 13.02, ~~subdivisions 9 and~~ subdivision 12, but, notwithstanding that section, the private ~~or nonpublic~~ data may be disclosed to the commissioner of revenue for purposes of tax administration.

Sec. 173. Minnesota Statutes 1998, section 295.57, subdivision 2, is amended to read:

Subd. 2. [ACCESS TO RECORDS.] For purposes of administering the taxes imposed by sections 295.50 to 295.59, the commissioner may access patients' records that contain billing or other financial information without prior consent from the patients. The data collected is classified as private ~~or nonpublic~~ data as defined in section 13.02, subdivision 12.

Sec. 174. Minnesota Statutes 1998, section 299A.61, subdivision 2, is amended to read:

Subd. 2. [DATA ON MEMBERS.] Data that identify individuals or businesses as members of the criminal alert network, including names, addresses, telephone and fax numbers, are private data ~~on individuals or nonpublic data~~, as defined in section 13.02, subdivision 9 ~~or~~ 12.

Sec. 175. Minnesota Statutes 1998, section 299F.095, is amended to read:

299F.095 [POWERS AND DUTIES OF FIRE DEPARTMENT.]

To the extent feasible, given the amount of funds and training available, the local fire department shall:

(1) mail or otherwise distribute hazardous substance notification report forms to employers within the jurisdiction of the fire department except for those employers for whom an inspection has been arranged or employers from whom a hazardous substance notification is considered not necessary by the fire department;

(2) retain and evaluate each hazardous substance notification report and notification of significant change submitted by each employer until the employer's workplace ceases to exist or the fire department determines retention of the hazardous substance notification report is no longer necessary;

(3) develop for fire department use appropriate fire and emergency procedures for the hazardous substance risks of each workplace based on the information received;

(4) investigate suspected violations of sections 299F.091 to 299F.099, and issue appropriate orders for compliance; and

(5) provide available material safety data sheets and hazardous substance notification reports at the request of other emergency response personnel.

Data collected under sections 299F.091 to 299F.099 is ~~nonpublic~~ private data not on individuals within the meaning of section 13.02, subdivision 9 12.

Sec. 176. Minnesota Statutes 1998, section 299F.096, subdivision 1, is amended to read:

Subdivision 1. [~~NONPUBLIC~~ PRIVATE DATA NOT ON INDIVIDUALS.] Before a fire department and emergency response personnel may have access to information received under section 299F.094, the department shall establish security procedures to prevent unauthorized use or disclosure of ~~nonpublic~~ private data not on individuals. ~~Nonpublic~~ Private data not on individuals must be made available in an emergency to emergency response personnel. No liability results under sections 299F.091 to 299F.099 with respect to disclosure of ~~nonpublic~~ private data not on individuals, if emergency response personnel, in response

to an emergency, reasonably determine that the use or disclosure of the data is necessary to expedite medical services or to protect persons from imminent danger. As soon as practicable after disclosure of ~~nonpublic~~ private data not on individuals is made by emergency response personnel, the circumstances necessitating the disclosure and the actual or estimated extent of the disclosure must be described in writing by the personnel and provided to the employer.

Sec. 177. Minnesota Statutes 1998, section 299J.13, subdivision 3, is amended to read:

Subd. 3. [CLASSIFICATION OF DATA.] Except as otherwise provided in this subdivision, data obtained from any person under subdivision 1 or 2 is public data as defined in section 13.02. Upon certification by the subject of the data that the data relates to sales figures, processes, or methods of production unique to that person, or information that would tend to affect adversely the competitive position of that person, the director shall classify the data as ~~private or nonpublic~~ data as defined in section 13.02. Notwithstanding any other law to the contrary, data classified as private ~~or nonpublic~~ under this subdivision may be disclosed when relevant in any proceeding under sections 299J.01 to 299J.17, or to other public agencies concerned with the implementation of sections 299J.01 to 299J.17.

Section ... Minnesota Statutes 1998, section 326.3382, subdivision 3, is amended to read:

Subd. 3. [PROOF OF INSURANCE.] (a) No license may be issued to a private detective or protective agent applicant until the applicant has complied with the requirements in this subdivision.

(b) The applicant shall execute a surety bond to the state of Minnesota in the penal sum of $10,000 and file it with the board. The surety bond must be executed by a company authorized to do business in the state of Minnesota, must name the applicant as principal, and must state that the applicant and each of the applicant's employees shall faithfully observe all of the laws of Minnesota and of the United States and shall pay

all damages suffered by any person by reason of a violation of law by the applicant or by the commission of any willful and malicious wrong by the applicant in the course of business.

(c) The applicant shall furnish proof, acceptable to the board, of the applicant's ability to respond in damages for liability on account of accidents or wrongdoings arising out of the ownership and operation of a private detective or protective agent business. Compliance with paragraph (d), (e), or (f) is satisfactory proof of financial responsibility for purposes of this paragraph.

(d) The applicant may file with the board a certificate of insurance demonstrating coverage for general liability, completed operations, and personal injury. Personal injury insurance must include coverage for:

(1) false arrest, detention, imprisonment, and malicious prosecution;

(2) libel, slander, defamation, and violation of rights of privacy; and

(3) wrongful entry, eviction, and other invasion of rights of private occupancy.

The certificate must provide that the insurance may not be modified or canceled unless 30 days prior notice is given to the board.

(e) The applicant may file with the board an annual net worth statement, signed by a licensed certified public accountant, evidencing that the applicant has a net worth of at least the following:

(1) for an applicant with no employees, $10,000;

(2) for an applicant with one to ten employees, $15,000;

(3) for an applicant with 11 to 25 employees, $25,000;

(4) for an applicant with 26 to 50 employees, $50,000; or

(5) for an applicant with 51 or more employees, $100,000.

Data indicating with which of the above requirements an applicant must comply is public data. The contents of the net worth statement are private data ~~on individuals or nonpublic data~~, as defined in section 13.02.

(f) The applicant may file with the board an irrevocable letter of credit from a financial institution acceptable to the board in the amount listed in the appropriate category in paragraph (e).

Sec. 178. Minnesota Statutes 1998, section 363.061, subdivision 2, is amended to read:

Subd. 2. [ACCESS TO OPEN FILES.] (a) Except as otherwise provided in this subdivision, human rights investigative data contained in an open case file are confidential data ~~on individuals or protected nonpublic data~~, as defined in section 13.02, subdivision 3. The name and address of the charging party and respondent, factual basis of the allegations, and the statute under which the action is brought are private data ~~on individuals or nonpublic data~~, as defined in section 13.02, subdivision 12, but are accessible to the charging party and the respondent.

(b) After making a finding of probable cause, the commissioner may make human rights investigative data contained in an open case file accessible to a person, government agency, or the public if access will aid the investigative and enforcement process.

Sec. 179. Minnesota Statutes 1998, section 363.061, subdivision 3, is amended to read:

Subd. 3. [ACCESS TO CLOSED FILES.] (a) Except as otherwise provided in this subdivision, human rights investigative data contained in a closed case file are private data ~~on individuals or nonpublic data~~, as defined in section 13.02, subdivision 12. The name and address of the charging party and respondent, factual basis of the allegations, the statute under which the action is brought, the part of the summary of the investigation that does not contain identifying data on a person other than the complainant or respondent, and the commissioner's memorandum determining whether probable cause has been shown are public data.

(b) The commissioner may make human rights investigative data contained in a closed case file inaccessible to the

charging party or the respondent in order to protect medical or other security interests of the parties or third persons.

Sec. 180. Minnesota Statutes 1998, section 383B.217, subdivision 7, is amended to read:

Subd. 7. [PURCHASES AND MARKETING.] (a) Contracting and purchasing made on behalf of the Hennepin county medical center of goods, materials, supplies, equipment and contracted services shall comply with sections 383B.141 to 383B.151.

(b) Notwithstanding section 471.705, the county board on behalf of the medical center may meet in closed session to discuss and take action on specific products or services that are in direct competition with other providers of goods or services in the public or private sector, if disclosure of information pertaining to those matters would clearly harm the competitive position of the medical center.

(c) The medical center shall inform the county board when there are matters that are appropriate for discussion or action under paragraph (b). The county administrator or the administrator's designee shall give the board an opinion on the propriety of discussion or action under paragraph (b) for each of the matters. The county board may, by a majority vote in a public meeting, decide to hold a closed meeting under paragraph (b). The purpose, time, and place of the meeting must be announced at a public meeting. A written roll of members present at a closed meeting must be made available to the public after the closed meeting. The proceedings of a closed meeting must be tape recorded at the expense of the county board and be preserved for not less than five years after the meeting. The data on the tape are ~~nonpublic~~ private data ~~under~~ not on individuals, as defined in section 13.02, subdivision 9 12, until two years after the meeting. A contract entered into by the county board at a meeting held on behalf of the medical center is subject to section 471.345. All bids and any related materials that are considered at the meeting must be retained for a period of not less than five years. After the expiration of the term of any contract entered into pursuant to this

subdivision or a period of two years, whichever is less, the contract, the bids, and any related materials are public data. The contract, the bids, and any related materials are subject to review by the state auditor at any time.

(d) Data concerning specific products or services that are in direct competition with other providers of goods or services in the public or private sector are trade secret information for purposes of section 13.37, to the extent disclosure of information pertaining to the matters would clearly harm the competitive position of the medical center. The data are trade secret information for the term of the contract or a two-year period, whichever is less.

(e) This subdivision applies to the medical center, ambulatory health centers, or other clinics authorized under section 383B.219, as well as any other organization, association, partnership, or corporation authorized by Hennepin county under section 144.581.

Sec. 181. Minnesota Statutes 1998, section 383B.225, subdivision 6, is amended to read:

Subd. 6. [INVESTIGATION PROCEDURE.] (a) Upon notification of the death of any person, as provided in subdivision 5, the county medical examiner or a designee may proceed to the body, take charge of it, and order, when necessary, that there be no interference with the body or the scene of death. Any person violating the order of the examiner is guilty of a misdemeanor. The examiner or the examiner's designee shall make inquiry regarding the cause and manner of death and, in cases that fall under the medical examiner's jurisdiction, prepare written findings together with the report of death and its circumstances, which shall be filed in the office of the examiner. When it appears that death may have resulted from a criminal act and that further investigation is advisable, a copy of the report shall be transmitted to the county attorney. The examiner may take possession of any or all property of the deceased, mark it for identification, and make an inventory. The examiner shall take possession of all articles useful in

establishing the cause of death, mark them for identification and retain them securely until they are no longer needed for evidence or investigation. The examiner shall release any property or articles needed for any criminal investigation to law enforcement officers conducting the investigation. When a reasonable basis exists for not releasing property or articles to law enforcement officers, the examiner shall consult with the county attorney. If the county attorney determines that a reasonable basis exists for not releasing the property or articles, the examiner may retain them. The property or articles shall be returned immediately upon completion of the investigation. When the property or articles are no longer needed for the investigation or as evidence, the examiner shall release the property or articles to the person or persons entitled to them. Notwithstanding any other law to the contrary, when personal property of more than nominal value of a decedent has come into the possession of the examiner, and is not used for a criminal investigation or as evidence, and has not been otherwise released as provided in this subdivision, the name of the decedent shall be filed with the district court, together with a copy of the inventory of the decedent's property. At that time, an examination of the records of the court shall be made to determine whether a will has been admitted to probate or an administration has been commenced. Personal property, including wearing apparel, may be released to or for the spouse or any blood relative or personal representative of the decedent or to the person accepting financial responsibility for burial of the decedent. If property has not been released by the examiner and no will has been admitted to probate or administration commenced within six months after death, the examiner may sell the property, other than firearms or other weapons, of a deceased person at a public auction upon notice and in a manner as the court may direct. The examiner shall release all firearms of a deceased person to the law enforcement agency handling the investigation and shall cause to be destroyed any other weapon of a deceased person that

is not released to or claimed by a decedent's spouse, blood relative, or representative of the estate, or other person who proves lawful ownership. If the name of the decedent is not known, the examiner shall inventory the property of the decedent and after six months may sell the property at a public auction. The examiner shall be allowed reasonable expenses for the care and sale of the property and shall deposit the net proceeds of the sale with the county administrator, or the administrator's designee, in the name of the decedent, if known. If the decedent is not known, the examiner shall establish a means of identifying the property of the decedent with the unknown decedent and shall deposit the net proceeds of the sale with the county administrator, or a designee, so, that, if the unknown decedent's identity is established within six years, the proceeds can be properly distributed. In either case, duplicate receipts shall be provided to the examiner, one of which shall be filed with the court, the other of which shall be retained in the office of the examiner. If a representative shall qualify within six years from the time of deposit, the county administrator, or a designee, shall pay the amount of the deposit to the representative upon order of the court. If no order is made within six years, the proceeds of the sale shall become a part of the general revenue of the county.

(b) For the purposes of this section, health-related records or data on a decedent, except health data defined in section 13.38, whose death is being investigated under this section, whether the records or data are recorded or unrecorded, including but not limited to those concerning medical, surgical, psychiatric, psychological, chemical dependency, or any other consultation, diagnosis, or treatment, including medical imaging, shall be made promptly available to the medical examiner, upon the medical examiner's written request, by a person having custody of, possession of, access to, or knowledge of the records or data. In cases involving a stillborn infant or the death of a fetus or an infant less than one year of age, the records on the decedent's mother shall also be made promptly

available to the medical examiner. The medical examiner shall pay the reasonable costs of copies of records or data provided to the medical examiner under this section. Data collected or created pursuant to this subdivision relating to any psychiatric, psychological, or mental health consultation with, diagnosis of, or treatment of the decedent whose death is being investigated shall remain confidential or protected nonpublic data, as defined in section 13.02, subdivision 3, except that the medical examiner's report may contain a summary of such data.

(c) After investigating deaths of unautopsied persons who are to be cremated, the medical examiner shall give approval for cremation and shall record such approval by affixing the examiner's signature on the reverse side of the deceased person's death certificate.

(d) The medical examiner has the power to subpoena any and all documents, records, and papers deemed useful in the investigation of a death.

Sec. 182. Minnesota Statutes 1998, section 390.11, subdivision 7, is amended to read:

Subd. 7. [REPORTS.] (a) Deaths of the types described in this section must be promptly reported for investigation to the coroner by the law enforcement officer, attending physician, mortician, person in charge of the public institutions referred to in subdivision 1, or other person with knowledge of the death.

(b) For the purposes of this section, health-related records or data on a decedent, except health data defined in section 13.38, whose death is being investigated under this section, whether the records or data are recorded or unrecorded, including but not limited to those concerning medical, surgical, psychiatric, psychological, or any other consultation, diagnosis, or treatment, including medical imaging, shall be made promptly available to the coroner, upon the coroner's written request, by a person having custody of, possession of, access to, or knowledge of the records or data. The coroner shall pay the reasonable costs of copies of records or data provided to the coroner under this section. Data collected or

created pursuant to this subdivision relating to any psychiatric, psychological, or mental health consultation with, diagnosis of, or treatment of the decedent whose death is being investigated shall remain confidential or protected nonpublic data, as defined in section 13.02, subdivision 3, except that the coroner's report may contain a summary of such data.

Sec. 183. Minnesota Statutes 1998, section 390.32, subdivision 6, is amended to read:

Subd. 6. [REPORT OF DEATHS.] (a) Deaths of the types described in this section must be promptly reported for investigation to the sheriff by the attending physician, mortician, person in charge of the public institutions referred to in subdivision 1, or other person having knowledge of the death.

(b) For the purposes of this section, health-related records or data on a decedent, except health data as defined in section 13.38, whose death is being investigated under this section, whether the records or data are recorded or unrecorded, including but not limited to those concerning medical, surgical, psychiatric, psychological, or any other consultation, diagnosis, or treatment, including medical imaging, shall be made promptly available to the medical examiner, upon the medical examiner's written request, by a person having custody of, possession of, access to, or knowledge of the records or data. The medical examiner shall pay the reasonable costs of copies of records or data provided to the medical examiner under this section. Data collected or created pursuant to this subdivision relating to any psychiatric, psychological, or mental health consultation with, diagnosis of, or treatment of the decedent whose death is being investigated shall remain confidential ~~or protected nonpublic~~ data, as defined in section 13.02, subdivision 3, except that the medical examiner's report may contain a summary of such data.

Sec. 184. Minnesota Statutes 1998, section 400.08, subdivision 4, is amended to read:

Subd. 4. [COLLECTION.] (a) The rates and charges may be

billed and collected in a manner the board shall determine.

(b) On or before October 15 in each year, the county board may certify to the county auditor all unpaid outstanding charges, and a description of the lands against which the charges arose. It shall be the duty of the county auditor, upon order of the county board, to extend the assessments, with interest not to exceed the interest rate provided for in section 279.03, subdivision 1, upon the tax rolls of the county for the taxes of the year in which the assessment is filed. For each year ending October 15 the assessment with interest shall be carried into the tax becoming due and payable in January of the following year, and shall be enforced and collected in the manner provided for the enforcement and collection of real property taxes in accordance with the provisions of the laws of the state. The charges, if not paid, shall become delinquent and be subject to the same penalties and the same rate of interest as the taxes under the general laws of the state.

(c) In addition to any other manner of collection that may be established under paragraph (a), a county may:

(1) require as a condition of a license issued under section 115A.93 that the licensee collect service charges established under subdivision 3 from solid waste generators for remittal to the county; and

(2) audit a licensed collector's records of the charges collected under clause (1) and the amount of waste collected only to the extent necessary to ensure that all charges required to be collected are remitted to the county.

Data received under clause (2) are private ~~or nonpublic~~ data as defined in section 13.02, subdivision 9~~, or~~ 12.

Sec. 185. Minnesota Statutes 1998, section 446A.11, subdivision 11, is amended to read:

Subd. 11. [FINANCIAL INFORMATION.] Financial information, including credit reports, financial statements and net worth calculations, received or prepared by the authority regarding an authority loan, financial assistance, or insurance is private data ~~with regard to data on individuals~~ as defined in section

13.02, subdivision 12 ~~and nonpublic data with regard to data not on individuals as defined in section 13.02, subdivision 9~~.

Sec. 186. Minnesota Statutes 1998, section 473.598, subdivision 4, is amended to read:

Subd. 4. [TREATMENT OF DATA.] (a) Except as specifically provided in this subdivision, all data received by the commission or council in the course of its negotiations and acquisition of the basketball and hockey arena is public data.

(b) The commission may keep confidential data received or prepared by its accountants or counsel for purposes of negotiations with existing or potential lessees of the basketball and hockey arena. That data ~~shall be~~ is confidential data ~~on individuals~~ under section 13.02, subdivision 3~~, or protected nonpublic data under section 13.02, subdivision 13, as the case may be~~, unless the commission determines that public release of the data would advance the negotiations, or until the potential lessees have executed agreements with the commission or the negotiations are unfavorably concluded.

(c) The following data ~~shall be~~ is private data ~~on individuals~~ under section 13.02, subdivision 12~~, or nonpublic data under section 13.02, subdivision 9, as the case may be~~:

(1) data received by the commission or council from the present lessees or potential lessees of the basketball and hockey arena which if made public would, due to the disclosure, permit a competitive economic advantage to other persons;

(2) data relating to affiliated entities of the parties referred to in subdivision 3 which is not relevant to the due diligence and economic feasibility study referred to under subdivision 3; and

(3) data on individuals which is not relevant to the finances of the basketball and hockey arena or useful to demonstrate the financial ability of the potential lessees of the arena to perform their agreements with the commission.

(d) For purposes of this subdivision, the terms "commission" and "council" include their members and employees, accountants, counsel, and consultants and the firm of

independent certified public accountants to be engaged under subdivision 2.

(e) Notwithstanding the exceptions in this subdivision, summary data which demonstrates the financial ability of the lessees and potential lessees of the basketball and hockey arena to perform their obligations under agreements with the commission and data which relates in any way to the value of the basketball and hockey arena and the amount by which the owners' investment in the arena, including debt obligations, exceeds the commission's payments to and assumption of the owners' debt obligations, ~~shall be~~ is public data.

Sec. 187. Minnesota Statutes 1998, section 473.6671, subdivision 3, is amended to read:

Subd. 3. [DUE DILIGENCE CONDITIONS.] (a) Before the commission may issue the revenue bonds described in subdivision 1, the commission must receive, in form and substance satisfactory to the commission:

(1) a report of audit of the commission's financial records for the fiscal year most recently ended or, if this is not yet available, a report for the preceding year, prepared by a nationally recognized firm of certified public accountants, showing that the net revenues received that year, computed as the gross receipts less any refunds of rates, fees, charges, and rentals for airport and air navigation facilities and service, and less the aggregate amount of current expenses, paid or accrued, of operation and maintenance of property and carrying on the commission's business and activities, equaled or exceeded the maximum amount of then outstanding bonds of the commission and interest thereon to become due in any future fiscal year;

(2) a written report, prepared by an independent, nationally recognized consultant on airport management and financing engaged by the commission, on the financial condition of the airline corporation, and any corporations selected by the commission and affiliated with the corporation by common ownership, projecting available revenues of the airline corporation at least sufficient during each year of the term of

the proposed revenue bonds to pay when due all financial obligations of the airline corporation under the revenue agreements and leases described in subdivision 1 and stating the factors on which the projection is based; and

(3) a written report prepared by a nationally recognized consultant on airport management and financing, projecting available revenues of the commission at least sufficient during each year of the term of the proposed revenue bonds to pay all principal and interest when due on the revenue bonds, and stating the estimates of air traffic, rate increases, inflation, and other factors on which the projection is based.

(b) Business plans, financial statements, customer lists, and market and feasibility studies provided to the consultant or the commission by the airline company or a related company under paragraph (a), are ~~nonpublic~~ private data as defined in section 13.02, subdivision 9 12.

Sec. 188. Minnesota Statutes 1998, section 473.843, subdivision 4, is amended to read:

Subd. 4. [EXCHANGE OF INFORMATION.] Notwithstanding the provisions of section 116.075, the agency may provide the commissioner of revenue with the information necessary for the enforcement of this section. Information disclosed in a return filed under this section is public information. Information exchanged between the commissioner and the agency is public unless the information is of the type determined to be for the confidential use of the agency under section 116.075 or is trade secret information classified under section 13.37. Information obtained in the course of an audit by the department of revenue is private ~~or nonpublic~~ data to the extent that it would not be directly divulged in a return.

Sec. 189. Minnesota Statutes 1998, section 475.55, subdivision 6, is amended to read:

Subd. 6. [REGISTRATION DATA PRIVATE.] All information contained in any register maintained by a municipality or by a corporate registrar with respect to the ownership of municipal obligations ~~is nonpublic data as defined in section 13.02,~~

~~subdivision 9,~~ or private data ~~on individuals~~ as defined in section 13.02, subdivision 12. The information is not public and is accessible only to the individual or entity that is the subject of it, except if disclosure:

(1) is necessary for the performance of the duties of the municipality or the registrar;

(2) is requested by an authorized representative of the state commissioner of revenue or attorney general or of the commissioner of internal revenue of the United States for the purpose of determining the applicability of a tax;

(3) is required under section 13.03, subdivision 4; or

(4) is requested at any time by the corporate trust department of a bank or trust company acting as a tender agent pursuant to documents executed at the time of issuance of the obligations to purchase obligations described in section 475.54, subdivision 5a, or obligations to which a tender option has been attached in connection with the performance of such person's duties as tender agent, or purchaser of the obligations.

A municipality or its agent may use the information in a register for purposes of offering obligations under a bond reinvestment program.

Sec. 190. Minnesota Statutes 1998, section 583.29, is amended to read:

583.29 [PRIVATE DATA.]

All data regarding the finances of individual debtors and creditors created, collected, and maintained by the mediators or the director are classified as private data ~~on individuals~~ under section 13.02, subdivision 12, ~~or nonpublic data under section 13.02, subdivision~~ 9.

Sec. 191. Minnesota Statutes 1998, section 626.558, subdivision 3, is amended to read:

Subd. 3. [INFORMATION SHARING.] (a) The local welfare agency may make available to the case consultation committee or subcommittee, all records collected and maintained by the agency under section 626.556 and in connection with case consultation. A case consultation committee or subcommittee member may share

information acquired in the member's professional capacity with the committee or subcommittee to assist in case consultation.

(b) Case consultation committee or subcommittee members must annually sign a data sharing agreement, approved by the commissioner of human services, assuring compliance with chapter 13. ~~Not-public~~ Private data, as defined by section 13.02, subdivision ~~8a~~ 12, and confidential data, as defined by section 13.02, subdivision 3, may be shared with members appointed to the committee or subcommittee in connection with an individual case when the members have signed the data sharing agreement.

(c) All data acquired by the case consultation committee or subcommittee in exercising case consultation duties, are confidential as defined in section 13.02, subdivision 3, and shall not be disclosed except to the extent necessary to perform case consultation, and shall not be subject to subpoena or discovery.

(d) No members of a case consultation committee or subcommittee meeting shall disclose what transpired at a case consultation meeting, except to the extent necessary to carry out the case consultation plan. The proceedings and records of the case consultation meeting are not subject to discovery, and may not be introduced into evidence in any civil or criminal action against a professional or local welfare agency arising out of the matter or matters which are the subject of consideration of the case consultation meeting. Information, documents, or records otherwise available from original sources are not immune from discovery or use in any civil or criminal action merely because they were presented during a case consultation meeting. Any person who presented information before the consultation committee or subcommittee or who is a member shall not be prevented from testifying as to matters within the person's knowledge. However, in a civil or criminal proceeding a person shall not be questioned about the person's presentation of information before the case consultation committee or subcommittee or about opinions formed as a result of the case consultation meetings.

A person who violates this subdivision is subject to the civil remedies and penalties provided under chapter 13.

Sec. 192. [REPEALER.]

Minnesota Statutes 1998, sections 13.02, subdivisions 4, 8a, 9, 13, and 15; 13.10, subdivision 1; 13.528; 13.54, subdivisions 3 and 5; and 13.77, subdivision 2; are repealed.

APPENDIX 6

Summary Statement of Current Information Policy Principles Underlying Minnesota Statutes

SOME CURRENT PUBLIC INFORMATION POLICY PRINCIPLES

I. Sources of Public Policy.

The following description of current public information policy principles is drawn from the three primary sources of policy established by the Minnesota legislature. Those sources are:

A. The "Official Records Act," Minnesota Statutes Section 15.17, first enacted in 1941;

B. The "Minnesota Government Data Practices Act," Minnesota Statutes Chapter 13, first enacted in 1974; and

C. The "Records Management Act," Minnesota Statutes Sections 138.163 through 138.225, first enacted in 1947.

All three of these sources of public policy recognize that government records and data are kept in paper, electronic and other physical forms.

Contrary to popular belief, the "Data Practices Act" is not just a "data privacy" law. The Data Practices Act combines and accommodates policy principles that relate to:

* public access to government data;

* fair information handling practices for data about individuals; and

* effectiveness for government entities in their handling of government data.

II. Public Policy Principles Drawn from the "Official Records Act."

* Government entities are required to keep at least some records to document their official activities.

* Government records can be copied and kept in a variety of physical forms.

* Certified copies of government records have the same evidentiary weight and effect as original records.

* Custodians of government records are required to deliver those records to their successors in office.

III. Public Policy Principles Drawn from the "Records Management Act."

* Not all government records meet the definition of a government record that is subject to the regulation by the Records Management Act.

* Government Records subject to the Records Management Act include records maintained in electronic form.

* An "official" government record cannot be destroyed or otherwise disposed of unless the government entity holding the record complies with the Records Management Act.

* Some governmental entities, including the Minnesota Supreme Court and the University of Minnesota, are not subject to the requirements of the Records Management Act.

IV. Public Policy Principles Drawn from the "Minnesota Government Data Practices Act."

A. Principles Relating to Public Access, i.e. "freedom of information."

* Government data include all data as long as the data exist in some physical form, including computerized, video, paper, microfilm and so forth.

* All government data are presumed to be accessible by the public unless the legislature has enacted a statute or federal law provides that certain data are not public because they are classified as private, confidential, nonpublic or protected nonpublic.

* Public government data must be kept and arranged so that they are easily accessible by the public.

* Government entities are required to establish procedures to insure that requests for access to government data are complied with promptly and appropriately.

* The public has a right to inspect, i.e. physically look at, public government data and cannot be charged any fee for the inspection.

* If the public requests copies of public data or asks that government data be transmitted electronically, the government entity may charge the actual costs of providing the copies or electronically transmitting the data.

* If the public requests a copy of an entire set of government data or a substantial and discretion portion of an entire set of government data in an instance where the government data has commercial value, the government entity may, in addition to charging for copies, charge an additional fee to recover its costs for developing the system of data.

* With the exception of computer software programs or components of software programs, the issue of whether government entities can claim and enforce intellectual property rights in public government data, and therefore limit public use of public data, is the subject of considerable dispute.

B. Principles Relating to Fair Information Practices, i.e. "data privacy."

* Collection and storage of data on individuals and use and dissemination of not public data on individuals are limited to purposes authorized by the federal government, the legislature and local governing bodies.

* Government entities cannot share private or confidential data about individuals with one another unless there is statutory or federal legal authority to do so.

* In most instances when a government entity wants to collect private or confidential data from an individual, the individual must be told why the data are being requested; whether the data must be provided; what the consequences are of providing the data; what uses will be made of the data; and, the identity of other entities to which the data will be disseminated.

* Not public data collected from an individual can be collected, stored, used and disseminated only for those purposes communicated to the individual at the time the data were collected unless the individual gives informed consent, the commissioner of administration approves or the legislature changes the rules.

* Individuals have the right to inspect or to receive copies of public or private data about them immediately or within five to ten days of a request to gain access.

* Government entities are required to assure that data on individuals are accurate, complete and current.

* Individuals are given the right to challenge the accuracy or completeness of public or private data that a government entity is maintaining about them.

C. Other Principles.

* The right of the public to gain access to public government data and rights of data subjects are enforced in most instances by suing government entities.

* Members of the public and government entities can request advisory opinions from the commissioner of administration about a variety of issues.

* The judiciary is not subject to the Data Practices Act. On issues of information, the judiciary is subject to certain specific legislative enactments and, on the issue of public access to records of the judiciary, is subject to rules promulgated by the supreme court.

APPENDIX 7

Draft Legislation Based on Task Force's Revised Policy Recommendations

Minnesota Statutes Section 13.03, subdivision 2, is amended to read as follows:

Subd. 2. **Procedures.** The responsible authority in every state agency, political subdivision, and statewide system shall establish procedures, consistent with this chapter, to insure that requests for government data are received and complied with in an appropriate and prompt manner. The responsible authority must prepare public access procedures in written form and update them no later than August 1 of each year if necessary, to reflect any changes in personnel or circumstances that might affect public access to government data. The responsible authority must make copies of the written public access procedures easily available to the public by distributing free copies of the procedures to the public or by posting a copy of the procedures in a conspicuous place within the agency that is easily accessible to the public. 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.

(Recommendation #3.)

Minnesota Statutes Section 13.03, subdivision 3, is amended to read as follows:

Subd. 3. **Request for Access to data.** Upon request to a responsible authority or designee, a person shall be permitted to inspect and copy public

government data at reasonable times and places, and, upon request, shall be informed of the data's meaning. If a person requests access for the purpose of inspection, the responsible authority may not assess a charge or require the requesting person to pay a fee to inspect data. For purposes of this section, "inspection" includes but is not limited to the visual inspection of paper and similar types of government data and, in the case of data stored in electronic form and available in an on-line fashion to personnel of the entity, on-line access to the data by the public and the ability ~~to~~ print copies of or down load the data being accessed. Any communication and terminal costs of on-line access for the purpose of inspection shall be borne by the public. The responsible authority or designee shall provide copies of public data upon request. If a person requests copies ~~or electronic transmittal of the data to the person~~, the responsible authority may require the requesting person to pay only the ~~actual~~ marginal costs of ~~searching for and retrieving government data, including the costs of employee time, and for making, certifying, compiling, and electronically~~ providing the copies, unless a statute clearly authorizes assessment of any additional fee, of the data ~~or the data~~, but may not charge for separating public from not public data. For purposes of this section, "marginal cost" means only the actual cost of making the copies themselves excluding any costs associated with labor, overhead or development costs. If the responsible authority or designee is not able to provide copies at the time a request is made, copies shall be supplied as soon as reasonably possible.

~~When a request under this subdivision involves any person's receipt of~~

~~copies of public government data that has commercial value and is a substantial and discrete portion of or an entire formula, pattern, compilation, program, device, method, technique, process, database, or system developed with a significant expenditure of public funds by the agency, the responsible authority may charge a reasonable fee for the information in addition to the costs of making, certifying, and compiling the copies. Any fee charged must be clearly demonstrated by the agency to relate to the actual development costs of the information. The responsible authority, upon the request of any person, shall provide sufficient documentation to explain and justify the fee being charged.~~ The responsible authority of a state agency, political subdivision or statewide system, which maintains public government data in a computer storage medium, shall provide to any person making a request under this section, a copy of any public data contained in that medium, in electronic form, if the government agency can reasonably make the copy or have a copy made. The agency may require the requesting person to pay the marginal cost of providing the copy.

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 inform the requesting person of the determination either orally at the time of the request, or in writing as soon after that time as possible, and shall cite the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based. Upon the request of any person denied access to data, the responsible authority or designee shall certify in writing that the request has been denied and cite the specific statutory section, temporary

classification, or specific provision of federal law upon which the denial was based.

(Recommendations #4, 5, 7 & 15.)

Minnesota Statutes Section 13.03, subdivision 5, is amended to read as follows:

Subd. 5. **Copyright ~~or patent of computer program~~ of government data.** ~~Nothing in this chapter or any other statute shall be construed to prevent a~~ A state agency, statewide system, or political subdivision ~~from acquiring~~ may acquire a copyright or patent for a computer software program or components of a program created by that government agency. In the event that a government agency does acquire a patent or copyright to a computer software program or component of a program, the data shall be treated as trade secret information pursuant to section 13.37. No state agency, political subdivision or statewide system shall copyright any other types of government data unless the state agency, political subdivision or statewide system has obtained legislative approval for the copyright.

(Recommendation #6.)

Minnesota Statutes Section 13.04, subdivision 2, is amended to read as follows:

Subd. 2. **Information required to be given individual.** An individual asked to supply private or confidential data concerning the individual 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 the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from 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. This requirement shall not apply when an individual is asked to supply investigative data, pursuant to section 13.82, subdivision 5, to a law enforcement office. When an individual is asked to supply educational data, as defined in Section 13.32, this requirement is fulfilled if, at the beginning of each academic year, the responsible authority provides to the individual a complete notice as prescribed by the subdivision that covers the possible data collection instances that may occur during the academic year. No further notice will be required except in those instances when data are being collected from a student and the data may be used to discipline the student. When an individual is asked to supply personnel data, as defined in Section 13.43, this requirement is fulfilled if, at the beginning of the employment relationship, which includes the application process, the responsible authority provides to the individual a complete notice as prescribed by this subdivision that covers the possible data collection instances that may occur during the course of the employment relationship. No further notice will be required except in those instances when data are being collected from an employee and the data may be used to discipline the employee.

(Recommendation #10.)

Minnesota Statutes Section 13.04, subdivision 3, is amended to read as follows:

Subd. 3. **Access to data by individual.** Upon request to a responsible authority, an individual shall be informed whether the individual is the subject of stored data on individuals, and whether it is classified as public, private or confidential. Upon further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge and, if desired, 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 that individual 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~~ ten days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. ~~If unable to comply with the request within that time, the responsible authority 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.~~

(Recommendation #11.)

Minnesota Statutes Section 13.05, subdivision 3, is amended to read as follows:

Subd. 3. General standards for collection and storage. Collection, ~~and~~ storage and use of all data on individuals ~~and the use and dissemination of private and confidential data on individuals shall be~~ is limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government. Dissemination of private and confidential data on individuals is limited to that necessary for the administration and management of programs specifically authorized by the legislature or mandated by the federal government.

(Recommendation #9.)

Minnesota Statutes Section 13.05, is amended by adding a subdivision to read as follows:

Subd. 11. **Utilization of Surveillance Devices.**

(a) For purposes of this section, "surveillance device" means any computer, video or audio recording equipment, caller identification features, thermal imaging devices, or similar electronic devices and purchases of surveillance services that are used to acquire data, recorded images and similar types of information.

(b) The responsible authority in any state agency, political subdivision, or statewide system shall, in a form specified by the Commissioner of Administration, report to the Commissioner that the agency, subdivision or

system has acquired any form of surveillance device. This reporting requirement shall not apply to agencies which carry on a law enforcement function, as described in Section 13.82, subdivision 1, if there is a compelling public safety reason not to provide public notice of the acquisition of surveillance devices.

(Recommendation #12.)

Minnesota Statutes Section 13.05, is amended by adding a subdivision to read as follows:

Subd. 12. **Monitoring of Citizens.**

(a) Unless specifically authorized by statute to do so, personnel of state agencies, political subdivisions and statewide systems shall not require citizens to identify themselves or to state a reason for or have to justify a request to gain access to public government data. A citizen may be asked to provide certain identifying information for the sole purpose of facilitating access to the data.

(Recommendation #13.)

Minnesota Statutes Section 13.05, 1998, is amended by adding a subdivision to read as follows:

Subd. 13. **Data Practices Compliance Officer.** No later than December 1, 1999, each responsible authority or other appropriate authority in every government entity shall appoint or designate an individual, who is an employee of the government entity, to act as the entity's data practices compliance officer. It shall be the duty of this officer to assure that the government entity complies with

this Chapter. No later than January 15, 2000, the responsible authority or other appropriate authority in every government entity shall report, in a form to be prescribed by the commissioner, about the individual designated to be the data practices compliance officer. Whenever the government entity makes a change in the individual assigned to the position of data practices compliance officer, it shall report that change to the commissioner. Each biennial budget session, the commissioner shall report to the appropriate finance committees of the legislature, on the progress of government entities in assuring compliance with this requirement.

(Recommendation # 17.)

Minnesota Statutes Section 13.05, 1998, is amended by adding a subdivision to read as follows:

Subd. 14. **Privatization.** In any instance in which a government entity determines to outsource any of its functions to a private person, the government entity shall include in the outsourcing contract, contractual terms that make it clear that all of the data created collected, received, stored, used, maintained or disseminated by the private person, in performing the outsourced functions, shall be subject to the requirements of this chapter and that the private person must act in conformity with those requirements as if it were a government entity.

(Recommendation #22)

Minnesota Statutes Section 13.072, 1998, subdivision 2 is amended to read as follows:

Subd. 2. Effect. Opinions issued by the commissioner under this section are ~~not~~ binding on the state agency, statewide system, or political subdivision whose data is the subject of the opinion, ~~but~~ and must be given deference by a court in a proceeding involving the data. The commissioner may bring an action in district court on behalf of a citizen to compel a government entity to act in conformance with the commissioner's opinion. A government entity may bring an action in district court to seek a declaratory judgement that the commissioner's opinion is not correct and need not be followed. The commissioner shall arrange for public dissemination of opinions issued under this section. This section does not preclude a person from bringing any other action under this chapter or other law in addition to or instead of requesting a written opinion. A state agency, statewide system, political subdivision, or person that acts in conformity with a written opinion of the commissioner is not liable for compensatory or exemplary damages or awards of attorneys fees in actions under section 13.08 or for a penalty under section 13.09.

(Recommendation #20.)

Minnesota Statutes Section 13.073, 1998, is amended by adding a subdivision to read as follows:

Subd. 6. **Preparation of Model Policies and Procedures.** The commissioner shall, in consultation with affected government entities, prepare

model policies and procedures to assist government entities in compliance with the requirements of this chapter that relate to public access to government data and rights of subjects of data. Upon completion of a model for any governmental level, the commissioner shall offer that model for formal adoption by that level of government. Government entities are free to adopts or reject the model offered by the commissioner. A government entity that adopt the commissioner's model shall communicate that adoption to the commissioner in a form prescribed by the commissioner. Any government entity choosing not to adopt the commissioner's model shall so inform the commissioner and provide a copy of the policies and procedures prepared and used by that government entity.

(Recommendation #16.)

Minnesota Statutes Section 13.08, subdivision 1, is amended to read as follows:

Subd. 1. **Complaints. Action for damages.** Notwithstanding section 466.03, a political subdivision, responsible authority, statewide system, or state agency which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents 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 this chapter. Any person who believes that a government entity is not in compliance with this chapter may file a complaint with the commissioner [or director]. The commissioner [or director] shall specify the form of the complaint. The commissioner [or director] shall conduct an investigation to determine whether or not the complaint is valid. If the commissioner [or director determines the complaint is not valid, the commissioner [or director] shall dismiss the complaint and so inform the person who filed the complaint and the government entity that was the subject of the complaint. If the commissioner [or director] determines the complaint is valid, the commissioner [or director] may take any of the following actions to resolve the complaint. The commissioner [or director] may attempt to resolve the matter informally or if both parties are willing, refer the matter to an alternative dispute resolution process and use the services of either the office of dispute resolution or the office of administrative hearings to arbitrate or mediate the dispute. The commissioner [or director] may choose to refer the complaint to the office of administrative hearings for formal resolution.

A complaint referred by the commissioner [or director] shall be heard as a contested case, except that the report of the administrative law judge shall be binding on all parties to the proceeding and if appropriate shall be implemented by an order as provided for below. The hearing shall be conducted at a place designated by the commissioner [or director], within the county where the alleged violation occurred or where the complainant resides or has a principal place of

business. The hearing shall be conducted in accordance with sections 14.57 to 14.62, and is subject to appeal in accordance with sections 14.63 to 14.68.

The administrative law judge shall make findings of fact and conclusions of law, and if the administrative law judge finds that the government entity has violated this chapter, the administrative law judge shall issue an order directing the government entity to take such affirmative action as in the judgment of the administrative law judge will effectuate the purposes of this chapter. The order shall be a final decision of the commissioner [or director]. If the administrative law judge determines that the government entity's failure to comply with this chapter has caused damage to the complainant, the administrative law judge may also order the government entity to pay any actual damages including damages for mental anguish and suffering.

(Recommendation #21.)

Minnesota Statutes Section 15.17, subdivision 1, is amended to read as follows:

Subd. 1. **Must be kept.** All officers and agencies of the state, counties, cities, towns, school districts, municipal subdivisions or corporations, or other public authorities or political entities within the state, hereinafter "public officer," shall make and preserve all records necessary to a full and accurate knowledge of their official activities. Government records may be produced in the form of computerized records. All government records shall be made on a physical medium of a quality to insure permanent records. Every public officer is

empowered to reproduce records if the records are not deemed to be of permanent or archival value by the commissioner of administration and the records disposition panel under section 138.17. The public officer is empowered to reproduce these records by any photographic, photostatic, microphotographic, optical disk imaging system, microfilming, electronic, or other reproduction method that clearly and accurately reproduces the records. If a record is deemed to be of permanent or archival value, any reproduction of the record must meet archival standards specified by the Minnesota historical society provided, however, that this section does not prohibit the use of nonerasable optical imaging systems for the preservation of archival records without the preservation of paper or microfilm copies. Each public officer may order that those photographs, photostats, microphotographs, microfilms, optical images, or other reproductions, be substituted for the originals of them. The public officer may direct the destruction or sale for salvage or other disposition of the originals from which they were made, in accordance with the disposition requirements of section 138.17. Photographs, photostats, microphotographs, microfilms, optical images, or other reproductions are for all purposes deemed the original recording of the papers, books, documents, and records reproduced when so ordered by any public officer and are admissible as evidence in all courts and proceedings of every kind. A facsimile or exemplified or certified copy of a photograph, photostat, microphotograph, microfilm, optical image, or other reproduction, or an

enlargement or reduction of it, has the same effect and weight as evidence as would a certified or exemplified copy of the original.

(Recommendation #1.)

Minnesota Statutes Section 15.17, subdivision 2, is amended to read as follows:

Subd. 2. **Responsibility for records.** The chief administrative officer of each public agency shall be responsible for the preservation and care of the agency's government records, which shall include written or printed books, papers, letters, contracts, documents, maps, plans, computer based data, and other records made or received pursuant to law or in connection with the transaction of public business. It shall be the duty of each agency, and of its chief administrative officer, to carefully protect and preserve government records from deterioration, mutilation, loss, or destruction. Records or record books may be repaired, renovated, or rebound when necessary to preserve them properly.

(Recommendation #1.)

Minnesota Statutes Section 138.17, subdivision 7, is amended to read as follows:

Subd. 7. **Records management program.** A records management program for the application of efficient and economical management methods to the creation, utilization, maintenance, retention, preservation, and disposal of official records shall be administered by the commissioner of administration with

assistance from the director of the historical society. The state records center which stores and services state records not in state archives shall be administered by the commissioner of administration. The commissioner of administration is empowered to (1) establish standards, procedures, and techniques for effective management of government records, (2) make continuing surveys of paper work operations, and (3) recommend improvements in current records management practices including the use of space, equipment, and supplies employed in creating, maintaining, preserving and disposing of government records. It shall be the duty of the head of each state agency and the governing body of each county, municipality, and other subdivision of government to cooperate with the commissioner in conducting surveys and to establish and maintain an active, continuing program for the economical and efficient management of the records of each agency, county, municipality, or other subdivision of government. When requested by the commissioner, public officials shall assist in the preparation of an inclusive inventory of records in their custody, to which shall be attached a schedule, approved by the head of the governmental unit or agency having custody of the records and the commissioner, establishing a time period for the retention or disposal of each series of records. When the schedule is unanimously approved by the records disposition panel, the head of the governmental unit or agency having custody of the records may dispose of the type of records listed in the schedule at a time and in a manner prescribed in the schedule for particular records which were created after the approval. A list of records disposed of pursuant to this subdivision shall be forwarded to the commissioner and the

archivist by the head of the governmental unit or agency. The archivist shall maintain a list of all records destroyed.

(Recommendation #2.)

Minnesota Statutes Section 138.17, subdivision 8, is amended to read as follows:

Subd. 8. **Emergency records preservation.** In light of the danger of nuclear or natural disaster, the commissioner of administration, with the assistance of the director of the historical society, shall establish and maintain a program for the selection and preservation of public records considered essential to the operation of government and to the protection of the rights and interests of persons, and shall make or cause to be made preservation duplicates or designated as preservation duplicates existing copies of such essential public records. Preservation duplicates shall be durable, accurate, complete, and clear, and such duplicates reproduced by photographic or other process which accurately reproduces and forms a durable medium for so reproducing the original shall have the same force and effect for all purposes as the original record whether the original record is in existence or not. A transcript, exemplification, or certified copy of such preservation duplicate shall be deemed for all purposes to be a transcript, exemplification, or certified copy of the original record. Such preservation duplicates shall be preserved in the place and manner of safekeeping prescribed by the commissioner.

(Recommendation #2.)

Proposed amendment to state departments appropriations bill:

(Recommendation #2.)

Language for a Task Force recommendations bill or the state departments appropriations bill.

Section ____. [Office of Freedom of Information and Privacy Created.] There is hereby created the office of freedom of information and privacy. This office is an agency in the executive branch managed by an executive director. The office shall provide leadership and direction for freedom of information, data practices and privacy policy in Minnesota.

(Recommendation #19.)

Section ____. [Transfer of duties.] All duties currently assigned to the commissioner of administration under Minnesota Statutes Chapter 13 are hereby transferred to the office of privacy and freedom of information. Personnel assigned to the public information policy analysis division of the department of administration and the funds appropriated for that division are hereby transferred to the office of privacy and freedom of information.

(Recommendation #19.)

APPENDIX 8

Analysis of Budgetary Implications of Task Force Recommendations

STATE BUDGET AND OTHER FINANCIAL IMPLICATIONS OF IPTF RECOMMENDATIONS

INTRODUCTION

This document contains an analysis of the Task Force's recommendations that have budgetary implications. In this document, the Task Force recommendations are identified by their current number and by a brief narrative description. This document contains three sections.

The first section identifies recommendations that have a financial impact that is either negligible or is difficult to estimate because of a variety of factors. These factors include the nature of the recommendation itself and the diversity of practices among the approximately 2000 government entities that are subject to the Data Practices Act.

The second section discusses a number of Task Force recommendations that have a positive financial impact. If implemented, costs of enforcing the Act and/or complying with the Act will be reduced. The positive financial impact of each recommendation is discussed.

Third, a number of the Task Force's recommendations involve either direction to state or semi-state agencies to conduct certain activities, involve the reorganization of certain organizations or, in one case, the creation of an entirely new agency. The activities associated with implementing the recommendations and estimates of the budgetary implications of those activities are provided with some level of detail.

1. Task Force Recommendations With Negligible or Difficult to Measure Financial Impact.

These recommendations include:

4. Limiting cost of copies to marginal cost.
5. On-line inspection of data is free.
6. No copyright without legislative approval.
7. Receiving copies of data in electronic form.
10. Change to Tennessen Warnings for educational and personnel data.
12. Reports on acquisitions of surveillance devices.
13. Limits on monitoring citizen access to data.
14. Changing obsolete/inconsistent language.
15. Repeal of authority for government entities to recover development costs.
22. Assuring access to privatized data.

The financial impact of these recommended changes is highly dependent on factors such as: the extent to which government agencies have already prepared written materials relating to policies and procedures for compliance; the ease or difficulty of altering

existing Tennessen Warnings to accommodate the modified requirement; the extent to which government agencies are using current statutory authority to recover development costs; and, the extent to which the delay in receiving copyright authority or disapproval of a request for authority from the Legislature would affect a government entity's use of copyright as a revenue source. Without very extensive research, including a survey of all government entities to determine how their current practices relate to these recommendations, it is difficult to compute a dollar figure on the financial impact of these particular Task Force recommendations.

2. Task Force Recommendations with a Positive Financial Impact.

These recommendations include:

2. Greater assistance to government entities to comply with records management requirements.
10. Change to the Tennessen Warning requirement for personnel and educational data.
11. Change to a straight ten day response time for requests by individuals to access data about themselves.
16. Department of Administration to do model policies and procedures.
18. Department of Administration appropriated sufficient resources to do training program.
19. Independent Office of Privacy and Freedom of Information.
20. Commissioner of Administration or Director's opinions made binding and authority given to Commissioner or Director to enforce opinions in court.
21. Amend remedies provisions of Data Practices Act.

The potentially positive financial impact of these recommendations would be felt by both government agencies, and therefore taxpayers, and by citizen themselves. The positive impacts include the following:

2. Currently, all government entities struggle with issues of records management and increasingly with issues of electronic records management. Although some assistance is available from both the Department of Administration and the Historical Society, the resources currently allocated for this assistance is far below what it has been at times in the past and does not meet demand or anticipated demand. The chief positive financial impact of this recommendation would make it less costly for government entities to comply with the Records Management Act through increased use of model retention schedules and electronic filing capabilities. Some potentially negative legal effects of improper records management that have dollar implications could be avoided.

10. These changes to the Tennessen Warning requirement would reduce the cost to educational entities and employers of complying with the requirement. This cost reduction would primarily come about because government entities would only have to provide Tennessen Warnings at the beginning of academic years and

employment relationships and would not have to provide Tennessen Warnings in those countless other instances when they ask individuals to provide educational or personnel data.

11. This change to the response time would eliminate the requirement that agencies, if they are not going to respond within five days of the individual's request, must send a written communication to the individual stating that the agency will take more than five days.

16. Currently, there are somewhere between 11 and 20 actions, policies and procedures that are required to be done by each government entity in order to comply with the Data Practices Act. This requirement must also be seen in the context of the reality that each entity should, once it has actually done these things, find some way to keep those actions and documents as part of the institutional memory of the entity. If the entity fails on its ability to preserve its institutional memory, it will find itself having to go back to step one and take the actions and do the work necessary to create the policies and procedures over again.

    Implementation of this recommendation would save all government entities the costs of preparing policies and procedures and eliminate the costs associated with loss of institutional memory. The Department of Administration would become a formal centralized source of policy and procedural compliance information. (The word "formal" is used in the previous sentence because the Department already provides informal services of this kind.) In addition, clear assignment of this role to the Department would save the costs of having other organizations, such as the Association of Minnesota Counties and state agencies, generate model compliance policies and procedures. This recommendation also offers the potentially positive impact of assuring that whatever models are developed will reflect the current reality of the law.

18. As the Task Force has discussed on a number of occasions, unnecessary disputes and unnecessary actions often stem from the simple fact that government entities are often not up to speed on what is actually required by the Act. Adequate funding for the training program, which is authorized in Minnesota Statutes Section 13.073, would take a significant step toward resolving unnecessary disputes, provide model policies and procedures to government entities to assist them in compliance and begin creation and institutional support for experts across state and local government who are available to also help resolve disputes and to make it easier for government agencies to comply. In the long run, compliance will make it less likely that citizens will have to sue to enforce their rights, thereby avoiding litigation costs for citizens and government entities. Implementation of the Section 13.073 training program would also create a central source for information and research about information policy issues and could therefore reduce the necessity for similar research to be done by the Legislature and other government bodies.

19. The primary positive financial impact of this recommendation would be in the area of reduced court costs, attorney's fees or costs and legal damages. An office empowered to resolve disputes would make it less likely that government entities would put such heavy emphasis on involving their attorneys in all aspects of government data issues. This recommendation would also have a positive financial impact on citizens because, instead of hiring attorneys to help them enforce their rights, they would be able to take disputes to this office. In most instances they would be able to represent themselves.

20. Knowledge that the Commissioner's opinions are binding and enforceable by the Commissioner could make it more likely that government agencies would follow them. By doing so, they would not incur the costs of attorney's fees, court costs and sometimes awards of attorney's fees to citizens that result from deciding not to follow an opinion by the Commissioner. The primary positive financial impact that would result from this recommendation would flow to citizens because they would no longer be required to file the legal actions necessary to uphold the findings made in a Commissioner's opinion.

21. The positive financial impact of this recommendation would be felt by citizens. In the current scheme for enforcement that the Legislature has devised for Chapter 13, disputes are resolved by citizens suing the government. Recourse to alternative dispute resolution mechanisms will reduce litigation costs for both citizens and entities.

3. Task Force Recommendations with Readily Available Cost Estimates.

The Task Force's recommendations in the area of improved enforcement have distinct financial implications. The following is a description and a discussion of each of those recommendations and an estimate of the associated costs. It should be emphasized that the intent of these estimates is to give "ball park" figures and to explain the detail associated with those figures.

Activities of the nature described in most of the Task Force recommendations are staff intensive. Most of the costs of actually carrying out the activity involve having staff available to do the work.

To provide some context for these recommendations of the Task Force, current staff allocated by the Department of Administration to carry out activities related to the Data Practices Act and the Records Management Act, in the Information Policy Analysis Division (IPA), is two and one half professionals, a full-time office manager and a division director. (This reflects the recent retirement of a full-time staff member, who was the only staff assigned to professional records management activities.) The budget for the Information Policy Analysis Division is currently $501,000 for each fiscal year of the biennium. The IPA budget request for 2000-2001 is the same. The Department of Administration has also requested $500,000 for each year of the biennium to fund recommendations of the Information Policy Task Force.

Detailed budget implications for each of the Task Force's recommendations that have substantial financial implications are as follows. The personnel costs shown below are computed by taking the annual salary cost of an employee and adding an additional 20% to reflect the cost of employee benefits. This is the standard way actual personnel costs of state employees are computed.

2. Department of Administration and Historical Society to provide more assistance on records management.

A. Associated Activities.

In the current statutory language dealing with records management, the Commissioner of Administration is given a central role in developing and implementing a records management program for the state and all of its political subdivisions. Some assistance for that effort would come from staff of the Archives Division of the Historical Society because of the Archive's interest in and expertise with records and archival issues.

The current record management system is a totally paper-based system in which government agencies submit the paper documents that are required to be approved to Administration and the Historical Society. The filings are reviewed for technical compliance and forwarded for approval to the Records Disposition Panel, which is the only body authorized by statute to approve the disposal of government records kept in any and all forms. Some of the activities that are contemplated in this recommendation include: replacing this paper-based system; streamlining the process of action on records disposition requests; preserving records in the event of disasters; researching legal and technical issues associated with the use of and disposition of electronic records; providing up-to-date information and assistance on records management issues; and, helping government agencies at all levels to deal effectively and legally with the emergence of electronic records.

B. Budget Implication: Estimated $374,800 per year.

This figure reflects the following:

1. Seven Professional staff, including:

1	State Planner Intermediate	$38,600
1	Management Analyst	$36,000
1	State Planner Principal (supervisor)	$54,000
2	Archivist professional staff	$108,000
1	Systems analyst/data base coordinator	$60,000
1	Clerk Typist II	$26,400
	TOTAL Personnel Costs:	$323,000

2. Office furniture, equipment including computers, space and other general operating expenses is an average cost of $7,400 per staff member or about $51,800 per year for operating costs.

3. Each government entity to prepare written procedures detailing public access and make those procedures available to the public.

A. Associated Activities.

Procedures describing how the public gets access to data in any entity subject to the Data Practices Act have been required since 1981. Any agency who has not prepared those procedures in writing would now be required to do so. All agencies would be required to make copies of those procedures available to the public. Except for those agencies that are large and/or have complex operations, these procedures are not particularly difficult to prepare.

B. Budget Implications: Difficult to estimate.

The most significant cost would fall on those agencies which have never prepared these procedures at all. It is difficult to estimate how many agencies are in this condition. The publication requirement would yield varying costs depending on how the recommendation, when turned into statutory language, actually defined publication. If publication was to be defined to include posting of the procedures at the principle offices of the entity, then the publication costs would be negligible. The dollar impact of this recommendation on individual entities would be lessened if Recommendation Number 16 becomes reality.

8. Legislature, when authorizing funding for electronic services or for electronic access to information, to include funding to allow those services and that information to be delivered to those who cannot afford or do not have the skills necessary to participate electronically.

A. Associated Activities.

This recommendation is intended to draw the Legislature's attention to the fact that authorizing the delivery of services and information electronically will, unless they directly deal with the issue, produce information and service "have and have nots," or more correctly, classes of citizens who will either easily or less easily be able to take advantage of these new means of delivering services or information.

B. Budget Implications: Difficult to estimate.

It is very difficult to provide any precise estimate of the budget implications of the concept implicit in this recommendation. It depends heavily on whether or not the Legislature would ultimately agree that there is a "haves and have nots" problem and whether or not they want to do anything about it. The decisions that the Legislature could take to deal with this problem, if there is agreement that it is a problem, occupy a very wide range of possibilities including such things as making sure every household in Minnesota is equipped with computer technology and increasing library budgets so that libraries can act as service and information centers for individuals without ready access to computer technology. Those options and others present a wide range of budgetary implications.

16. Department of Administration to do model policies and procedures.

A. Associated Activities.

Activities associated with this recommendation include: collecting existing policies and procedures from each type of government entity subject to the Data Practices Act; preparing proposed models based on that collection; reviewing and revising those models with assistance from representatives of the various governmental sectors; preparation, printing and distribution of the final versions of the models; posting of the models on the Department's web site; and, training government entities on implementation and use of the models.

B. Budget Implication: None.

The activities associated with this recommendation can be done with the existing staff and dollars currently appropriated to IPA. (However, this assumes that IPA's current budget request for same level funding will be approved in the '99 session.) To make this recommendation both cost and policy effective, it would be helpful if any legislation drafted to implement would include language to the effect that the models are legally required to be followed or some similar way of assuring that the work of the Department of Administration will not be in vain.

17. Each government entity to designate a "Data Practices Compliance Officer."

A. Associated Activities.

All government entities would be required to: specifically designate an individual to be their Compliance Office; report on who has been

designated to the Department of Administration; and, update their reports as needed when there are changes to the Compliance Officer.

B. Budget Implication: Estimated $35,000 the first year and $5,000 each year thereafter.

The first year estimates reflect a cost of the reporting requirement for each government entity subject to the Act at $10.00 per entity for the actual correspondence to the Department of Administration to report the initial designation. The additional $15,000 in the first year would be for the Department of Administration to process filings, to put them on a data base and to do reminder letters and other follow-up activities to assure that reporting is as complete as follows. The $5,000 in each additional year is the estimated costs for government entities to report any changes to the Department and for the Department to maintain and up-to-date data base of Compliance Officers.

18. Appropriation of sufficient resources to the Department of Administration to implement and administer the training program authorized by Minnesota Statutes Section 13.073.

A. Associated Activities.

The training program authorized by Section 13.073 authorizes the Commissioner of Administration, if she chooses, to perform the following activities: develop a basic training component, including actual training and associated materials, about information policy laws and deliver that component to all public employees; develop and deliver sector specific training to deal with information policy issues within a service area which could be either governmental entities such as cities or counties or functional areas such as law enforcement or human services; identify and train individuals who will become sector or functional area information policy experts; work with various government agencies to assist in the delivery of compliance related information using on-line inquiry and response, telephone hot lines and other forms of technical assistance; and, establish the capability to conduct policy analysis and support for the examination of information policy issues.

B. Budget Implication: Estimated $350,000 the first year and $250,000 each year thereafter.

Development of the basic training and sector specific components of the training program would produce a first year expense, estimated at $100,000. This money would be used to prepare training materials and the means to deliver them, including professionally produced videotapes, printed materials, on-line training materials, audiotapes, and computer

based materials including discs and down load capabilities. The $100,000 figure is derived from consultation with professionals who deliver training as a business. It reflects their expert advice that materials, such as professionally done training videos, may cost in the $50,000 range. Development of these materials in the first year, delivery of the materials in the first and subsequent years would be the responsibility of four professionals and a support staff person. As illustrated in the discussion of Recommendation 2 above, personnel costs range from $30,000 to $60,000 per year, including benefits, for appropriate personnel. This activity would be staffed by four professionals, one of whom would be a supervisor, and one support staff. In addition to the supervising professional, other professional staff would include two management analysts principal (or comparable) and an experienced public information officer. The cost of those employees including space rental, equipment computers and other associated support is estimated at $250,000 per year.

19. Transfer Department of Administration duties to an Office of Privacy and Freedom of Information and give that office additional duties to handle citizen complaints.

A. Associated Activities.

This recommendation should be read to include all the current duties of the Commissioner, including the training program described above. Under this recommendation, additional duties of investigating citizen complaints and resolving those complaints by use of ADR methods or by court action would be added to the duties of the Office.

B. Budget Implication: Estimated additional $200,000 per year.

Some portion of the cost of investigating citizen complaints could be absorbed by the existing appropriation to IPA. Additional funds for training would be necessary as described in Recommendation 19 above. Additional professional staff would be needed to carry out any investigations of an extensive and detailed nature. ADR services could be provided either by personnel of the Office itself (with appropriate training), by hiring professional arbitrators or mediators, or by contracting for ADR services with organizations such as the Office of Dispute Resolution (ODR) or the Office of Administrative Hearings (OAH). Per hour costs of ADR services range from $60 at the ODR to $89 at the OAH to more than $100 from some experienced arbitrators and mediators. Any staff hired would have the associated support costs, as described in Recommendation 2, B. 2. above. Taking complaints to court on behalf of citizens would entail paying the Attorney General's billable rate for legal services or, in instances where a state agency was being complained about, paying outside counsel to represent the Office. The $200,000 figure

estimated above is intended to cover both ADR and court related costs. It is difficult to estimate just how many complaints would be processed each year. The number of complaints would determine the actual costs of ADR services and legal costs of enforcement actions.

20. Make Commissioner of Administration [or Director] opinions binding and authorize the Commissioner [or Director] to enforce opinions in court.

A. Associated Activities.

The Commissioner [or Director if Recommendation 19 were implemented] would prepare opinions in more of a legalistic fashion in anticipation of using them as the basis for an enforcement action. Bringing legal actions against other government agencies would require the Commissioner [or Director] to acquire and pay for legal services from the Attorney General's office or, in actions against other state agencies, services from outside counsel.

B. Budget Implication: Estimated $125,000 per year.

Costs associated with this estimate include: an estimated annual cost of $60,000, including operating costs, to hire a legally trained staff person to research and review opinions drafted by other staff; and $65,000 in estimated attorney costs for either AG or outside legal services.

21. Amending remedies provisions of Data Practices Act.

A. Associated Activities.

The intent of this recommendation is to make it easier for citizens and government entities to resolve disputes by making available to them an alternative dispute resolution system. The major activity associated with this recommendation would be the establishment and operation of the dispute resolution system.

B. Budget Implication: Approximately $150,000.

The activities associated with this recommendation are similar to Recommendation 19. The costs and basis for those costs are as described in Recommendation 19. The $50,000 difference is a function of no need for dollars to pay for AG legal services or outside legal counsel.

APPENDIX 9

Written Comments on Drafts of the Task Force's Report

(Not available electronically.)

MINNESOTA DEPARTMENT OF
TRADE AND ECONOMIC DEVELOPMENT

500 Metro Square
121 7th Place East
Saint Paul, Minnesota 55101-2146 USA

October 13, 1995

Mr. Thomas Satre
Government Information Access Council
Information Policy Office
Minnesota Department of Administration
320 Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Tom:

Thank you for the opportunity to be part of your "October Group" and to have input into the deliberations of the Government Information Access Council and the Information Access Principles Working Group as they consider policy on intellectual property developed by state agencies.

As a publisher of more than twelve million pages of information each year this office is most concerned with the issue of copyright for state publications. In that context, I want in this letter to present, very briefly, the basis for this office's belief that copyright of such publications is not only congruent with the goal of public accessibility of information, but is, indeed, the best (I personally would say the only) way of ensuring that accessibility.

In developing and publishing its works, this office seeks to remedy what economists call the problem of information costs. That is, it is expensive - in terms not only of money but also time, effort, expertise and lost opportunity - for an individual or business to acquire information on the start-up, operation or expansion of a business in Minnesota. These costs exist because information is imperfect (it is not always available in one place and lacks elements of timeliness, accuracy, comprehensiveness, understandability and the like) and because information is asymmetrical (some may have more or easier access to information because of location, resources, expertise and the like). As a matter of fairness in the provision of information to all citizens, and as a matter of the state itself broadening the universe of individuals and firms that can contribute to economic growth, the state through our office produces publications which seek to make that information "more perfect" and more "symmetrical."

Let me say here as an aside that (as you and I have discussed in another context) if these imperfections and costs did not exist, then it is a settled economic principle that the most efficient way of providing such information would be "rationing by price," that is, by the exclusively commercial production and distribution of information. But it is precisely because the market is imperfect that the state chooses to allocate resources to information production and distribution so that the costs to users is reduced.

An Equal Opportunity Employer

(612) 297-1291
(800) 657-3858
TTY/TDD (612) 282-6142
FAX (612) 296-1290

One major element of the effort to make information more perfect is this office's use of outside, private sector experts who contribute their expertise *pro bono* as authors or contributors to publications. This ensures a degree of quality greater than might be expected from a staff produced work and heightens the public's credence in the work itself and in the state's ability to deliver useful materials. That use of experts also has the purely economic benefit to the state of production efficiency. In using contributed expertise this office eliminates its own sunk costs of information collection and reduces the overall cost of putting the publication in the users' hands.

Copyright gives an incentive to these private contributors to provide their expertise to our publications without concern that the expertise and its expression will be appropriated for commercial use by another through reproduction or use in derivative works. I am convinced that our ability to attract such contributed expertise would be lost (not merely compromised) in the absence of the ability to copyright.

Copyright also offers an additional means of information perfection by providing a reasonable way of controlling the integrity of the text and the credibility of the state as its developer and publisher. As you know, we have had situations in the past where others have reproduced or used our material in derivative works in ways which are not accurate, are out of date or which draw conclusions not supported by the text. While nothing will stop the dedicated infringer, copyright does allow this office to review requests for use to ensure that the public's confidence in information on which they will be relying in making business decisions is preserved.

Likewise, copyright contributes to making information more symmetrical by ensuring that the supply of that information continues to be available from a public source, accessible to all, on an on-demand basis, and at no charge. To speak again in economic terms, not only is production efficiency advanced by copyright but allocational efficiency as well.

In short, I believe copyright not only preserves but increases access to our information without the distortions of commercial markets.

Best regards.

Sincerely,

Charles A. Schaffer
Director
Small Business Assistance Office
(612) 296-0617

CAS:mc

MINNESOTA DEPARTMENT OF
TRADE AND ECONOMIC DEVELOPMENT

500 Metro Square
121 7th Place East
Saint Paul, Minnesota 55101-2146 USA

October 23, 1995

Mr. Thomas Satre
Director
Government Information Access Council
Information Policy Office
Minnesota Department of Administration
320 Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Tom:

In my letter of October 13, I stated the basis in theory and practice for this office's position that copyright protection of its publications is the best way of ensuring continued public access to those publications. (A copy of that letter is attached.)

Here, as a supplement to that letter, I want to state three adverse consequences that, I believe, will result from the loss of the ability to copyright our publications.

* The problem of unintended consequences. Potential users of business information, like consumers of other products, very often seek that information from the first or most obvious source that they believe can provide that information. (That fact of consumer behavior is the reason why businesses take out large ads in the Yellow Pages.) Even after ten years of publishing our materials, this office is still often the second or third source from which information is sought. In the absence of copyright for our publications, a private firm with name recognition in the information market and substantial advertising capability could become that first source and could charge for material which would continue to remain free of charge from this office. The consumer responding to the economic rent of the private firm, would not know that the information was available at no-cost from this agency. No cost access would be reduced, if not lost, by the action which sought to increase that access.

* The diminution of fairness. The goal of all public policy should be what economists call "Pareto Optimality:" In short, no one should be made better off by action which makes another party worse off. A policy which denies government agencies copyright protection (protection sought to broaden access to all) effectively transfers a wealth producing asset to another party(ies) that, as noted above, may not share the goals of

no-cost access and broad dissemination. It is a mistake to believe that allowing such use of government data will result in an efficient market with attendant benefits to consumers. Making a market contesable (here by removing copyright as a barrier to entry) does not make the market competitive. Those firms which have the greatest market presence as current incumbents will secure the easiest ability-to-publish, and, with their existing economies of scale and scope, will effectively control the information.

* The possible corruption of a public good. It is important never to lose sight of that fact that the public does rely on our information in making life-changing decisions; decisions involving the expenditure of real personal assets of money, time, effort and opportunity. In producing and publishing its information this office makes a promise of fidelity to the public: that the information is timely, accurate, comprehensive, comprehensible, etc. In the absence of copyright this office will no longer be able to ensure that integrity of the information it has produced but which has been appropriated by others.

Sincerely,

Charles A. Schaffer
Director
Small Business Assistance Office
(612) 296-0617

CAS:mc

Attachment

city of
bloomington, minnesota

Anne

Legal Department 2215 W. Old Shakopee Rd. • Bloomington MN 55431-3096 • (612) 948-8753 • FAX: 948-8754 •
TDD: 948-8740 WRITER'S DIRECT DIAL NUMBER: 948-3886

December 30, 1998

Ms. Anne M. Barry
Commissioner
Minnesota Department of Health
85 East Seventh Street
St. Paul, MN 55101

Re: Draft Report of the Information Policy Task Force to the Minnesota Legislature

Dear Ms. Barry:

Thank you for this opportunity to respond to the Draft Report of the Information Policy Task Force. This letter addresses only one of the recommendations the Task Force is considering: the recommendation requiring government entities to acquire specific legislative authority to copyright.

Since 1974, the City of Bloomington has operated a cable television service to the public. The City's cable television station creates original news and entertainment segments and is one of the oldest public cable television stations in the state to do so. On a regular basis the City's cable television station produces programs with original artistic and entertainment content that is governed by agreements with artists and protected by copyright laws. Permission is granted by the City's Cable Administrator for use of these programs on a case-by-case basis, but the protection the copyright laws provide to such original programming is invaluable. Many requests for the cable programs and videos are from large commercial video companies that want to use segments of the program or video for private sector commercial projects.

If the Task Force's copyright recommendation is enacted into law, each session the City's Cable Administrator will be appearing before numerous legislative committees with long lists of cable programs and videos that need copyright protection. I cannot believe the Legislature will want to be burdened each session with hundreds of these requests. But there is even a greater concern regarding the Task Force proposal. Cable television programs created and produced in the months that the Legislature is not in session would be left unprotected until a bill is enacted in the next legislative session. The protection of the copyright must be immediate in order for it to be meaningful. In general, the Task Force's copyright proposal as written is inherently unworkable.

The City will actively oppose any legislative change to restrict its ability to copyright such original artistic programming. Further analysis by the Task Force regarding the impact of such a broad copyright restriction is in order. Cable television programming is only one example of the negative impact and burden such a broad restriction has on government operations.

Thank you for this opportunity to express the City of Bloomington's concern regarding the Task Force's copyright recommendation.

Very truly yours,

Greg Brooker

Greg Brooker
Associate City Attorney

cc: City Manager
Cable Administrator
Bloomington Legislative Delegation

KNUTSON, FLYNN, DEANS & OLSEN

PROFESSIONAL ASSOCIATION

1155 CENTRE POINTE DRIVE, SUITE 10
MENDOTA HEIGHTS, MINNESOTA 55120
TELEPHONE: (651) 222-2811 FAX: (651) 225-0600

TO: Members of the Information Policy Task Force

FROM: Thomas S. Deans
Legal Counsel Minnesota School Boards Association

RE: Comments Regarding Draft Report of the Information Policy Task Force

DATE: January 4, 1999

We have reviewed the proposed Draft Report of the Information Policy Task Force to the Minnesota Legislature (12/30/98). We are providing general comments and observations, but reserve the right to raise additional issues during legislative consideration after we have received further input from our members.

Recommendations That Relate to the Information Policy Principles

1. **Recommendation 3.** This proposed recommendation requires each government agency to "publish" in some form the procedures in effect in the agency. Our concern relates to the use of the word "publish" in the recommendation. We believe that the draft legislation amending Minnesota Statutes, Section 13.03, Subdivision 2, which allows posting to meet this requirement, to be a reasonable accommodation.

   We are going to discuss the issue of attorneys' fees below. However, let us use the provisions of this proposed change to reflect how technical application of the law could make school districts subject to large fee awards. The proposed amendments to Section 13.03, Subdivision 2 require the responsible authority to update the agency's procedures each year no later than August 1 to reflect any changes in personnel or circumstance that might affect public access to government data. If this timeline is inadvertently missed or

if a new employee is unaware of the requirement or the timeline, the school district or other public agency will be a target for individuals wishing to make a living by bringing such actions. The attorneys' fees provisions will change the entire dynamic of access to government data and will greatly increase the adversarial relationship between the public and government agencies.

2. **Recommendation 4.** We would oppose the provisions of this recommendation that would only allow the charging of marginal costs for the provision of government data. The recommendation totally overlooks the legislative history of Minnesota Statutes, Section 13.03, Subdivision 3. The marginal cost concept may work well for minor requests such as a copy of a particular document or a particular piece of information. However, it does not work at all well for massive data requests which require dozens or even hundreds of person hours of work to search for, retrieve, compile and provide the requested government data. One must be aware that in most school districts and other political subdivisions these duties are in addition to and on top of the duties for which the individual is otherwise employed. To the extent that an individual already has a full work day to complete the duties for which he or she was hired, these requests create a major burden. It is unclear in all cases that immediate compliance with this law should have a higher priority than compliance with all other statutory or other functions of the employee. This certainly will be regarded by all public agencies as an additional unfunded mandate. If the legislature wishes this to be a state priority, it should fund these additional local government costs.

   We would also point out to the Task Force that there are situations that arise when an individual or group is intending to harass or intimidate a public body. Massive data requests and continuing requests for similar but different information can cost a public body thousands of dollars and inefficient use of its employees. Under these provisions, the public body would be required to comply, could not charge for its time and would be subject to suit with attorneys' fees and the time of the harasser paid by the public body. This issue has been discussed over many sessions and we believe that these provisions would provide another measure to open public bodies to harassment and reprisal.

3. **Recommendation 6.** This recommendation relates to the prohibition of the copyright of government data by governmental entities. While we are not certain as to all the implication of this prohibition, we are certain that there are situations in which curricular materials, presentations and performances are developed by school districts which would be subject to copyright under the existing law. We believe that it would be unfair to allow a publisher or a promoter to be able to come in and request those materials, to rearrange them slightly and to copyright them itself. The public's interests would be converted to private gain with no remuneration to the entity that created it. Moreover, once it is copyrighted by that private entity, the public entity might no longer be able to use it without permission without paying fees and royalties. This concept has had

extensive legislative discussion in the past and should not be changed without certainty as to the implications.

The provision in the proposed amendment requiring specific legislature permission to copyright particular data would tend to clog the system and may result in the action coming too late after a private entity has beaten the governmental body to the punch.

The proposed amendments to Minnesota Statutes, Section 13.03, Subdivision 5 further do not recognize the distinction between the automatic existence of copyright protection upon creation of the work verses the protections afforded by registration of copyright ownership. The proposed amendment does not mesh well with federal law and will create more uncertainties and inconsistencies than it cures.

4. **Recommendation 7.** We are not certain whether this provision allowing the requester to determine the medium in which the data will be prepared would be abused. The public body apparently would only be able to charge for the cost of a disk or like object. However, it may have to send out to a private contractor to have the data put on that disk and could not recover those charges. For example, if the requester wished the information to be provided on a DVD and the district had no in-house method to do so, it would have to contract out at its own expense. This again is an unfunded mandate.

5. **Recommendation 10.** While we agree that the Tennessen Warning provisions need to be changed as they relate to employees and students, we do not believe that the proposed amendments will solve the problem. The key exception that creates the problem is the requirement that no further notice will be required except in those instances when the data may be used to discipline the student or the employee. When one is conducting inquiries which may relate to how an employee is carrying out his or her functions or the manner in which a student is behaving, one is never certain whether the answers will lead to discipline. These exceptions will lead to endless litigation as to whether students or employees have had their "rights" read to them at the appropriate time. We would remind the Task Force that we are not talking about criminal procedure. Discipline of an employee or discipline of a student is a civil matter. The employee or student does not have Miranda rights in a civil proceeding. Those two exceptions are completely unacceptable and do not solve the problems raised by the governmental units in the debate over these matters.

6. **Recommendation 11.** We agree that the timeframe for response will be better met by an increase from 5 to 10 days and we support that change. However, even the 10 days does not take into account massive requests for thousands of documents or for requests for documents that must be extensively redacted so that private governmental data on individuals other than the requestor is not released. We would ask the Task Force not to underestimate the time required to fulfill such requests. An exception should be added

that would allow the 10 days to be extended for a reasonable period of time in the event of large or complicated data requests.

7. **Recommendations 19 and 20.** We do not have a specific position on the creation of a separate, independent state Office of Privacy and Freedom of Information. However, giving either the Commissioner or the Director of that office authority to issue binding opinions and to enforce privacy matters against governmental entities by litigation will create an entirely new relationship. Many of the requests for opinions today are from political subdivisions or their attorneys. The requests for opinions deal with troublesome and unclear areas of the law and allow the political subdivision to get an answer upon which it may rely. The changes that are proposed will make the new office and all governmental entities in the state exist in an absolutely adversarial relationship. If one is a potential defendant, one does not work closely with and lay out one's questions to the plaintiff.

8. **Recommendation 21.** This recommendation relates to mandatory awards of attorneys' fees to parties bringing actions against the state and its political subdivisions. This provision alone will have a huge impact on the volume of litigation in this area. Moreover, it will foster an adversarial relationship between such entities and those seeking information from them. Matters that today would be easily resolved would have to be fought to the end to protect against unjust awards of attorneys' fees. Noncompliance will always be plead as an additional cause of action in any litigation against a government entity. We would recommend that the Task Force review the explosion in litigation under Section 1983 of the Civil Rights Act and under the special education laws as examples that should be avoided. We believe that this will have exactly the opposite result that the Task Force intends. It will breed another group of attorneys and individuals whose sole practice relates to preying on governmental entities that have made errors in the administration of what is conceded to be one of the most difficult and confusing areas of law.

Moreover, the proposed amendments to Section 13.08 by adding a new Subdivision 7 establishes an absolute liability standard in the law. If the governmental entity has failed in any manner to comply with the law and the person sues, the person will be absolutely entitled to attorneys' fees and amounts to compensate the citizen for the time spent in bringing the action. No harm of any sort must be demonstrated. We think that this standard is unprecedented and goes far beyond other attorneys' fees provisions in Minnesota law. The exception for litigation that is frivolous and without merit and basis in fact will not apply if there has been even an inadvertent violation of the law.

The standard for liability and the attorneys' fees and costs provisions are ill advised and will work against the public policy that the Task Force is attempting to create. When a request for a release of data involves a troublesome area, one is damned if you do and damned if you don't. If the entity releases and it shouldn't have, it will be sued. If the entity doesn't release and it should have, it will be sued. At least under the present law, a person must be harmed in order to recover. Under this proposal, a public body and its taxpayers will always be the losers.

We appreciate the work that the Task Force has done on these matters during the interim and feel that many of its recommendations are positive. However, those items that are set out above are very important considerations and will certainly impact our ability to support the legislation. We believe that we must strenuously oppose the attorneys' fees provisions, the standard of liability and the copying cost provisions.

Minnesota Department of Natural Resources
OFFICE OF THE COMMISSIONER
500 Lafayette Road
St. Paul, Minnesota 55155-4037

January 4, 1999

TO: Michele Ford
State Senate
306 Capitol

FR: Gail I. Lewellan
Assistant Commissioner
Human Resources and Legal Affairs

RE: Draft Report of the Information Policy Task Force
to the Minnesota Legislature

On Tuesday, December 29, 1998, the Department of Natural Resources received notice of the opportunity to comment on policy recommendations in the Draft Report of the Information Policy Task Force to the Minnesota Legislature. We were advised that the final version of the draft report would be available on the Internet on Wednesday, December 30, 1998. Written comments are requested by January 4, 1999, for review by the task force on Wednesday, January 6, 1999. This allows one business day for review and comment. "Brief verbal comments" at the January 6 meeting are also permitted.

A brief review of the 25 recommendations reveals major changes in longstanding information management practices with significant policy implications. The recommendations impose significant additional workloads on state agencies, and have significant fiscal impacts. Disturbingly, some recommendations evidence a lack of understanding of the current federal law of copyright, and indicate assumptions about the legal implications of agency practice which are simply false.

The recommendations are too significant to allow only one business day for a thoughtful written reply. Additionally, this comment period exists during a time when all but three state agencies have been advised that the terms of their current commissioners expire on the day the comments are due. Please let us know if the task force chooses in the future to provide a meaningful opportunity for comment on these important public policy issues.

CITY OF FRIDLEY

FRIDLEY MUNICIPAL CENTER • 6431 UNIVERSITY AVE. N.E. FRIDLEY, MN 55432 • (612) 571-3450 • FAX (612) 571-1287

January 4, 1998

Commissioner Anne Barry
Senator Don Betzold
Information Policy Task Force
306 Capitol Building
St. Paul, MN 55155

Dear Commissioner Barry and Senator Betzold,

We are writing on behalf of the Minnesota Clerks and Finance Officers Association Records Retention Task Force. Our responsibility is to update the State of Minnesota Records Retention Guidelines for Cities. We have been reviewing the Retention Guidelines for Cities for the past ten years. As part of our review, we also review data practices classifications.

It has just come to our attention today, that the Information Policy Task Force will hold a public hearing on January 6th to receive feedback on their Report/Recommendations to the Minnesota State Legislature for Amending the Data Practices Act. From the information we have received, we do not believe there has been an appropriate opportunity for input from local governments. In addition, we also believe there may be some unfunded mandates associated with the proposed legislation.

We have not had time to fully examine the Information Policy Task Force Draft Report to determine all of the impacts it may have on local government. We do, however, have concerns about the following issues:

- No longer allowing cities to charge for actual costs for the development or labor associated with data requests
- No longer allowing cities to copyright anything without legislative approval
- That the opinions from the Commissioner of Administration would be legally binding, possibly even over the Attorney General or the courts. (Should the State Supreme Court be consulted before enacting this type of legislation?)
- Cities would be required to provide electronic information in an easily accessible fashion to the public (i.e., by providing information on a diskette or other form of electronic media)

- Cities would no longer be able to monitor public access to government data
- Cities of a certain size would have to establish a position of Data Practices Compliance Officer
- That the public could bring charges of noncompliance with the Data Practices Act, and regardless of showing any harm done, could collect attorney fees and other damages.

This proposed legislation could have huge ramifications for smaller cities. There are many commercial entities, which, if given free rein, would deluge public entities with requests for data and demand it in the electronic form they deem acceptable. The cities of Edina and Chaska have already experienced these types of requests.

Cities also pay to have software written to manage information to help with special assessments, business licensing, building permits, and absentee ballot logs. Most, if not all, of these programs may contain confidential information (i.e., social security number, date of birth, etc.) Most of us would rather err on the side of not disclosing personal information to the general public.

We feel that cities are inundated with requests for public information. In fact, some information asked for requires staff to do extensive research for a constituent on certain topics. Sometimes we wonder if we are doing someone else's research or homework.

We are asking that local governments have more opportunity to review your report and give more input to you before your report becomes final and sent to the Minnesota State Legislature.

Sincerely,

Debra A. Skogen

William A. Champa

Chairpersons MCFOA State Retention Task Force

MINNESOTA

Trade & Economic Development

Business & Community Development

January 4, 1999

Ms. Anne Barry
Commissioner, Minnesota Department of Health
450 Metro Square
121 7th Place East
St. Paul, MN 55101

Dear Ms. Barry:

Thank you for the opportunity to comment on the December, 1998 Draft Report of the Information Policy Task Force (Draft Report).

In October, 1995, this office prepared two sets of comments on the copyright-of-state-government-publications issue for the Government Information Access Council. The first of these letters (October 13, 1995) described the basis in economics for the copyright of state government publications. The second letter (October 23, 1995) dealt with adverse consequences of removing the ability to copyright.

I will appreciate your making this letter and those of October 13 and October 23, 1995, part of the record of the Draft Report.

Sincerely,

Charles A. Schaffer
Director
Minnesota Small Business Assistance Office
(651) 296-0617

500 Metro Square, 121 7th Place East, Saint Paul, Minnesota 55101-2146 USA
612-297-1291 • 800-657-3858 • Fax 612-296-1290/296-5287 • TTY/TDD 800-627-3529
www.dted.state.mn.us

Marcia Hinds 5201 Windsor Ave. Edina, MN 55436 (612)925-9803

Fax (612)925-9467

January 4, 1999

To: Anne Barry
Chair of the Information Policy Analysis Task Force

From: Marcia Hinds

Subject: Draft Report Review

I wanted to thank you for allowing me to testify before the task force and share the problems I have had as a citizen trying to gain access to information from the Edina School district.

The draft report you will be forwarding on to the legislature will do much to help citizens gain access to data. There are several sections of the draft which, if implemented, would eliminate problems I have encountered:

- Recommendation 4 that states,"...government agencies should only be able to charge for the actual costs of making the copies and those costs should not include labor..."
- Recommendation 11 that states,"...[agencies should] provide access within 10 days of the request of a data subject."
- Recommendation 13, "...Furthermore the amendment should prohibit government entities for asking citizens to explain reasons for or to justify access to government data."

When I requested information from the school district under the current language of the Data Practices Act, administrators used delay tactics to circumvent compliance and test my perseverance. Sometimes it took weeks before the school district attorneys could review my requests.

I was required to make requests in writing. I was forced to pay for employee time spent searching for and compiling the data. I was interrogated as to why I wanted the information. The district hoped that intimidation would make me go away.

I was told the information regarding the Superintendent's travel expenses could be accessed, but it would take awhile because the records were in the archives

Comments on
Information Policy Task Force Draft Recommendations

Dave Ruch, Vice Chair, Information Policy Council
4 January 1999

Here are my thoughts after reviewing the draft. These are my own views and do not reflect any larger organization's position.

- It is ironic that the comment period should be so short for the subject - effective access to information. The presentation of the recommendations falls short of the standard aspired to in their content.
- It seems like there are several conflicting goals:
    - First, the present and proposed laws require that data be collected by government only in support of assigned purposes.
    - Second, there is an assumption that one of the assigned purposes of government is to be a purveyor of data. The argument presented is that this is implicit in the idea of a free society where openness is a requirement of true democracy, and openness means free access to any data sought within some limited boundaries of privacy.
    - Third, it appears that the emphasis in the proposed policies is on government failing to provide data with methods for preventing that result. It seems equally likely to me that future issues will revolve around government providing too much data; that privacy concerns will out-shout access concerns.
- If the Task Force recommends that government organizations have the added purpose of data dissemination, then that duty should be incorporated explicitly into the enabling statutes for each organization. That allows resource requests to be made through the budget processes to support this duty.
- It may be that the public purposes which generate the requirements for data are the appropriate avenue to follow about classification of data. I think it might be a mistake to treat government data as a single, monolithic entity that is somehow separate from the processes that gather or create it and store it. We have already seen that it is a mistake to separate information technology as if it has some independent life from the programs it supports.
- I am troubled by the prospect of giving data to others who will then sell it while government is prohibited from doing so, This seems like poor stewardship of the taxpayers' money, especially given the sharp limits on cost recovery permitted.
- The Task Force is correct in urging the move to electronic record-keeping. The legal community has been a barrier to employing these technologies. This is a place where the Task Force could make substantial progress.

I appreciate the chance to comment. If you have further questions, please contact me.

Phone: 651.296.9816
Email: dave.ruch@state.mn.us

DATE: January 4, 1999

TO: Information Policy Task Force

FROM: Anne Barry, Chair Information Policy Task Force
David Doth, Member of the Information Policy Task Force

SUBJECT: **Comments on Information Policy Task Force Report**

The report of the information Policy Task Force represents the culmination of nearly a year and a half of examination of data practices and other information policy laws in Minnesota. The discussion of these matters was at times very informative and in depth, even if, at times, polarized. The people of Minnesota were well-served by this process, where attendance by members was high and discussion of issues was deliberative. Unfortunately, the deliberative process was truncated as the time for this report came nearer. In addition, just when hard decisions on the recommendations and implications of the creation of a new office were necessary, the attendance by members was quite low.

The report contains recommendations and legislative proposals that would substantially change information policy laws in Minnesota. Lest the legislature believe that the report represent the unanimous view of the task force members, we find it necessary to point out our disagreement with some of the recommendations and the proposed legislation accompanying those recommendations. We disagree that an independent Office of Privacy and Freedom of Information needs to be created. Our main disagreement with the report is the recommendation that the legislature create an Office of Privacy and Freedom of Information to which all of the current duties of the Department of Administration and some new enforcement duties, such as binding opinions, would be added. See Recommendations 19 and 20 and the draft legislation supporting these recommendation in Appendix 7 of the report. The current structure of the executive branch is sufficient to meet the changing needs of government information policy even if the legislature believes that binding opinions are necessary ensure enforcement of data practices laws.

The task force report recommends creation of an independent office of information. If Minnesota were to follow this model it would have the public's advocate, judge & jury on information policy matters in one office. When these functions are combined with education and training duties, we think the office would lack necessary objectivity in its work. We think this lack of objectivity would be very problematic for government agencies and the general public alike. On one hand, the office would need to be a strong advocate for citizens in dealing with noncompliant government agencies. On the other hand, the office would need to be a resource to which government agencies can turn to for guidance and training on complex information policy matters. And on yet a third hand, the office would need to be dispassionate enough to resolve matters on the merits of the circumstances and the law. We believe that these duties must, by their nature, be separate.

We support giving the Information Policy Analysis Division of the Department of Administration better resources and a more streamlined mandate to provide training, draft forms and provide quick/efficient, yet non-binding, guidance/advice in order to ensure compliance with information policy laws.. This office could continue to act as a reporting function to the legislature on all the reporting requirements placed on agencies. Finally, this office could be given a more formal role to act as advocate for citizens in information policy matters.

We strongly urge the legislature to look at several models that would not require the creation of a new Office of Privacy and Freedom of Information, yet would ensure enough independence and neutrality to decide information policy matters on their merits:

1. Agency Referee Model

One possibility is to require each agency to establish an independent administrative review process for information policy matters. This model can be seen in the welfare system where referees at the Department of Human Services conduct hearings on changes affecting welfare recipients' benefits. The referees make findings and draft orders for the commissioner which are binding upon the recipients and county and state human services agencies. The decisions are appealable to district court. This model might work well for large state agencies or for large groups of data such as in the welfare system. The orders could act as the clear voice of the responsible authority on the agencies' information policy questions. An additional benefit would be the efficiency obtained because of the agency's familiarity of how the information in their particular state program affects the clients of the agency. This is an especially important factor where the data questions are complex and mult-faceted. This model would require referees to be sufficiently independent from the policy-making and administrative parts of the agency. Implementation of this model would require that the agency or program area already have an administrative review system in place. Few government agencies have such a model but where they exist, it would be an efficient use of state resources to augment this process to include information policy matters.

2. Office of Administrative Hearings Model

The Office of Administrative Hearings (OAH) seems an ideal place for the legislature to provide authority to issue binding opinions in information policy matters. The administrative process is clearly laid out for contested case hearings. Administrative Law Judges are somewhat familiar with data practices issues since the OAH currently evaluates accuracy and completeness challenges referred by the Department of Administration. The OAH operates largely in an independent manner from the agencies.

One criticism of the OAH model is that its opinions should not usurp the powers of the judicial branch. The OAH currently is subject of a Court of Appeals decision stating that its child support orders, matters traditionally decided by the judicial branch, are an Unconstitutional usurpation of judicial powers. Data practices concerns have also traditionally been resolved in the district courts. This concern could be better remedied if OAH information policy decisions were appealable to the district court.

3. Office of the Attorney General Model

Another possible model would be to have the Office of the Attorney General (AG) issue binding opinions on the treatment of data. The AG's Office is an independently-elected constitutional office, thus ensuring independence from appointment by the governor. The AG's Office can also issue formal opinions on legal matters. The formal opinions of the Attorney General are given much deference in the courts. The legal soundness of the opinions would be high. The question of independence, where the AG's Office has advised its agency client of a data practices matter would require the establishment of a separate function within the office similar to the agency referee model, above, to hear and decide data practices questions.

4. The District Court Model

The district court has traditionally been the forum to resolve data practices disputes. It has also been criticized for being too expensive and remote for most people to bring data practices disputes. Perhaps if the courts were provided more resources or a process were designed to hear data practices concerns in a more timely manner, then citizens would use the forum more readily. Margaret Westin, a former chair of the Minnesota State Bar Association's Public Lawyer Subcommittee on Data Practices and author of a data practices law review article, has written about using writs of mandamus to address data practices matters. A writ of mandamus is an order issued by a court after the court determines that there is a failure of an official duty clearly imposed by law, a public wrong specifically injurious to the petitioner, and no other adequate specific legal remedy. It is obtained when a person files a petition for a writ of mandamus. It is an equitable remedy. The procedure takes 24 or 48 hours and allows for a hearing on the facts with judicial review. Pursuant to Minnesota Statutes, section 586.03-.06, there are two types of proceedings to obtain a writ of mandamus. There are preemptory writs and alternative writs. A preemptory writ will issue if the respondent (government) has no valid excuse for nonperformance. If the respondent has a valid excuse, the court issues an alternative writ and allows the respondent to answer on the day the writ is returned. There is an opportunity for a hearing about whether the person seeking the writ is entitled to one. Although a Writ of Mandamus is not allowed unless there is no adequate remedy at law, the legislature could create a similar process under Minnesota Statutes, section 13.08 for information policy matters.

Thank you for consideration of our comments.

Anne Barry

David S. Doth

dothmem5.wpd

MINNESOTA Department of Revenue
Commissioner's Office

BY FAX

January 5, 1998

To: Michele Ford
Information Policy Task Force

From: John Lally
Assistant Commissioner

Subject: Legislative Proposals of the Information Policy Task Force

This memo presents the Department of Revenue's general comments regarding the draft language that will be proposed for legislation by the Information Policy Task Force. We appreciate the opportunity to comment, and believe that the draft, while incomplete, clearly articulates some general principles we endorse.

For purposes of this memo I am addressing only the proposed statutory changes included in the most recently available draft. However, while our main content concerns are with the amendments listed below, we are also concerned that several draft amendments do not seem consistent with the recommendations in the draft report. After we know which version would be proposed, we may have additional comments.

The Department has significant concerns with several topics in the language. The first is the draft proposal to amend Minn. Stat. §13.03, subd. 3 - **"Request for Access to Data."**

While we agree with what we understand to be the underlying intent of the proposed change -- to provide electronic access to public records -- there are very significant practical problems that would occur in this agency and potentially many others. This is an extraordinarily complex issue and our general reaction is that the language is overly simplistic, burdensome and limiting. It also will, we believe, produce outcomes contrary to those desired by the task force.

This section would apparently require all electronically stored public government data to be available for *on-line* access by the public. It is not clear how "on-line" will be defined or interpreted, but in the context of the report we assume that means available from any location *via* the Internet.

Revenue's work involves hundreds of electronic databases containing tax data. Some of these are extremely large and complex. These by their nature can involve a mix of public and nonpublic or private data, while other databases have purely public data. Some of these systems are as much as 30 years old, and for most of them, the information would not be in any readable format for on-line access from outside the agency. The only access to

current data is through these core operational databases. Direct access to these cannot be granted without compromising data integrity or systems operations. This means it would be necessary to develop and program new formats to make the information accessible or maintain separate parallel databases. This is extremely costly, especially in an agency of this size, with the number of databases we maintain. In any new computer system we develop, we recognize the need to anticipate this kind of public access, and in fact, we are planning to build that capability into new systems such as our reengineered individual income tax system. However, the cost for changing the old systems would be significant.

In addition, much of this information, if accessed by the public, will be raw data without context or explanation, severely limiting the utility of the data as information resources to the public. In most cases the taxpayers will benefit from either consultation or assistance in directing and formulating requests for information. This "value-adding" process has been our practice for many years, and to our knowledge had not created problems for citizens needing information.

Since the bulk of our information is highly confidential state and federal tax return information, we would need to modify all of our existing data security systems and safety firewalls to ensure that the proposed on-line access would not enable someone to go through a public database into other databases that contain confidential information, or to infer private data from correlation of multiple public data items. While this is not impossible, again, it is a highly expensive and time-consuming task.

In general, we question the value and need for giving on-line, independent access to those few who may want to access data, especially for some of the more esoteric internal databases. On-line access is very expensive, and the cost of making data available and responding to information requests from people unfamiliar with the data, its structure, limitations and meaning is likely to be prohibitive. The huge cost of compliance for a few requests could come at the expense of other vital services to taxpayers if there is no additional budget resources to fulfill these legislative mandates. We have documented the reduction in actual compliance and service resources caused by long-term unfunded increases in required base IT and fixed costs; imposition of much greater unreimbursed costs for providing data will only exacerbate that trend.

This provision also changes the ability of state agencies to charge for their costs to search for and retrieve requested data. The current statute provides that "actual" costs can be recouped. The proposed change would only allow "marginal" costs. This has been defined to mean only the actual cost of making the copies, no labor or other overhead, or development costs. This could result in a state agency incurring a great deal of non-reimbursable expense in programming costs associated with an electronic data practices request.

In order to respond in a timely manner to access requests, we will have to expend significant funds to establish retrieval mechanisms to our complex operational database files...and all to make accessible information that may be rarely if ever requested. This is to

a major waste of taxpayer dollars. It could also have a chilling effect on our agency's inclination to store data electronically because of the potential costs involved with preparing or retrieving that data...the opposite effect from what the task force and the department would like to implement.

Revenue has an additional problem in that we continually interact with groups with an avowed goal of disrupting government activities in general and tax administration in particular. This proposal opens the door for these groups to make multiple requests for voluminous public information as a tactic for damaging our effectiveness since we are required to produce the information without regard to actual cost. This is not an example of bureaucratic paranoia...such requests are a common practice nationwide.

Another department concern is a proposed change to Minn. Stat. §13.05 - **Monitoring of Citizens**. This is another new section that prohibits state agencies from monitoring citizen access to and use of public data. This would include use of electronic devices or software features that allow the agency to acquire information that identifies the citizen or device the citizen is using to gain access to the data.

A few examples may illustrate our concern. Revenue recently purchased a new phone system that contains Caller ID on every employee's phone. Having that feature enables us to provide better customer service when dealing with taxpayers. Our new systems are designed to speed response to inquiries by linking caller information with our databases. By way of comparison, many fast-food delivery businesses use this capability to minimize customer inconvenience in ordering. The identity of taxpayers who make data practices requests are not recorded or tracked through the use of Caller ID, but it appears this proposed change could prohibit us from using that feature for any purpose.

There is also an apparent contradiction in the technology implications. Making databases available "on-line" requires a certain amount of tracking who and what an outside person accesses - e.g. "cookies" - to maintain a connection. This proposal would hamper our ability to make that on-line access a reality. It appears that this basic necessity for access may be prohibited, although this is unclear in the language.

As a more mundane example will show, our inability to capture information poses a service problem and security hazard as well. We use an identification procedure and sign-in sheet at our main office and all field offices for the purpose of building security. That information may not be directly related to data practices requests, but we don't know that when the visitor comes in, and failure to follow these procedures compromises our physical and data security systems. There appears to be little or no coverage of the physical security concern in the task force report.

It appears that all of these processes are covered by the proposed legislation and we could potentially be prohibited from using Caller ID, sign-in rosters, or similar products if the intent of the proposed legislation is to cover recording citizen access attempts in the process -- whether the intent of the process is to provide service, security or another purpose.

We object to the revisions to Minn. Stat.. §13.08, subd. 1 - **"Complaints."** This proposal could place a huge burden on the DOR to defend unjustified complaints by taxpayers (especially by tax protesters) that the department is not complying with the Data Practices Act, and result in a substantial increase in the number of contested case hearings involving the department. For us the issue is not a matter of fearing accountability; rather, we are concerned that there are no consequences identified for recovering costs of frivolous or unjustified complaints made by tax protesters. We view as problematic the ability of an administrative law judge to award monetary damages -- something we believe is unprecedented in the law. This is a power that has always been reserved for the courts.

We also have problems with the recommended provisions under Minn. Stat. §13.08, subd. 3 - **"Action to compel compliance."** We feel that it is a dangerous practice to encourage persons to file lawsuits without demonstrating that they have standing because they are or will be harmed.

We question the advisability of creating another state entity to exert leadership in aspects of information policy. As a customer as well as an information provider, we think accountability for results is best served by unambiguous authority and responsibility for access being vested in the Commissioner of Administration and not distributed among multiple agencies.

On the positive side, we agree with many of the proposals not identified above, and strongly endorse the draft amendment (to Minn. Stat. §13.03, subd. 2) that requires agencies to prepare, maintain, and publish written access procedures for the public. This fits with the spirit of the data practices act and helps to ensure that citizens know or can easily find out how to access public information in each agency.

In summary, we support -- and have consistently supported -- the principles of data access. However, we feel that the specific requirements and limitations of the proposed legislation as currently drafted are based on an idealized vision that isn't responsive to realistic problems with many -- primarily negative -- consequences.

Again, I appreciate the opportunity to comment on these issues. I hope the task force will consider our perspectives in completing the report and drafting proposed legislation. We will be happy to provide you with any further information you might desire on any of these points, and will continue with our analysis of the full report as it evolves.

c: Matt Smith, Commissioner of Revenue
Don Gemberling, Information Policy Task Force

UNIVERSITY OF MINNESOTA

Office of the General Counsel

325 Morrill Hall
100 Church Street S.E.
Minneapolis, MN 55455
612-624-4100
Fax: 612-626-9624

January 5, 1999

Commissioner Anne M. Barry
Chair, Information Policy Task Force
Minnesota Department of Health
P.O. Box 9441
Minneapolis, MN 55440-9441

Re: *Information Policy Task Force Report and Draft Legislation*

Dear Commissioner Barry:

We write on behalf of the Public Law Section of the Minnesota State Bar Association. The Public Law Section is composed of members of the state bar association who have an interest in governmental and public law issues. One of the Section's committees is the Data Practices Committee, which has submitted comments to your Task Force over the past year. As you now seek public comment on the report of the Task Force, the Public Law Section as a whole appreciates the opportunity to express its views.

We appreciate the time and effort that have been devoted to the complex issue of information access. We share the Task Force's desire to establish clear principles and rules to ensure citizens swift access to public information. We also appreciate the concerns raised about citizen privacy in an increasingly complicated world. As we share the same views as the Task Force with respect to much of the report, we will limit our comments to the few areas of concern that we have with the report and the proposed legislation.

Unfortunately, because the newest versions of the report and draft legislation were not on-line until Thursday, December 31, and public comments were due within a few days, we had limited time to review the materials in-depth. In addition, it appears that the version that came on-line may not have been the same as the version available in hard copy; for example, the on-line version does not include draft legislation relating to out-sourcing government functions to private entities. We therefore base these comments on our quick review of the on-line report and draft legislation.

A. Tennessen Warning.

Recommendation 10 appropriately suggests that the Tennessen warning provision should be changed when data is collected from an employee by government employers or from students by a school. As was demonstrated at the

debate between public lawyers and private plaintiffs attorneys,[1] the law requiring a Tennessen warning whenever an employee is asked anything about his or her work is unnecessary, impractical, and contrary to the public interest. The plaintiffs attorneys asserted at the debate that whenever a public doctor asks another member of the medical staff anything about his or her care of a patient (a question that must occur hundreds if not thousands of times a day in any public hospital), the doctor first must pull a Tennessen warning out of his or her pocket and read it to the employee like a Miranda warning — even if the doctor was not investigating the employee. No employer, public or private, could (or should have to) meet this impossible standard. All employees, public or private, know that their performance will be relevant to management decisions about them, and no "warning" is needed to advise them of this obvious fact.

As was also demonstrated at the debate, there is no *ad absurdum* limit on the necessity of a Tennessen warning in school. Under the present law, public school teachers literally must give a Tennessen warning to students of any age whenever the teachers assign homework, ask questions in class, investigate who pushed whom in the hallway, and so on. A change is needed to exempt schools from the Tennessen warning requirement in the context of the ongoing educational relationship with students.

While the Task Force's recommendation is sound, the recommendation is undermined by the inconsistent draft legislation issued on December 31. Rather than exempting schools and public employers from a Tennessen requirement when they seek information as part of the educational or employment relationship, the draft legislation would require public educators and employers at the start of the relationship to know warn students and employees of "*all of the possible data collection instances that may occur* during the duration of the employment or academic relationship." (Emphasis added.) No one has the prescience to anticipate all possible questions that "may" be asked of employees or students in the future.

Even more disturbingly, the latest draft legislation adopts precisely the argument advanced by the plaintiffs attorneys, despite the recommendation of the Task Force. The draft legislation would require the equivalent of a Miranda

[1] It is noteworthy that the Report describes a bar committee of public lawyers (who, for the most part, are salaried public employees with no personal interest at stake) as an "interest group" (a term that carries negative connotations), but does not describe the *ad hoc* coalition of private attorneys who represent employees in disciplinary matters in the same terms. Instead, the plaintiffs attorneys are described simply as the representatives of "citizens." Such characterizations color the report, and in fairness should be changed.

warning every time a public employer or teacher asked a question the answer to which *"may"* be used in discipline. Before a supervisor asked the following everyday questions, whether or not the supervisor thought that the answer *may* result in discipline against the employee, the supervisor would have to give a Tennessen warning: "Medical Resident A, what medications did you prescribe for Mrs. Brown?" "Secretary B, have you finished typing that letter?" "Public Lawyer C, the court called because you weren't at the scheduled hearing. What happened?" "Forest Ranger D, were you at your station yesterday?" "Bookkeeper E, what is this expense for $15,000?" A law prohibiting the discipline of public employees for poor performance or misconduct at work unless the employees were first given a Miranda-style warning would make for abysmal public policy. The same is true for the discipline of students. Should teachers really have to Tennessen warn a 6th grader before asking her why she was not in class during fifth period?

Either the draft legislation should accord with the recommendation of the Task Force, or the Task Force should leave the Tennessen warning alone and let the courts deal with the law in the employment or school cases in which it arises. In no event should the Act be amended to enshrine in the law precisely the position advanced by the plaintiffs attorneys who represent public employees in disciplinary matters. In addition, if the Task Force is going to include draft legislation in its report, the draft legislation should be approved by a majority of the Task Force members. Otherwise, the draft legislation carries the imprimatur of the Task Force, without actual approval by the Task Force.

B. Recovering Development Costs of Publicly Funded Formulae with Commercial Value.

At the end of the "Principles" section of the Report, the Task Force adds a paragraph recommending the elimination of Minn. Stat. § 13.03, subd. 3, which permits public entities to recover the development costs of commercially valuable and publicly funded formulae, compilations, techniques, databases, etc. In the "State Budget and Other Financial Implications of IPTF Recommendations," this change is identified as having "negligible or difficult to measure financial impact." In fact, the change may not be the least bit "negligible." The inability of taxpayers to recoup their investment in commercially valuable government data may have a very substantial financial impact. For example, taxpayers supporting local government have spent millions of dollars developing and implementing systems and software, the cost of which can presently be recouped under the law. In addition, the publicly funded University of Minnesota develops sophisticated and costly research techniques which it may sell to private industry under the present law.

Recommendation 15 and its rationale suggest that members of the public end up paying twice for commercially valuable information when they are charged development costs because a portion of their tax dollar already was spent in the endeavor. In fact, however, many requesters of such commercially valuable information may not be individual taxpayers (many requesters seeking commercially valuable information are, in fact, commercial entities) and may not even be Minnesota taxpayers. A requester seeking commercially valuable, government-developed medical technology may well be a non-Minnesota medical products company, not a Minnesota taxpayer. Before such a radical and costly revision as this is proposed, additional input is needed, especially regarding the financial cost to Minnesota taxpayers.

C. Copyrighting Government Information.

Recommendation 6 suggests that the Minnesota Government Data Practices Act be amended to preclude government entities from copyrighting information without specific legislative authorization. Better understanding of the effect of a government-held copyright is needed before this change is proposed. The rationale to Recommendation 6 suggests that a copyright would limit *access* to government data. In fact, a government-held copyright does not limit access to data, or even access to copies of data. It simply conditions the later commercial *use* of the data for a number of sound policy reasons (including to protect the authenticity of the data by precluding a state-sponsored report from being altered and misrepresented as the view of the state). The copyrighting of government information is a controversial and important topic. It is presently the subject of a Commissioner's Opinion and a conflicting Attorney General's Opinion. Copyright is an area that requires fulsome and serious discussion from interested parties and experts before any change is made to the law.

D. Compliance Officer.

Recommendation 17 would require all government entities to appoint a "compliance officer" in addition to a "responsible authority" or "designee" of a responsible authority, and to make reports to the Commissioner of Administration regarding the names, addresses, and phone numbers of the compliance officer (and to update the Commissioner whenever there is any change, for example, if the employee's phone number changes). The justification for this new regulation is elusive. Many government entities already have and pay for a responsible authority. This legislation would require that this public employee — the responsible authority — hire yet *another* public employee to do exactly what the responsible authority already is charged with doing. The report does not explain

why two people are necessary to do the work of a responsible authority, nor does the report or its draft legislation propose additional appropriations to government entities to support this additional employee. For those agencies for whom the head of the entity is the responsible authority, there is no evidence in the report that the responsible authority's designee under the current law is not fulfilling the statutory responsibilities. There seems to be little reason for this additional bureaucracy and public expense.

E. Identifying Requesters of Public Data.

Recommendation 13 states that government entities shall not "monitor" citizen access to and use of public data and shall not demand reasons for requesting information. The recommendation goes on to state, however, that government entities can ask for names and other identifying information for the purpose of facilitating access to data. This is a reasonable recommendation. Government entities should not condition access to data on the use that requesters intend to make of it, but government entities need to know the identity of a requester of information for a number of valid reasons, including: (1) to know whether the person is the "subject" of the data and therefore entitled to more favorable copying rates and deadlines; (2) to maintain records that establish that the government complied with a request in the event of later litigation; and (3) to be aware of potential safety concerns (including for public employees) if public information is asked about an individual. Moreover, when requesters ask for information on-line, they self-identify since e-mail necessarily identifies the sender.

The draft legislation, however, differs from, and is contrary to, the Task Force report in that it would preclude government entities from "requiring citizens to identify themselves" at all. This is bad public policy. Government entities certainly should not condition access on later use of the data, but they must be able to maintain records of their compliance with requests. If persons want to maintain anonymity, they can easily have someone else request the data. But government entities should be able to ask for the requester's name.

F. Remedies and Enforcement.

The biggest changes to the most recent Task Force report and draft legislation concern remedies and enforcement. While at this point, there has been limited time to address these proposals, several elements bear comment now.

Most importantly, a great deal of further thought must be given to the idea of creating a unique super-agency that has the power to both define and enforce the

law. Under the draft legislation, one state agency would be both judge (determining in a "binding" fashion what the law is) and prosecutor (suing on behalf of individuals to enforce its own binding interpretation of the law). Serious issues of due process, the role of the courts, increased litigation, costs to litigants, and so on must be addressed before such a novel agency is created. In addition, it is unclear what is meant "binding" opinions. How can the Department of Administration hold a district court to its version of the law? Are the opinions "binding" on ALJs and the appellate courts? If so, of what value is an administrative hearing or a right of appeal to the Court of Appeals? Further exploration is needed. While an administrative model might be a valid approach for dealing with the MGDPA, no enforcement scheme should exclude the courts from their role as the interpreters of the law.

Also of concern is the unprecedented provision for attorney's fees and costs in Recommendation 21. Unlike other fee-shifting statutes (consumer fraud laws, antitrust laws, civil rights laws, etc.), the attorney's fees provision here would *require* the award of attorney's fees and divest courts of any discretion in awarding fees. Moreover, unlike in those laws, here the proposed legislation would not only pay the plaintiff's attorney's fees, but would also pay the plaintiff for the time he or she spent on the case. We are aware of no other situation at law in which plaintiffs are actually *paid* to litigate. The report does not explain why data practices lawsuits are of such greater social value than civil rights or consumer fraud lawsuits to justify such a lucrative scheme for plaintiffs and plaintiffs attorneys. This proposal is a recipe for increased court litigation, and is at odds with the underlying principle that data practices litigation should be reduced, not increased.

G. "Surveillance" of Citizens.

Finally, the Report contains several interesting provisions regarding citizen privacy. In an increasingly technological world, privacy is an increasingly important topic. Caller ID, phone systems capable of recording time spent on individual calls, computer technology permitting records of electronic mail use and Internet use, etc., are all standard fare in numerous private and government settings. In the employment setting, employee privacy and the rights of employers to limit the use of their equipment to work-related purposes is a hot topic of debate and court opinions. There is also already existing legislation regarding electronic privacy. Congress, after much debate, passed the Electronic Communications Privacy Act, and the Minnesota legislature has also addressed electronic privacy in legislation.

While further legislation ultimately may be worthwhile, enactment of new privacy laws in this context may be premature. The Minnesota Government Data

Practices Act generally deals with access rights to existing government data. It is not an employment statute, nor does it impose limits on government unrelated to government data. While legislation limiting the "surveillance" capabilities of public entities or public employers may be a part of Minnesota's future, it should probably take place in a different context, and following full and informed debate. In addition, the consequences of such legislation should be more fully considered. It is not clear that having each government agency tell the Commissioner of Administration when it has acquired a new phone system or new computer system will be of much value to the public.

CONCLUSION

While the Task Force report contains some valuable ideas, there are several substantive areas of concern as described above. In addition, there is a very real concern that the draft legislation meant to implement the views of the Task Force in some cases may not do so. Before the Task Force appends any draft legislation to its report, the draft legislation should be carefully studied and a majority of the members should approve it. Finally, as the Task Force has not yet included an appendix of draft legislation to correct inconsistencies in the law, we cannot comment on this aspect of the Task Force's work.

Thank you for your consideration of these comments to the Task Force. We look forward to healthy changes to our information practices law, and appreciate the opportunity to participate in the process.

Very truly yours,

Tracy M. Smith
Associate General Counsel
University of Minnesota
Co-Chair, Data Practices Committee

Brian Asleson
Chief Attorney, Civil Division
Wright County Attorney's Office
Co-Chair, Data Practices Committee

Greg Brooker
Co-Chair, Public Law Section
Minnesota State Bar Association

Harriet Sims
Co-Chair, Public Law Section
Minnesota State Bar Association

Memo

DATE: January 5, 1998

TO: Members, Information Policy Task Force

FROM: Robert Hanson, Director, Information Technology

SUBJECT: Information Policy Task Force Recommendations

For your consideration, I have attached comments to the proposed additions and changes to the "Principles Relating to the Public Access to Government Information."

If you have any questions, please contact Denis Nolan at 612-348-6596 or e-mail at **Denis.Nolan@co.hennepin.mn.us**.

Thank you for your consideration.

342

12/28/98

HENNEPIN COUNTY COMMENTS/DISCUSSION

The following is a discussion of the adopted government data access principles proposed by the Government Information Task Force. Hennepin County comments are on the adopted principles and not on the Task Force Recommendations/Rationale.

PRINCIPLES RELATING TO THE PUBLIC ACCESS TO GOVERNMENT INFORMATION
(New principles as proposed by the Government Information Task Force are in **BOLD**; Hennepin County Comments are in "Hennepin Co. Discussion.")

1.The public must be able to gain access to public government data, no matter what type of storage modality is chosen by the government to create, collect and store the data, as long as the data exist in some physical form, including computerized, video, paper, microfilm and all other forms of recorded data.

2. In a democratic society, government data should be presumed by law to be available for public access and examination to the greatest extent possible. Data held by the government should only be declared to be not public by statute, as required by federal law, or under the authority granted the Commissioner of Administration to issue temporary classifications of data.

3. Public government data must be kept and arranged so that they are easily accessible to the public.

4. Government entities must establish and publish procedures to insure that requests for access to government data are complied with promptly and appropriately and to ensure that the public understands how to gain access to public data.

5. Public access to government information for the purpose of inspecting the data shall be at no charge to the person seeking to inspect the data. When a person asks for copies of government information, any charge for the copies shall not exceed marginal cost, which means that the cost of providing copies must exclude labor, overhead and development costs.

Hennepin Co. Discussion 5: It is Hennepin County's policy, as contained in the County's Administrative Manual, to charge either a Flat Rate or Special Rate for copies of government data. Currently, the Flat Rate is $.25 per page for "routine" copying. The Special Rate is charged when staff time and other direct costs significantly exceed the Flat Rate. Pursuant to MS 13.03, subd. 3[1], the County does not charge for separating public from not public data. Neither overhead nor development costs are incorporated into the Special Rate. MS 13.03, Subd. 3[2] does provide that when a request for data that has commercial value, the responsible authority may charge a reasonable fee for the information in addition to the costs of

---

[1] MS 13.03, subd. 3 reads, in part: "If a person requests copies or electronic transmittal of the data to the person, the responsible authority may require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from not public data

[2] When a request under this subdivision involves any person's receipt of copies of public government data that has commercial value and is a substantial and discrete portion of or an entire formula, pattern, compilation, program, device, method, techniques, process, data base, or system developed with a significant expenditure of public funds by the agency, the responsible authority may charge a reasonable fee for the information in addition to the costs of making, certifying, and compiling the copies. Any fee charged must be clearly demonstrated by the agency to relate to the actual development costs of the information. The responsible authority, upon the request of any person, shall provide sufficient documentation to explain and justify the fee being charged.

making, certifying, and compiling the copies. While there are complaints from staff about the time resources needed to respond to the data requests we receive and some complaints about charges to the public and data subjects for copies of data, the current language in the Act is workable and has worked for 20 years.

6. Access by members of the public to government data in electronic form, using their own computers and incurring the cost of any communication charges, shall be considered inspection of government data at no cost to the public, regardless of whether the member of the public only examines the data in question, downloads the data, or prints a copy of the data.

Hennepin Co. Discussion 6: Hennepin County has a Web page on the Internet which provides information about County services, departments, jobs, happenings, documents, frequently called numbers, frequently asked questions, etc. Extensive property information (PINS) about each tax parcel and property owner is available on-line. All of this information is on-line and free of charge.

A dial-up to the County's mainframe computer is also available to access SIP (Subject in Process) Criminal and Civil defendants and case records as well as property information. The SIP data is a hierarchical database and is not Web-enabled. Since the dial-up service uses mainframe or CPU time, telecommunication lines, baud rate/band width resources and support personnel, a charge is made for each Information Management Service (IMS) transactions and "communication services." Except for certain proprietary data, all the information on the Web site and the dial-up service can be downloaded, printed and used for any purpose a requestor may have. .

7. With the limited exception of computer software, government data should not be copyrighted without express legislative approval.

Hennepin Co. Discussion 7: A copyright offers a certain degree of control over the use and dissemination of government information or products, it does not however preempt the provisions of the Data Practices Act and the accessability of government data by the public. The State of Minnesota exercises copyright in State Supreme Court Decisions (copyrighted by the Secretary of State), Headnotes of Minnesota Statutes (copyrighted by the Revisor or Statutes), Minnesota Rules (copyrighted by Revisor of Statutes), the Environment and Natural Resources Trust Fund has copyright authority (MS 116P.10) and the Council on Quality Education (MS 120.90). Several State Department of Natural Resources publications are also copyrighted.

Except for Minnesota Statutes 13.03, subd. 5[3], statutory guidelines are really not available to guide political subdivisions in the use of copyrights and patents. To ask that the legislature review each and every request for a copyright is not realistic.

8. To the greatest extent possible, public government data that are maintained in electronic form should be made available in electronic form to citizens who request data in that form. Government agencies should design and implement electronic

---

[3] "Copyright or patent of computer program. Nothing in this chapter or any other statute shall be construed to prevent a state agency, statewide system, or political subdivision from acquiring a copyright or patent for a computer software program or components of a program created by that government agency. In the event that a government agency does acquire a patent or copyright to a computer software program or component of a program, the data shall be treated as trade secret information pursuant to section 13.37."

government data systems in such a fashion that the public data contained in those systems are easily accessible for electronic use and copying by the public.

Hennepin Co. Discussion 8: MS 13.05, subd. 3 provides that: "[c]ollection and storage of all data on individuals and the 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 or local governing body or mandated by the federal government."

Generally, the design of program data collection, storage, use and dissemination is guided primarily to meet the needs of the administration and management of programs in a cost effective manner and not whether it is in a format that may be accessible on-line or on a Web page. Currently, information is put on our Web page that is needed, wanted, and used by the public -- a library does not maintain every book, periodical or magazine but only those for which the public may desire while considering the budget and space limitations of the library.

9. All citizens, regardless of geographic, physical, cultural, socio-economic status or other barriers, shall have equitable and affordable access to government information.

Hennepin Co. Discussion 9: The County provides access by the public to government data as required by the Data Practices Act[4]. Public terminals are available at the Government Center to access criminal and civil court information and property tax information on any Hennepin County property. A public library with Internet access can access the County's Web Page. A philosophy of "equitable and affordable access" goes beyond the following basic premises of the Act that ensures access by the public:

1. All government data shall be public unless classified as "not public";

2. The responsible authority shall establish procedures to insure that requests for government data are received and complied with in an appropriate and prompt manner;
make them easily accessible for convenient use.

3. The responsible authority shall keep records in such an arrangement and condition to make them easily accessible for convenient use.

10. When a government entity contracts with a private sector entity to perform a government function, all data created, collected, received, stored and maintained by the private sector entity as it performs that function must be subject to requirements of the Data Practices Act.

---

[4] MS 13.03 Subd. 2, provides that: "The responsible authority in every state agency, political subdivision, and statewide system shall establish procedures, consistent with this chapter, to ensure that request for government data are received and complied with in an appropriate and prompt manner."

Section 13.03, Subd. 3, provides that: "The responsible authority or designee shall provide copies of public government data upon request."

In the case of data on individuals, section 13.04, subd. 3 provides that: "Upon request to a responsible authority, an individual shall be informed whether the individual is the subject of stored data on individuals, and whether it is classified as public, private or confidential. Upon further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge, and, if desired, shall be informed of the content and meaning of the data. . . . The responsible authority shall provide copies of the private or public data upon request by the individual subject of the data.

Hennepin Co. Discussion 10: Under current practice the following language is added to contracts which require the collection, use, and dissemination of data required by the terms and conditions of the contract.:

"Contractor agrees to abide by the provision of the Minnesota Government Data Practices Act and all other applicable state and federal law, rules and regulations relating to data privacy or confidentiality, and as any of the same may be amended. Supplemental to any indemnification provision herein. Contractor agrees to defend and hold the County, its officers, agents and employees harmless from any claims resulting from Contractor's unlawful disclosure and/or use of such protected data."

Generally, this language applies to the data collected, created, used and disseminated by the contractor in performance of duties required by the contract.

Information Policy Task Force Report

by Lyno Sullivan, January 6, 1999

<http://www.freedomain.org/^lls/mpdn/19990106-iptf.html>

January 6, 1999
To: "Michele Ford" <michele.ford@senate.leg.state.mn.us>
cc: "Don Gemberling" <don.gemberling@state.mn.us>, mn-netgov@egroups.com
Fr: "Lyno Sullivan" <lls@freedomain.org>
Re: Information Policy Task Force Report

I was at the Information Policy Task Force meeting today. I am working on my feedback on the Recommendations but I wanted to first discuss a couple possible processes. I am an unaffiliated, private citizen and must apologize for not having been aware of how to provide feedback, before the meeting.

RECOMMENDATION

I sincerely recommend that the Task Force spare itself the pain of trying to introduce fundamental change at the last minute. If it were mine to do, I would simply issue the Report intact and attach a Preface that explains how the public testimony is being handled. Then the Task Force might pick one or both of the following alternatives, or make up your own. I would describe this as an experiment in government, and record that fact in the Preface.

I don't want to sound whiney but I feel like I am cut out of the existing process. I can seldom afford to take the time off work, to be at scheduled meetings, in brick and mortar buildings, to discuss topics like Information Policy, even though I care deeply about the issue. If the Task Force will open itself to email based electronic discussions, as I propose in Alternative 2, then I can attend those discussions at my leisure. I am sure every member of the Task Force suffers from similar scheduling problems. The processes I propose frees the Task Force members too.

Although both alternatives demonstrate my naivete about the current process, they might be reasonable ways to imagine the future. Alternative 1 might be an expedient way to handle the current situation. It would be quite reasonable to "freeze" the past, as proposed in Alternative 1, and then create the future, as proposed in Alternative 2.

ALTERNATIVE #1

Place the public testimony, and the minority opinions of the Task Force, at the web site, as hyper-text links within the Report. Recommend that legislators visit the web site to view the current public testimony and member minority reports. Offer to print this material for any who wish to read it, rather than browse it.

This approach will provide a useful analytical tool for those preparing the changes to Statute. People will be able to browse the Report's summary recommendation and then, by following a link to other documents, they can view the detailed commentary. It will be especially helpful because the commentary will be easily available, on a topic by topic basis, rather than buried in multiple documents. Also, search engines can index this text.

If this works for the Task Force, automated free software tools can easily be assembled, that could help build future Reports, in an automated manner. This first experiment will be painful because the tools haven't been installed. However, the resulting Report and Commentary might serve as a prototype for the future automation.

Let me explain how this might look from the perspective of someone browsing the Report. The browser would see each of the Recommendations. At the end of each Recommendation (let's use 6 as the

example) they would see a "Commentary" hyper-text link. That link would bring them to a page like "IPTF Recommendation 6 Commentary". They might see all the commentary listed or, if it is extensive, they might see a list of links to other pages (even pages at the web sites of the commentators). Under the heading "Recommendation 6, Strongly Disagree" they would see "Lyno Sullivan, citizen" listed. If they click that link they could read my objection and my proposed alternative.

ALTERNATIVE #2

Here is another way you could handle this. There are several free software tools that automatically build searchable, threaded archives of listserv discussions. This second approach would involve much less work to create the public discussion and would be available for input, from anyone with an email account.

You could create a listserv MN-IPTF (or something similar) and invite people to join in the discussions. The moderator could introduce the recommendations one by one. People could provide their commentary, in response to the listserv postings. If people did a nice job of putting links to supporting documents into their postings, a fabulous analysis tool would be created. The final Report can easily contain the links directly into the listserv archive.

This is my preferred approach. It establishes a nice precedent for future Statute work. These searchable, public discussion archives will always be available as a resource, to people who contemplate future Data Practices statute changes. It also creates a forum where people, interested in this issue, can continue to have discussions about proposed legislative changes. These discussions would continue throughout the year, even outside the legislative session.

348

ASSOCIATION OF
AMC
MINNESOTA COUNTIES

January 6, 1999

Ms. Anne Barry
Chair, Information Policy Task Force
C/o Michele Ford
Room 306 State Capitol
St. Paul, MN 55155

Dear Commissioner Barry:

The following are the Association of Minnesota Counties comments on the third draft report of the Information Policy Task Force. These comments are general in nature, and I have encouraged individual counties and county staff to also provide comments on the specifics of the draft report.

While AMC agrees with the basic principle of providing access to government data, many of the task force recommendations raise significant concerns. Historically, the Legislature has decided certain data to be not public for good reason, including protecting the rights and security of individuals, and to enhance governments ability to provide effective and efficient services to the public. We must remember that a local government's primary role is to deliver services, and there is increasing pressure to deliver those services in an efficient manner with the lowest cost possible.

Over the last week, AMC has heard concerns about the task force report from county human resource directors, GIS directors, and county attorneys. I will try to summarize the issues they have raised, but will not touch on many that have been raised.

First, many of the recommendations have cost implications to local government. For example, the recommendation to publish data request procedures that tell people how to gain access to information, may only be a small expense for any one unit of government, but in total it is a significant amount. We must recognize there is a "snowflake effect" from the many "insignificant" unfunded mandates that are passed on to local governments. At some point, all the "snowflakes"can bring down the building. In addition, county officials believe having the data request procedures readily available at the location where citizens go to get the information can accomplish the goal of this recommendation more efficiently.

125 Charles Avenue, St. Paul, MN 55103-2108
(651) 224-3344, fax (651) 224-6540
www.mncounties.org

The recommendation to restrict local units to charging only the marginal cost of providing the data will have serious financial impacts and will restrict the ability of some local governments to provide certain services to the public. The most compelling example of this occurs in the area of

Geographic Information Systems. For example, it seems that Dakota County would have to furnish their entire GIS database, which cost over $2 million to develop, to an out-of-state company for $1.50, the cost of the disk. The recommendation requiring local units to employ a Data Practices Compliance Officer would also have a serious financial impact.

Serious concerns were raised about the recommendation to restrict a local government's ability to copyright certain government data. It is important to remember that copyrighting data does not impede the public's access to the data. Again, this is a major concern for individuals working on GIS.

AMC believes the intentions of many of the recommendations are good, but feel there are significant problems that need to be addressed before moving forward. Many of the recommendations are vague and conflict with other requirements placed on local units. In addition, a number of individuals believe there are constitutional questions related to at least the recommendation making Commissioner of Administration opinions binding, and take precedence over Attorney General Opinions.

The Association of Minnesota Counties is willing to work with the task force and the Legislature to address the issues surrounding public access to information in this time of great technological change.

Sincerely,

Rose Arnold

Rose Arnold
Stearns County Commissioner
AMC President

Information Policy Task Force Public Hearing 1/6/99

Ladies and gentlemen of the Information Policy Task Force: January 6, 1999

My name is Gary Baran. I live at 3223 Canterbury Court, in Woodbury.

I am not a professional lobbyist for any company, nor a lawyer with an agenda to advance, nor a privacy issues expert by any means, nor do I aspire to be so.

I am here today as an ordinary citizen, taking annual leave to be here. I am one of the many millions of Minnesotans you all are charged with representing.

I have two main points I want to make.

First:

As a person doing family genealogy research, I frequently find it just too expensive to get public information about family members. Costs of $ 11 - 14 per birth certificate, or $ 11 per death certificate, when looking up family tree information, are beyond most normal persons means, unless one cares only about parents and grandparents, excluding all others in ones ancestry.

What really rankles me, is that all this information was collected and is still stored by public agencies, agencies that are publicly funded. I and all the other taxpayers of Minnesota have already paid for this information. Yet, we still have to pay PREMIUM prices, and fill out forms just to access such information. We ALREADY paid for it. It is ours already. Public agencies are only repositories of OUR information. Make it available for free reviewal, without exorbitant costs or difficulties in getting to it. Web access to Birth/Death Certificate Request Forms is nice, but the high costs are still there.

There are hundreds of thousands of Minnesotans doing their genealogy, in every city, town and Legislative district. I attended a national Genealogy conference several years ago, and Genealogy Research is the LARGEST hobby in our country. Too many Minnesotans are not as fortunate as I am, living here in the Twin Cities with closer access to the Historical Society and Health Department offices. Outstate Minnesotans are really hampered in doing the same research as I am.

We have over 800 persons on my wife's side already identified, and about 600 on my side, filling a dozen 3 inch binders of information and pictures. We DON'T need certified copies of birth and death certificates for ALL these people. But for dozens of our ancestors, birth and death information will help us to identify and trace back our family trees.

This is where all of you, as members of this Task Force, can help all of us, in our genealogy searching. Short term, reduce the costs to JUST the cost of photocopying the document, whether 10 or 25 cents, either is fair and reasonable. $11 to $14 is a User Fee structure gone rampant.

Longer term, put this information on microfilm and copies in the Minnesota Historical Society, who can make it available to the public, for free reviewal. MHS may need larger reference room seating, more film readers, etc, but that is all within reason.

My second, and more general comment:

There was discussion in early Task Force meetings, and by only a 5-4 vote, the "Presumption that Government Data are Public" was barely reaffirmed by this Task Force. To me, we live in a society in which government exits to serve its constituents, not to collect and then hide information. Government must keep government data public, not hide it under the guise of too difficult to retrieve or disseminate. Minnesota's citizens paid for its collection. We should be able to access it, freely, at any time. If too much information has been collected, then don't collect that much anymore. What government collects, it must maintain. Collect only what government will accurately maintain. Inaccurate information can be damaging.

As I initially stated, I am only one person, but feel I speak for many, who want access to government data, particularly what can help in our genealogy research, at reasonable costs, not $11 - $14 per certificate. The Task Force's Recommendation # 4 and the associated Rationale is exactly what is needed. I support it entirely.

I thank you for your time and consideration.

LMC
League of Minnesota Cities
Cities promoting excellence

145 University Avenue West, St. Paul, MN 55103-204
Phone: (651) 281-1200 • (800) 925-1122
Fax: (651) 281-1299 • TDD (651) 281-1290

January 6, 1999

Anne Barry, Commissioner of Health
Chair, Information Policy Task Force
c/o Michele Ford
306 Capitol
St. Paul, MN 55155

Dear Commissioner Barry:

Enclosed are the written comments of the League of Minnesota Cities on the draft report of the Information Policy Task Force dated December 30. This initial review represents views of city officials responsible for administering and carrying out duties under provisions of the Minnesota Data Practices Act and related state statutes. The League is aware of task force members' commitment to addressing key public policy issues raised by the rapid change of technology and increased recognition of the importance of public access to information. City officials likewise seek to act upon and respond to a wide range of requests for information
and in an efficient and timely manner and to use technical resources to enhance that capability. City officials are also keenly aware of their responsibilities as stewards of public resources and to be accountable for effective administration of personnel and service delivery.

At the outset, the League wishes to indicate our concurrence with a number of task force recommendations that improve and clarify measures - among them making compliance with Tennessen Warning requirements less burdensome and complicated. The League also appreciates the efforts the task force made to strengthen the role of state government in providing education, training and materials to help guide local units of government in carrying out state information policy.

The League also needs to point, however, that there are serious concerns about other recommendations the task force has proposed. The League urges the task force to take the time necessary to directly involve local government in developing final recommendations and to consider carefully the implications of such proposals at the local level.

City officials are directly engaged in delivering services, including information, to the public and are accountable for doing so in an efficient and responsive manner. In addition, local officials are responsible for employee relations and supervision, service delivery and the design and use of (as well as access to) public government data via information management systems. The League strongly encourages the task force to recommend to the legislature that local government perspectives be examined more thoroughly and that a method to be found to bring that expertise to bear on the discussion of how to improve current state information policy. It is reasonsable to suggest that the legislature extend the term and charge to the task force in view of the far-reaching nature of the changes to state policy reflected in many of the task force recommendations.

The current task force schedule has not permitted sufficient notice or opportunity for local officials to reflect on the implications and outcomes likely to arise from enactment of many of the proposed recommendations. Local officials have had limited time to obtain and digest the full sweep of the final draft of the task force report prior to the public hearing on January 6. Many cities and other local units of government that do not have direct on-line access to the report are effectively excluded from learning the contents of the proposals the task force is considering and reflecting upon them in the public hearing. The League urges the task force to identify additional means for those affected by the proposed recommendations to respond to the current draft.

The League is interested in pursuing avenues that would permit cities to work in partnership with state government to help meet the challenges of providing access to public government data in a period of rapid technological change. City officials recognize the importance of addressing these changes and responding to the opportunities those create for access to information.

Sincerely,

Ann Higgins

Ann Higgins
Intergovernmental Relations Representative

Enclosure

COMMENTS ON THE 12/30 DRAFT REPORT OF THE INFORMATION POLICY TASK FORCE BY THE LEAGUE OF MINNESOTA CITIES

The League of Minnesota Cities takes this opportunity to offer comments on the draft of the report of the Information Policy Task Force to the 1999 Minnesota State Legislature. In doing so, the League retains the option to provide additional comments that reflect concerns and responsibilities of city government. The short time available to develop and transmit comments to the task force left limited opportunity to ascertain sufficiently the insights of local officials who are regularly and directly involved in providing access to government data and development of procedures and policies for that purpose.

Task Force Discussion of Information Policy Principles

The League takes particular note of the task force discussion about the "Tennessen Warning" principle. The task force deliberations on this topic involved extended discussion and the presentation of contrasting points of view by practitioners and those representing both public and private sector interests. As a result, the task force arrived at conclusions that reflect a more carefully considered point of view. The presentation of more detailed positions and explanations helped reveal the complexity of the issues confronting interested parties. Task force members were in a far better position to adopt a principle which recognized the need to make the statute less restrictive and therefore less likely to result in litigation.

Surveys to Determine Compliance

The fact that the Task Force identified the importance of acquiring information on how information policy principles are actually being dealt with in practice underscores the League's view that direct involvement of affected local jurisdictions and the circumstances in which they operate would serve task force deliberations. On the other hand, reliance on written and "secret shopper" survey instruments that illustrated only certain outcomes and provided limited reliability in determining where the need for change is most acute.

Research on the Issue of Electronic Surveillance

While the task force engaged in more extensive discussion on matters related to electronic surveillance, presentations failed to provide necessary explanation of the variety of devices and safeguards that result from the progress of technology and the efforts to protect the public from unreasonable intrusion on their privacy.

Compliance and Enforcement

The discussion of enforcement and compliance issues unfortunately took place at meetings where less than a quorum of the task force was in attendance and failed to involve extensive discussions of and with local and state units of government that have been impacted by the current law enforcement and compliance systems. The fact that the 12/29 (version #3) draft of the report suggests that the task force may be prepared to finalize its recommendations and present the proposed legislation that is appended to the report is a source of some consternation and is disappointing since it leaves little opportunity for the task force to engage local units of government in developing the final form of the report on this topic.

Summary/Conclusion

If, indeed, the Task Force decides to review what is presented at the January 6 public hearing and to finalize that same day its recommendations and legislation to present to the legislature, that process gives insufficient attention to the wide variety of circumstances and factors that affect routine and daily efforts to administer and carry out state information policy at the local level.

Recommended Information Policy Principles

Principles relating to government accountability - The Task Force has indicated that local government authority to maintain data in a variety of media must be predicated equally upon efficiency and facilitating public access. While such a policy position is arguably desirable, the practical implementation of that point could generate substantial costs for local property taxpayers as government is subject simultaneously to both objectives.

Principles relating to the public access to government information - Whereas the Task Force has recommended that government publish procedures to insure compliance with requests for government data, city officials maintain that it is more important for governmental units to establish such procedures and make them easily available. The one-time publication of those procedures or subsequent publications of any changes is not at all as sure a way of serving the public interest as is making the procedures clear and making efforts to provide them to all in need of them.

When the Task Force recommends that public access to government information must be provided solely at marginal cost, local taxpayers will be expected to underwrite the private commercialization of public data collected, compiled and maintained at public cost. While the task force maintains that such costs not cover the expense of creating and maintaining the actual information management system that provides the data, it is clearly a costly requirement to bar government from recovering actual costs incurred to provide the data in the form and content that is requested.

Insistence by the Task Force that government data generally should not be copyrighted without specific legislative authorization again increases the taxpayer burden of covering the public costs of allowing private interests to obtain public data and reap a profit from it. The need to approach the legislature each session for specific approval for copyrighting will be subject to problems of timeliness and be largely unworkable.

The recommendation that electronically maintained public government data be made

available in that form to those requesting the data in that manner forces local jurisdictions, from the wealthiest to the one with a small tax base, to incur the additional cost of designing information systems to not only deliver services to the public in an efficient manner but also to make the public data located there available easily for electronic access and copying. The full implications of doing this have not been addressed and need to be before the task force recommendation is considered by the legislature.

Lastly, when the Task Force maintains that all government data controlled by a private sector entity under contact to perform a government function must be subject to the requirements of the Data Practices Act, chances are that the willingness of the private sector to even entertain the notion of offering such a service will be short-lived. Unfortunately, that may well likely discourage the very types of contracting that would permit smaller units of government to enhance service delivery to local taxpayers.

Principles related to fair information practices, i.e., "Data Privacy." - To insist that cities only collect, store or use data on individuals for purposes strictly authorized by state government (#2) will at least impede if not actually frustrate development of shared data systems and prevent future data links. City officials have also voiced concerns that such restrictions may well create circumstances in which various local government entities will need to collect the same data that may already exist in electronic form for another purpose, thereby increasing local tax expenditures. In addition, restricting local government dissemination of not public data suggests the task force has failed to recognize local control of data which has been collected and maintained by the local jurisdiction. Instead, it is feared that this principle could create the necessity of repeated contact with a centralized authority in order to proceed.

Principles #'s 3 and 5 also appear to re-create the Tennessen Warning in a new setting by insisting that a government entity that wants to collect private or confidential data from an individual must tell that person why; whether the data must be provided; the consequences are of providing it; the uses to which it will be put; and the identity of other entities to which the data will be disseminated. It is imperative that local government be authorized to undertake that data collection without prior notice; and while the Task Force appears to have recognized that, it has provided only limited authority to do so. Insisting that government assure that maintenance of data on individuals within information systems is carried out in an accurate and complete manner appears reasonable on its face (#8), but insisting that the data be kept current may subject the governmental unit to immediate liability and demands that every aspect of such data be maintained to assure accuracy in each and every detail of that data, something which would be extraordinarily costly to undertake and which is likely to be unworkable or unrealizable.

Principle #10 is overly broad in its insistence that government not acquire technology which "will enhance the capability of the agency to conduct surveillance..." unless public notice is given by notifying the Commissioner of Administration. It would appear to be sufficient to provide that local government provide notice in the public proceedings of its governing body. It is simply not realizable to suggest that local units of government notify the Commissioner of Administration in each and every instance where they intend to acquire or employ technology that either does or could potentially allow the recording of information about activities with respect to buildings or service delivery systems deemed critical to the health, safety and welfare of the public.

Principle #11 also appears to foreclose circumstances in which it is reasonable for local government to monitor access to public information. In many instances, requiring persons to identify themselves or explain reasons for seeking access is intended to facilitate response to

those very requests or to create a record to improve management and staffing. Cities have no objection to informing persons that it is using monitoring techniques, but it is more helpful to be given general policy direction in this regard than to be solely and summarily mandated to do so only under strict state or federal authorization.

Task Force Recommendations

A. Recommendations that relate to the information policy principles

Recommendation 3: The League suggests that the Task Force simply provide that government entities should establish procedures to explain how to get access to public information rather than to insist that such procedures be published. It is also more reasonable and workable to recommend that when changes in policy occur, that governmental units shouldupdate those procedures.

Recommendation 4: If the task force wishes to recommend that assessing copying charges be limited to marginal costs, any amendment should provide that government may charge the actual costs of making available unaltered copies or copies of raw data that is available. Otherwise, a reading of this recommendation that excludes actual labor and development costs incurred in the process of re-formatting or compiling that data to provide access to the data requested creates a taxpayer subsidy of a private request. At minimum, it is necessary to authorize government to recoup the actual cost for compiling or arranging data to respond to such requests. It should not be necessary for local government to seek specific statutory authority to charge more than marginal costs to make such information available to those requesting it.

City officials are particularly concerned about the consequences of restricting local authority in in this area. Local taxpayers must not be forced to subsidize private commercialization of public government data collected and maintained at taxpayer expense. It is not acceptable to simply state that ..."it seems to be a reasonable price to pay..." to make public access to that data regardless of the private profit to be made. The League is mindful of comments made on this matter by former task force member Dave Johnson, Chief of Police for the City of Blaine.

Recommendation 5: The League agrees that on-line inspection of data as well as downloading and printing is, in many respects, a form of visual inspection. Butt it is important to provide some restraint and to set some parameters. Otherwise, unlimited access could well obstruct or curtail access by others. It would be well to explore this recommendation further with those who respond to requests by the public for on-line information. While it may be that electronically-shared data may make such requests for public access less of a burden in the future, it is important not to tie the hands of government officials at this time. The current circumstances provide the right to inspect such information at government offices. While placing specific data on the Internet provides for increased public convenience, the task force should be cautious in expanding electronic access without first identifying how to assign responsibility for that access and ensuring government control over such information systems containing that data. Local government has gone a long way to cooperate in placing specific data on-line for the

convenience of the public. That voluntary initiative should be encouraged via North Star II. Mandating placement of local public government data on-line would defeat and further thwart positive steps that are already underway.

Recommendation 6: The League does not agree that the Data Practices Act should be amended to require government to obtain specific legislature authority to copyright various forms of government data. The League does not agree with the task force assertion that "... use of this authority can have a serious and negative impact on the public's right to gain access to government data...". Copyright does not restrict access, including the right to acquire copies of the data or to use it. Cities are in the business of providing services and are not intend on thwarting use of public government data. Although it is still unusual for cities to copyright materials, doing so is undertaken to protect the compilation or analysis drawn from that work. It is not necessary or timely for the legislature to be expected to determine whether certain data should be copyrighted. Rather a general policy should be enacted providing for government tocopyright compilations and original works, and governments using that authority could be expected to report such actions to the Commissioner of Administration on an annual basis, if the legislature determines that such actions would be prudent.

Recommendation 7: When the task force insists that government should be expected to provide copies of electronic data in an electronic format, it should also include the option for government to make that information available in the most cost-effective manner. When it is feasible, government data systems should be developed to provide easy access to public data. The state can do its part to encourage (rather than mandate) that outcome through providing grants and other incentives to local units of government.

Recommendation 8: The open-ended nature of this recommendation leads to the conclusion that the task force may be suggesting an extra-ordinary obligation on the part of government when the means to do so should also be provided by telecommunications service providers in return for the value of using public rights-of-way and limited high frequency spectrum.

The League concurs with the objective that such funding be directed to assure equal access to on-line information services. Local officials suggest, however, that the task force be mindful that offering mechanisms to permit the public to take advantage of programs which offer electronic access to government information should recognize that there are some costly development, maintenance and future improvement endeavors involved that could burden communities with small tax base. Questions regarding cost of providing access to GIS datasets and the issues that arise out of potential commercial uses of the data make such decisions ones which should be made only after careful deliberation and direct involvement by government entities responsible for the collection, compilation, and access to the data.

Recommendation 9: This recommendation follows from a principle to which the League also objected. It is not appropriate for the Data Practices Act to be amended to further limit local government authority to decide how to disseminate not public government data The League finds nothing inconsistent about current provisions assigning responsibility

for data classification at the state level while reserving authority for local units of government to make decisions about how such data is disseminated. To do otherwise would unnecessarily centralize the control of information which local government is in a better position to determine and act upon in a responsible manner.

Recommendation 12: The League fails to understand how requiring government entities to report to the Commissioner of Administration when acquiring any electronic device that enhances the conduct of public surveillance will give visibility to the affected members of the public at the local level. It would be beneficial to define what is to be included in the notion of surveillance. Would it include building security systems, caller I-d, traffic management? What about computer back-up and e-mail systems? This also calls into question how such steps would affect efforts to encourage and support e-commerce.

Recommendation 13: The League opposes the recommendation to amend the Data Practices Act to prevent local government from monitoring public access to public government data. There is nothing nefarious or under-handed about requests for further information from members of the public who seek such information. In fact, those assisting the public in this regard are mindful of their responsibility to respond to such requests in a full and timely manner. Questions regarding reasons for the request can and do assist in turning over accurate and complete information. In fact, at least in some instances, identifying those requesting information helps generate a record to defend against claims of damage or liability.

General Recommendations

Recommendation 15: This recommendation is troubling, both because it would deny local units of government authority to be reimbursed for actual costs associated with providing copies of data that require extensive compilation, redirection of staff time, and re-formatting of data. It is further disturbing to find that the sharp divisions that existed on the task force (among the five members present for this discussion) is not reflected in the rationale statement.

Recommendation 17: The League does not agree that the Data Practices Act should require all government entities to designate a "Data Practices Compliance Officer or Officers" who will be expected to make sure that unit of government complies with the act. Thrusting such broad and extensive responsibility solely onto a minimal number of local officials simply aggravates already difficult circumstances in which cities are expected to comply. (The populations of numbers of cities are actually smaller than in some townships, and yet townships are largely from such provisions.) Assigning DPA responsible authority to local officials with leadership authority is appropriate and does not create a conflict in priorities. Rather, circumstances in which local officials must balance a number of responsibilities will continue in the since many local units of government depend on a few individuals to carry out necessary and critical functions in addition to carrying out the mandates of the Data Practices Act.

Rather, the League suggests that the task force recommend that the legislature encourage local units of government in this regard by recognizing the importance of allowing them flexibility in determining how to assign such responsibility (flexibility) and not mandating responsibility that carries with it the threat of personal liability for non-compliance.

Recommendation 18: Although this recommendation was deferred until budget costs of other recommendations could be further explored, it is imperative that state government undertake a critical role in furthering extensive training and public education on information policy issues. With 3,200 political subdivisions, it is likely that a higher cost for such a program will be necessary.

Recommendation 19: This recommendation has not been given the careful attention it deserves. The League does not believe that the task force has demonstrated that it is appropriate to create an office independent of both the legislature and the executive branch of government. The courts function to resolve complaints; however, the addition of an alternative dispute resolution mechanism to help reduce litigation would be welcome. If the governor is to appoint the official to head an Office of Privacy and Freedom of Information, the League questions how independent and non-political that office be would perceived to be in dealing with information policy issues which the task force agreed are of a "...some time political nature... ."

Certainly, it would be beneficial for the task force to engage in a wide-ranging discussion with affected local units of government of how best to enforce information policy. With involvement from a broad array of interests, it may be possible to arrive at a clear model based on experiences here in Minnesota rather than in Canada.

Recommendation 20: The League does not support the recommendation to provide that opinions of the Commissioner of Administration or the proposed Director of the Office of Privacy and Freedom of Information are binding and to authorize either of those officials to bring about litigation.

Rather, this proposition would appear to further the tension between government entities responsible for complying with the Data Practices Act and the office charged with issuing binding opinions. If, in fact, those opinions were made binding, it would be sufficient to provide government with authority to seek a declaratory judgement setting aside that opinion in order to proceed to act in a manner contrary to the opinion put forward by the commissioner or the director.

There are indeed differences on interpreting various aspects and provisions of the law. The League is concerned that the task force may recommend that such opinions are binding. At the very least, the task force should carefully explore the implications of that recommendation and its counter-part, the authority to compel compliance by court action. Circumstances arising out of efforts to carry out of the law vary widely and result in different points of view on the part of competent counsel. It is important that any recommendation in this area seek balance.

Recommendation 21: The League strongly opposes amending the Data Practices Act to allow anyone to bring action in court with no proof of harm. The proposal would cause a wasteful and unnecessarily costly series of litigations regardless of whether there was any intent to willfully avoid complying with the act. While the League encourages the task force to support alternative means of resolving disputes including mediation, it does not follow that mediators or others authorized to conduct proceedings on such matters should also be authorized to award attorney fees or damages. Such determinations should solely be the result of court action.

The League does not believe that this recommendation puts members of the public in the driver's seat with respect to enforcement. Instead, it would appear that the primary agent would become either private attorneys or measures at the state level to compel compliance.

Recommendation 22: The League maintains that when local governments contract out functions to the private sector, they most often do so to either make it possible to provide services that would otherwise not be available to the public at the local level or to take advantage of enhancements offered to the public in return for access to functions and information of benefit to private sector product or service provision. If the private sector is expected to comply with requirements to administer, collect, receive, store or maintain data in compliance with the Data Practices Act, it is likely that there will be many fewer of such contracts made available to benefit the public. The League is not aware that local government is intent on contracting out functions to avoid public scrutiny. Rather, local government is most often interested in seeing to it that local residents get the benefit of services or improved services that would otherwise not be affordable within the limited resources of that governmental unit.

From: **Anne.Collopy@co.hennepin.mn.us**
To: **michele.ford@senate.leg.state.mn.us**
Date sent: **Fri, 8 Jan 1999 18:44:55 -0600**
Subject: **Re: Information Policy Task Force Schedule**

Michele,

I won't be able to attend the evening hearing on January 19th. Unfortunately, I had to miss the last one (January 6), too, because of a funeral. But I would like to share a few thoughts on the IPTF report and proposals.

Please understand that in this letter I am speaking only as a private citizen, NOT on behalf of Hennepin County (my employer) or any of its elected or appointed officials. I've worked for both State (1968-71) and County government (1972-present) since I graduated from college (1968), always in the field of records management, so I am fairly conversant with the topics being discussed. Therefore, it seemed important to me to offer what observations I could, inasmuch as most private citizens don't even know that the Information Policy Task Force exists, let alone what it is all about.

Although I have not always liked certain parts of the Data Practices Act, I know that the government offices with which I've worked have diligently tried to adhere to its requirements. During many of the IPTF meetings, when participants were particularly critical of "the government", "bureaucrats", etc., I wondered who they were talking about. I often felt that for every instance anyone could give of non-compliance, I could provide an instance of citizen misuse of public data -- and I mean egregious misuse, up to and including first degree murder -- victims' names and personal information having been obtained from "public" data, over which the subject of the data had ZERO control. (Some rights!)

Moreover, for every alleged abuse (and to be honest, I don't recall that more than a few specific instances were presented during the IPTF meetings), task force members either forgot or were unaware of the thousands upon thousands of times each day when government employees and officials provide information upon demand, give Tennessen Warnings, honor releases for not public data, and otherwise comply fully with all provisions of the Data Practices Act.

In the IPTF report ("Discussion of Two Important Principles", page 4), I found the word "presumption" used in paragraph "a" no fewer than six times. This is not correct, as I have been pointing out since about 1978. There is NO "presumption" of openness in the MGDPA; there is a MANDATE of openness. The distinction is not insignificant, and in the interests of intellectual honesty at a very minimum, I wish the correct terminology would be used. Euphemisms are entirely inappropriate in public discourse over such important matters. The public and the legislature have the right to know exactly what task force members are haggling over. Here, I sense that the news media in particular may hide behind misleading terminology, just as they prefer to use "secret" and "secrecy" in place of "private", to give the government a cloak-and-dagger mien. This is extremely disheartening to one who has seen so much goodness, and yes, I have seen very much goodness, in government!

I take exception to the assertion in Recommendation #5 that

"downloading data or printing copies of data is, in this electronic age, a form of inspection of data. This type of inspection of government data, JUST LIKE [emphasis added] inspection by visual examination of paper records. . . ."

Various writers in business and privacy journals have addressed the phenomena of speed and universal access in modern communications. Obviously, people wishing certain data formerly had to seek it physically, which is no longer the case. The implications of this mode shift are probably only beginning to be understood, but I believe they are vast.

There is a quantum leap from visiting a County Service Center to request a specific document, to taking home every document on file in the Service Center. With electronic access, the latter is possible. Now, all sorts of personal data on all sorts of citizens can be readily used for all sorts of purposes by all sorts of people. Only the most naive or the most idealistic (or the most deranged) among us would assume that this is an unmitigated good. Indeed, it should give all of us serious misgivings!

There is probably nothing I can say or do that will change the apparent devil-may-care attitude of the news media and their sympathizers to such unfettered access to citizens' private lives (and I state unequivocally that merely calling a document such as a driver license "public" makes it no less personal and private to the data subject -- who usually has no control over his/her own data, any more than the government does, under the MGDPA.) Much less can I prevent the inevitable downloading of all public data to all computers operated by persons who wish to engage in snooping for whatever reason.

But I will at least point out the very great difference between (a) visiting a government office and (b) taking home all its records! And I predict that a day will come when either we, or some future generation, will bitterly regret allowing this kind of uncontrolled play and manipulation of personal information on private citizens, who now can be victimized in ways hitherto unimagined.

I remember some years ago, when we were in the thick of the Medical Examiner issue (the news media and associates were pushing to make all M.E. records public -- i.e., autopsies, suicide notes, photos, etc.; Hennepin and all 86 other Minnesota counties took the unanimous position that such intensely personal data could be made public with a signed release from survivors, but not otherwise.) I remember a meeting of the parties then involved in the issue, at which a young attorney from one of the outstate counties said, "We find ourselves in the odd position of defending citizen's genuine rights to privacy against the intrusions of the media and every other curious snoop who does not respect them." How right she was. The "evil government", in fact, often seems to stand alone in being concerned to protect the citizens on whose lives we hold so much data, often precious and painful, as well as terribly personal.

Ask the CITIZENS how they feel about their data being made public without their knowledge or consent! Ask the citizens if they would like to know who has come in to a government Service Center counter and requested their home address, birth date (DOB), height, weight, or a wide variety of other personal "public" information, and for what purpose. Tell me that the average man or woman on the street would support this!

Isn't it interesting that for a government agency (or agent) to tap a telephone line, a court order must be obtained first, while any citizen can tap

a wire easily (albeit illegally), with no detection, and without any court order? Not only that, but wiretapping is probably done far more often than most of us would like to believe. I talked to an employee at an office supply store recently who recounted having done it, having broken into people's voice mailboxes readily, and having had some fun in the process (not that the victims knew about or would have appreciated it.) I'd be willing to bet there will be people in attendance at the hearing Tuesday night whose phone calls have been intercepted on more than one occasion -- and certainly NOT by the wicked government.

Surveillance equipment, some of it very high-tech, is standard fare in many computer supply stores today. "The government" is not the salesperson -- or the customer. What protection does anyone have from the kinds of people who might buy this stuff? At least the government has to obey the law and the courts before undertaking reconnaissance missions.

With all that in mind, I would like to offer a few thoughts on the proposed "surveillance device" reporting requirements (Recommendation #12.) Consider the number of businesses that routinely use all sorts of surveillance devices. Banks come to mind immediately, but how about MTC buses, department stores, grocery stores (among other examples, the "mirrors" which are not mirrors at all, but screens for management to watch what's going on), newspaper offices, utilities, clinics. . . . and no doubt the list is much larger than that and growing logarithmically.

Do you have a peep-hole in your front door? Is that a surveillance device? Do you go further and hire Honeywell or ADT to fit your home with intrusion protection? Do you have caller ID on your telephone?

Is there something wrong with any of this? Perhaps only in the mind of the one who would violate your God-given rights -- but I believe the public would enthusiastically support all of the examples I have just provided. I, for one, have absolutely no fear of being photographed OR listened to by any government agency. (Guess what: I'm not doing anything wrong.)

Incidentally, the rental truck used in the Oklahoma City bombing was identified and traced through a surveillance camera.

Government offices are surely no less vulnerable to invasion or attack than homes or businesses. Arguably, they are MORE vulnerable. What the average citizen needs to know and understand is not that there are cameras in the Capitol, but that we live in a surveillance society PERIOD -- and that the government does no more of it than any other business, and probably a lot LESS than many businesses, including and perhaps especially those associated with the news media. The comment on page 19 of the most recent draft of the IPTF Report, beginning with "Development of greater capacity and faster computers. . . . " and ending with ". . . a small step toward beginning that dialogue", speaks once again as though government were an evil entity, indeed the only evil entity, spying on innocent citizens, when the reality is very, very far from that.

After 30+ years of working for the government, I believe that citizens have MUCH more to fear from other citizens and from the news media than from any government agency. "The government" is a wonderfully convenient straw man to hold up for public excoriation and heavy-duty regulation (this, by agencies who will not suffer the slightest regulation of ANY of their activities, nefarious or otherwise.) And oh, by the way, "government" also has lots of juicy information on private citizens that can generate a lot of revenue for the

profit-making news agencies who often appear to delight in involuntary indecent exposure of those same private citizens they purport to defend. Anyone who has witnessed this lobby in action can never look at them naively or trustingly again.

I want to close by reiterating that the opinions I have expressed are solely mine, that they represent NO government agency or official. Thank you for hearing me out.

Budget, Policy and Planning

Minnesota Department of Economic Security
DES
Helping People Help Themselves Achieve Economic Security

Voice: 651/296-3293
TTY: 651/297-2220
Fax: 651/296-7192

306

NUMBER OF PAGES (INCLUDING COVER SHEET): 3

TO: Michelle Ford

COMPANY: Information Policy Task Force

FAX NUMBER: (651) 296-6511 Sent 1-8-99

FROM: Mark Buttala

PHONE NUMBER: (651) 296-8007

NOTES: Departments Response to the Draft Task Force Report.

Office of the Commissioner

Minnesota Department of Economic Security
MDES
Helping People Help Themselves Achieve Economic Security

Voice: (612) 296-3711
TTY: (612) 282-5909
Fax: (612) 296-0994

Jan. 8, 1999

Commissioner Anne Barry
Senator Don Betzold
Information Policy Task Force
306 Capitol Building
St. Paul, Mn. 55155

Dear Commissioner Barry and Senator Betzold;

Thank you for the opportunity to respond to the Draft Report of the Information Policy Task Force. This letter presents the comments of the Department of Economic Security regarding the proposed recommendations contained in the Draft Report dated 12/29/98. While we support the general principles of the report we have the following concerns with those recommendations listed below.

Recommendation 4.
Access to public data is a right that must forever be readily and easily available to our citizens. The existing language of the Minnesota Government Data Practices Act (MGDPA) currently ensures that this right to view or inspect public data is not denied. However, when copies of public data are requested we believe that more than just the marginal costs of production should be borne by the requester. Charging for all costs associated with producing copies of public data rather than only the marginal costs, as proposed in Recommendation 4, would not impact on the public's right to access and would enable recovery of the significant expenditures of staff and financial resources. Without a means of recovering the enormous costs which would result from this recommendation, the delivery of other government services will surely be impacted. Requesters of copies of public data should be responsible for the total costs to retrieve, compile and deliver the data they request rather than just marginal costs.

Recommendation 7.
Government data is increasingly collected and stored on electronic media due to the benefits of increased efficiency and the significant cost advantages that these technologies provide. The data is often provided by the data subject on non-electronic media prior to being converted to some electronic form. The electronic media options to which the data can be converted are changing almost overnight. CD's, floppy disks, PC's, mainframes, DVD disks are but a few. One can only wait to see what electronic options will be available in the future. Decisions as to the electronic storage media used to store data must remain with the steward of the data as long as the public's access to the data is not prevented or unreasonably delayed.

Government entities chose or design electronic media based on the ability to process and produce a specific job or product. The media on which the output is obtained is that which best addresses the needs of the data steward or user. Often the output of electronically stored data is on a non-electronic form, ie. paper. To program or design the output on the ever newly emerging electronic media would require significant expenditures of technical staff and financial resources to write programs to extract and produce data in electronic form. Cost for the retrieval, based on Recommendation 4, is assumed to be the responsibility of the government entity, while the requester is free to determine the specific form of electronic media the copies should take. Requiring that copies of data stored in electronic media be provided in electronic media is a significantly more complex and potentially expensive proposal for government entities. The Department of Economic Security is opposed to Recommendation 7 in its present form and believes it warrants further review before an issue of this magnitude is proposed.

The Department of Economic Security is committed to ensuring that citizen access to data is not delayed or unreasonably denied. However, those items as set out above are very important and should not be overlooked when considering their impact on our ability to continue to provide additional services to these citizens.

Thank you for the opportunity to express our concerns regarding the Tasks Force's report.

Very truly yours,

Mark Butala
Director
Internal Security

cc: Earl Wilson, Acting Commissioner
Al St. Martin, Assistant Commissioner

LMC
League of Minnesota Cities
Cities promoting excellence

145 University Avenue West, St. Paul, MN 55103-2044
Phone: (612) 281-1200 • (800) 925-1122
Fax: (612) 281-1299 • TDD (612) 281-1290

January 8, 1998

Ms. Anne Barry
Chair, Information Policy Task Force
Attn: Michele Ford
306 State Capitol
St. Paul, MN 55155

Dear Ms. Barry:

Thank you for the opportunity to provide additional written comments on the recommendations of the Information Policy Task Force. As a public sector human resources practitioner, I would like to provide some examples of real life situations that city officials may encounter if the Task Force's recommendations are enacted into law.

Recommendations #5 and #7. Allowing public access to public data using on-line inquiry methods and providing data on electronic storage devices/mediums.

- Cities tend to maintain most of their data in inexpensive, off-the-shelf software programs that cannot be manipulated to provide data in any electronic format that is commonly used by the public. These systems come with "canned" reports and often have limited means by which to write custom reports. It is difficult to explain this to a requester who may not be computer literate. It will be more difficult if the law states that they have a right to information in this format.
- Governments maintain a mixture of public and private data in all of their databases, which is separated only at a great cost in staff time. Other proposed recommendations prohibit governments for charging for the cost of this time.
- Many governments are already making tremendous progress in providing the data that is *most commonly requested* by the public on web sites and through other electronic means. Cities have built-in incentives to do this because it is easier, cheaper and saves staff time.

Recommendation #10. Use of Tennessen warning before collection of data for disciplinary purposes.

- It is impossible to know in advance when a question asked of an employee may ultimately result in disciplinary action. To be on the safe side, supervisors will feel compelled to give the Tennessen warning at almost every conversation they have with an employee. While I'm sure that is not the intent of the Task Force, it will be the result in many jurisdictions.

- The Tennessen warning is confusing and frightening to employees, especially younger, seasonal, and part-time employees who have never encountered it before. It has the impact of "chilling" the conversation between supervisors and employees. This results in poor communication and bad management.
- The public sector has enough protections built in for employees; we don't need yet another law to keep us from managing our workforce and thereby serving our taxpayers. We have unions, binding arbitration, discrimination laws, whistleblower laws, civil service requirements, the police bill of rights law, veteran's preference, privacy laws and many others.
- Cities do not have large human resources or training staff to train their supervisors on how to administer this change in law. Most cities do not even have one person in the role of Human Resources Director. They struggle to keep up with the existing human resources laws and still meet the service needs of their taxpayers.

Recommendation 21. Providing the right to citizens to file actions against governments and paying them for their time and attorneys' fees to do so.

- There are numerous reasons why members of the public might file frivolous actions against a government agency. It would be relatively easy for someone to disguise the real reasons for their request and present reasons that appear to be legitimate public purpose. Here are a few examples:
  - Discharged employee with a grudge against the City Administrator/Council.
  - Political opponent of a current Councilmember.
  - Private citizen who doesn't like the current City Administrator wants to find something in the record to remove them from their position (something which generally doesn't exist).
- Cities run across these situations quite frequently. I assume that paying such persons for their time and attorneys' fees would not be the intent of your recommendations but it would be the reality.

I have tried to keep my comments brief and to the point. The Task Force has done a commendable job of representing citizens' rights to access public information. Please take the time now to seriously consider the impact of your recommendations on the taxpayers of Minnesota. The realities I have described above must either increase taxes by adding to the costs of conducting government business or reduce the services we provide to taxpayers.

Sincerely,

Laura Kushner

Laura Kushner
Human Resources Director

Michele, please find attached a Word Document with my response to the Information Policy Task Force recommendations. Please contact me at 651-281-1240 or lkushner@lmnc.org if you have any questions.
<<Data Pract Resp 2.doc>>
Laura Kushner
Personnel Services Manager
League of Minnesota Cities
Lkushner@lmnc.org

January 8, 1998

Ms. Anne Barry
Chair, Information Policy Task Force
Attn: Michele Ford
306 State Capitol
St. Paul, MN 55155

Dear Ms. Barry:

Thank you for the opportunity to provide additional written comments on the recommendations of the Information Policy Task Force. As a public sector human resources practitioner, I would like to provide some examples of real life situations that city officials may encounter if the Task Force's recommendations are enacted into law.

Recommendations #5 and #7. Allowing public access to public data using on-line inquiry methods and providing data on electronic storage devices/mediums.

- Cities tend to maintain most of their data in inexpensive, off-the-shelf software programs that cannot be manipulated to provide data in any electronic format that is commonly used by the public. These systems come with "canned" reports and often have limited means by which to write custom reports. It is difficult to explain this to a requester who may not be computer literate. It will be more difficult if the law states that they have a right to information in this format.
- Governments maintain a mixture of public and private data in all of their databases, which is separated only at a great cost in staff time. Other proposed recommendations prohibit governments for charging for the cost of this time.
- Many governments are already making tremendous progress in providing the data that is *most commonly requested* by the public on web sites and through other electronic means. Cities have built-in incentives to do this because it is easier, cheaper and saves staff time.

Recommendation #10. Use of Tennessen warning before collection of data for disciplinary purposes.

- It is impossible to know in advance when a question asked of an employee may ultimately result in disciplinary action. To be on the safe side, supervisors will feel compelled to give the Tennessen warning at almost every conversation they have with an employee. While I'm sure that is not the intent of the Task Force, it will be the result in many jurisdictions.

- The Tennessen warning is confusing and frightening to employees, especially younger, seasonal, and part-time employees who have never encountered it before. It has the impact of "chilling" the conversation between supervisors and employees. This results in poor communication and bad management.
- The public sector has enough protections built in for employees; we don't need yet another law to keep us from managing our workforce and thereby serving our taxpayers. We have unions, binding arbitration, discrimination laws, whistleblower laws, civil service requirements, the police bill of rights law, veteran's preference, privacy laws and many others.
- Cities do not have large human resources or training staff to train their supervisors on how to administer this change in law. Most cities do not even have one person in the role of Human Resources Director. They struggle to keep up with the existing human resources laws and still meet the service needs of their taxpayers.

Recommendation 21. Providing the right to citizens to file actions against governments and paying them for their time and attorneys' fees to do so.

- There are numerous reasons why members of the public might file frivolous actions against a government agency. It would be relatively easy for someone to disguise the real reasons for their request and present reasons that appear to be legitimate public purpose. Here are a few examples:
  - Discharged employee with a grudge against the City Administrator/Council.
  - Political opponent of a current Councilmember.
  - Private citizen who doesn't like the current City Administrator wants to find something in the record to remove them from their position (something which generally doesn't exist).
- Cities run across these situations quite frequently. I assume that paying such persons for their time and attorneys' fees would not be the intent of your recommendations but it would be the reality.

I have tried to keep my comments brief and to the point. The Task Force has done a commendable job of representing citizens' rights to access public information. Please take the time now to seriously consider the impact of your recommendations on the taxpayers of Minnesota. The realities I have described above must either increase taxes by adding to the costs of conducting government business or reduce the services we provide to taxpayers.

Sincerely,

Laura Kushner
Human Resources Director

Information Policy Task Force Report, Recommendation 6

by Lyno Sullivan, January 9, 1999

January 9, 1999
To: "Michele Ford" <michele.ford@senate.leg.state.mn.us>
cc: "Don Gemberling" <don.gemberling@state.mn.us>,
mn-netgov@egroups.com, mn-politics@mr.net
Fr: "Lyno Sullivan" <lls@freedomain.org>
Re: Information Policy Task Force Report, Recommendation 6

This document <http://www.freedomain.org/^lls/mpdn/19990109-iptf6.html> constitutes my public testimony on certain features of the "Report of the Information Policy Task Force to the Minnesota Legislature" <http://www.state.mn.us/ebranch/admin/ipo/pipa/tfreport.html>.

DEFINITIONS

The term "copyright" covers ALL manner of intellectual property "Work" or "Works", now known and later devised, in "Copyright Law of the United States of America, contained in Title 17 of the United States Code" <http://lcweb.loc.gov/copyright/title17/>.

The term "Work of Government" applies to any Work that is created with any portion of money budgeted by the Legislature or any other entity of government.

The entire collection of all Works of Government is referred to as the "Public Trust".

The term "Public Domain" and "Notice of Copyright" assumes their commonly understood meanings. "Notice", unless otherwise qualified, is equivalent to "Notice of Copyright".

The principle of "Copyleft" is defined in the document "What is Copyleft?" <http://www.gnu.org/copyleft/copyleft.html >. For purposes of this document, the following definition will suffice. "Copyleft" refers to the principle that copyright freedom is best preserved under a license. A Copyleft license assures everyone the following rights: 1) to freely copy, distribute and modify a Work, 2) to incorporate modified or unmodified portions into other works, 3) to sell the Work or provide it at no cost, and 4) to be free of (to disclaim) any implied or stated warranty, on any original or derived work. These freedoms are granted provided that: 1) a copy of the license is either included with the Work or cited at a permanent URL, 2) the resulting work is in an easily modifiable form, free of any intellectual property encumbrances such as patents or proprietary, non-public standards, 3) the resulting work is copyrighted, and 4) the copyright notice also grants the same permissions under these same conditions, and disclaims any warranty.

SUMMARY JUDGMENT

I am strongly opposed to Recommendation 6 as it is currently worded. I recommend alternative wording that fulfills the same intent as the existing Rationale and then expands that intent into a form that assures that the Legislature assume its proper role as the protector of the Public Trust. The Public Domain is not a satisfactory repository for the Works of the Public Trust. The Public Domain may be considered an abdication of stewardship responsibilities for the Public Trust.

The absence of a copyright notice automatically places a Work under Title 17 copyright protection. Therefore, it is my understanding that, every Work of Government must have a Notice of Copyright, even if that Notice were to place the Work into the Public Domain.

The Legislature must, therefore, define the wording that will comprise the Notice of Copyright that shall

be affixed to the Works of Government. Separate Notice text is necessary for each type of data: public, private and confidential.

This judgement does not discus patents, trademarks and other manner of intellectual property, now known or later devised, since the Report did not discuss these topics. I concur with the absence of recommendations for these other forms of intellectual property, until the matter of copyright is suitably resolved.

I recommend that either an existing Copyleft license such as the GNU General Public License (GPL) <http://www.gnu.org/copyleft/gpl.html> be adopted for the Works of Government or that the Office of the Minnesota Attorney General create a Copyleft license that may be written into statute, as the requirement for all Works of Government.

RECOMMENDATION 6:

The Data Practices Act should be amended to require government entities to affix a copyleft Notice to every work of government that is pure public data. The specific notice text should be defined in the Data Practices Act. This notice must include, but not be limited to, fixation on all email, web pages, printed documents, electronic files that contain only public data. Any work that contains private or confidential data must contain a notice of copyright that contains specific wording to be defined in the Data Practices Act. Works that contain a mixture of public, private or confidential data must clearly demarcate each part as to the type of content and, further, must contain all applicable notices of copyright. The markup annotation <public>, </public>, <private>, </private>, <confidential> and </confidential> should be cited in the Data Practices Act.

RATIONALE

The principle of "free" information" carries with it, the obligation of government to take the steps necessary to assure that the information remains "free". Copyleft is a necessary and sufficient step. Beyond that, government should leave the matter of enforcement to the citizenry.

Copyleft is based upon the principles of honor and trust. One need merely observe the operation of the free software community, to understand how effective such public policing can be. Rather than litigating for infringement remedy, the public shame of erring in the matter of copyleft, is usually a sufficient deterrent. When this does not suffice, people often boycott those who infringe.

The statutes that protect the whistle blower and the statutes that protect citizens from slap suits might be reviewed to be sure they would protect people who report situations of copyleft infringement.

I used to recommend that all citizens be enabled to sue, on behalf of the public good, for infringement of copyleft and that they be permitted to keep all damage awards brought to light in their suit. I no longer support this position, because it would have a chilling effect on the utilization of copylefted works. It would create litigation over simple errors of process that are easily remedied. I favor the softer enforcement policy, cited in the previous paragraphs.

I hate those situations where public money is spent to create works that are modified and placed under restrictive licenses, for which the public must pay again.

Thank you for re-considering the matter of Recommendation 6.

Lyno Sullivan, unaffiliated citizen,
Stillwater, MN 55082

Information Policy Task Force Report, General

by Lyno Sullivan, January 9, 1999

January 9, 1999
To: "Michele Ford" <michele.ford@senate.leg.state.mn.us>
cc: "Don Gemberling" <don.gemberling@state.mn.us>,
mn-netgov@egroups.com, mn-politics@mr.net
Fr: "Lyno Sullivan" <lls@freedomain.org>
Re: Information Policy Task Force Report, General

This document <http://www.freedomain.org/^lls/mpdn/19990109-iptf-gen.html> constitutes my public testimony on certain features of the "Report of the Information Policy Task Force to the Minnesota Legislature" <http://www.state.mn.us/ebranch/admin/ipo/pipa/tfreport.html>.

DEFINITIONS

This document makes reference to the Minnesota Public Digital Network (MPDN) initiative which may be viewed at <http://www.freedomain.org/^lls/free-mn/19981222-mpdn.html>. In summary, the MPDN proposes that the Connect Minnesota fiber optic backbone be connected to approximately 100 Local Community Digital Networks (LCDN) that provide a fiber optic connection to every habitable building in Minnesota. Each LCDN oversees the local community issues of 40,000 or so persons. Each LCDN operates under a joint powers commission of the cities and towns that comprise the LCDN. The Connect Minnesota concept of the 20% public thoroughfare and 80% private thoroughfare is extended into the LCDNs and onto the fiber that reaches every work, home and school location in Minnesota. For the monthly basic service fee of $30, each person gets free access to the public thoroughfare, which includes email, public television, public radio, those parts of the Internet deemed appropriate by each local community, and all the not-for profit creative works of humanity. The private thoroughfare has all the fee based programming and full Internet access. In accordance with the precedent established by Connect Minnesota, local community monopolies will be granted to a single vendor (likely a consortium) which will dig up the right of way and lay the fiber within each local community. In Stillwater, the likely private consortium would be NSP, U.S. West and MediaOne and, perhaps, other infrastructure providers that might want to join. The 20% public thoroughfare would be universally available in the basic fee. The consortium, under the guidance of the LCDN and the State PUC, would provide an open market for the sale of digital subscriber services.

PREAMBLE

The IPTF has my sincere kudos for having done an admirable job of protecting citizens from the intrusions of government. My general sense is that some of the recommendations are too generic and that much confusion and cost can be avoided by clearly specifying certain situations, in the manner that I recommend.

I have been a mainframe database designer and programmer for thirty years and am qualified to make certain technical recommendations. I understand that my recommendations may not make political sense.

PROTECTION FROM CITIZEN HARASSMENT

Government needs a workable process for dealing with harassment actions from citizens and groups. An agency needs a clear process, to ask for a ruling by impartial person, perhaps the Commissioner of the Department of Administration (or the Office of Privacy and Freedom of Information), that a request, or a set of requests, constitutes harassment. Government needs an objective process that allows it to say "no" to a data request that is part of a pattern of harassment.

Alternatively, I recommend that the specific requests that are permitted, be specified in statute and by

the agency, upon consultation with the Office of Privacy and Freedom of Information. This is necessary to protect the agencies from the costs of random requests. Further, a given request need only be honored on a periodic basis, perhaps once a year. If I request data today it is reasonable that I get it within ten days. However, it would be a form of harassment if I were permitted to request that same data every ten days.

WORKING DATA OF GOVERNMENT

Government creates much information within its internal processes that is public information. Every government worker must become aware of, and clearly label, which information transactions (email, documents, etc.) are public and which are private. These internal documents, that are public in nature, should be available for public inspection. This is one aspect of opening government to its citizens.

For example, it is reasonable that a citizen be able to inspect the internal public record of why a given decision was made. However, it would be inappropriate to open these working documents too soon, lest too much meddling occur. Perhaps a two year closure would be sufficient. After the period has expired, the working papers, email correspondence, etc. should be made available on the MPDN for public inspection. The "working data of government" needs clarification as a discrete sub-collection of public data.

DATA INSIDE THE AGENCY

In my view, the manner of storing data inside the agency systems is not a matter for the IPTF. I support converting from paper to electronic data and I believe the State needs to find creative ways to help small local governments attain this goal. The MPDN recommends for the creation of a free software based Government Information Toolbox (the GIFT) that furthers this goal.

FORM OF PRESENTATION

When data leaves the agency and is presented to the citizen, the matter of the form of presentation is an essential issue. I believe the IPTF should recommend that all data be presented in a uniform manner. I recommend that proprietary data formats and any data format that is not an international standard should be forbidden. Instead, the IPTF should recommend that all data presented by the agency be in the form of SGML text files. The language of statute needs to allow the international standard of XML, as soon as it becomes available. Beyond SGML now, and XML within a few months, no other alternative makes sense and the matter should simply be written into statute. The statute must also require that a dictionary be available, that defines, at a readable level, each of the markup tags. Every adult must be able to understand the data that accompanies the markup.

I have met with the Information Policy Council (IPC), who are the senior information architects for Minnesota State government, and they seem interested in pursuing this matter of SGML. I ask that the IPTF concur with this recommendation, so the matter can be put to rest and the implementation can proceed.

CITIZEN REQUEST FOR PERSONAL DATA

Each agency knows me by some unique identifier. Prior to requesting my agency data, I must go through a dialogue that establishes my unique identifier for that agency. That agency identifier must then be securely tied to my digital signature. The Office of the Secretary of State has a Digital Signature program <http://www.sos.state.mn.us/digital/digital.html> for this purpose. I refer to this in the MPDN as each person needing a unique, cradle to grave, email address that can become a secure, and authenticated address. These two issues are closely related because I will send an email today requesting data and, within ten days, expect it to be delivered via email. These transactions must be secure. Government cannot accept bogus requests from anyone representing themselves as me. Nor can government send my private data to someone outside government, without my permission. The signature

377

must be so secure that no person, public or private entity can forge my digital signature or snoop into my email content. Interagency sharing of my data must be under my permission, statute or court order.

I believe that every agency must create a process whereby a citizen can say "here is my digital signature or the digital signature of a person for whom I am the lawful guardian, please give me a copy of all the public and private data you have on file related to the digital signature." Beyond that request, I am doubtful of any citizen's right to request specific data about any other citizen, without a court order or without a specific situation, enabled in statute.

If this recommendation ends up in statute, then every agency will know exactly what it must do and implementation can begin immediately. It may take a while for all agencies to comply with a request for data, by digital signature, but this is a matter that is well within the abilities of each agency's software engineers.

I recommend that statute say that the agency has fulfilled its obligation once it prepares an SGML file that contains this data and presents it to the requestor. Those who wish to receive it electronically, can download the file or receive it via MPDN email. For those who wish a paper copy, the agency can run a simple SGML to text process that will produce a formatted report, than can be picked up or sent via regular mail.

DATA SUB-REQUESTS

Agencies are required to provide the "All Data" request described above. I anticipate that many agencies will create requests for specific sets of data, and on a more frequent than yearly basis. For example, is seems reasonable that I be able to email Motor Vehicles and get only the information about a specific vehicle that I own. Each agency will study the situations that warrant specific data requests.

DATA CORRECTION AND INPUT MECHANISMS

As a citizen, I would request my data from all agencies every year or two and review it for factual errors. Beyond that, I would only request specific data when I wanted it. If I noticed any factual errors, I would send an email that notified the agency of the factual error and the correction that is needed. If the agency was assured of my digital signature, certain updates to their data might be permitted based on my input.

Two aside issues: some agencies might merely send me various SGML forms that I can complete and return via email. Other agencies might choose to send me information whenever certain data is modified. Once my email address is secure, there are many transactions of government for which I might like to receive notification. These features help reduce the cost and improve the service level of government.

ORGANIZATION REQUEST FOR DATA

A similar requirement should be established whereby a business or other organization could say "here is my digital signature, please provide the data". In all other matters, this data request should work in the same way that it works for persons.

INTER-AGENCY DATA REQUESTS

Perhaps each person should be able to name all agencies for which they have an interest and the requests can be forwarded to each agency. The resulting SGML files, from each of the agencies, can be collected centrally for single-point distribution. The centralized data routing system can assure that all agencies report either: 1) that they have no data or 2) send the data they have. Existing federal and inter-state data sharing models already do this (without SGML) so it is nothing new. Perhaps this inter-agency data routing system could be made an implementation responsibility of the IPC, since all the right people are part of that committee.

PUBLIC DATA

I recommend that "public data" about persons be defined as narrowly as possible. Except for the specific recommendations that follow, I am opposed to anyone being able to get even my personal public data from government unless I have specifically authorized its public dissemination.

I recommend that "public data" about businesses, organizations, etc. be defined as WIDELY as possible. I believe that the citizens need more information about entities (other than persons and families) contemplated by statute.

MULTI-PERSON DATA REQUESTS

I am opposed to any public dissemination of information about persons, in any aggregate form, except for statistical elements without identifying data (name, address, etc.). I recommend that each agency periodically (no less frequently than yearly) provide a statistical file that contains useful statistical data about every entity the agency has on file. This file should be in an SGML (or XML) format. It should be the responsibility of the recipient to process the SGML file into a usable form.

In terms of geographic location information, I propose that the information be keyed, along political lines, down to the precinct and ward level. Zip code could also be used provided that no overlapping boundaries of geographic location become so narrow that an exact address can be ascertained.

In general, I would err on the side of providing more rather than less data. I recommend that every item of data, that has statistical significance only, be provided. Otherwise the agency will be accused of withholding data. Also, if the agency provides all the data, I cannot see how anyone could ask for more.

The alternative of having to handle each request uniquely, is simply too expensive and draining of agency technical resources. Once all the statistical data is exported into an SGML file, the agency's responsibility is fulfilled. The costs of reducing this data must be the responsibility of those who use the data.

LOCAL GOVERNMENT COSTS

The costs to small cities and towns could become excessive. The cost of a full-time Data Practices Officer alone creates a burden, not to mention the cost of automation. The MPDN initiative proposes that local governments enter into a joint powers agreement to oversee local community network resources. In my experience with the City of Stillwater, Internet Task Force I have determined that a good rule of thumb is the community networks seem to aggregate naturally at the level of about 40,000 citizens within a geographic digital community.

Assuming that 100 or so LCDNs were to be created in Minnesota to oversee the development of network resources within the community, that would be an effective level at which a full-time Data Practices Officer would be cost-effective.

SUMMARY

I understand that these are somewhat radical recommendations. I hope the IPTF will recognize that they drastically reduce the complexity of many aspects of the existing recommendations. Thank you for considering these recommendations.

Lyno Sullivan, unaffiliated citizen,
Stillwater, MN 55082

379

Minnesota Department of Transportation

Transportation Building
395 John Ireland Boulevard
Saint Paul, Minnesota 55155-1899

January 11, 1998

The Honorable Don Betzold
Senator, District 48
306 Capitol
St. Paul, Minnesota 55155

Dear Senator Betzold:

These are the comments of the Minnesota Department of Transportation (Mn/DOT) with respect to the recommendations and proposed legislation contained in the Information Policy Task Force Report to the Legislature. The department agrees that the public should have ready access to government data that are not confidential or private and has always done its best to provide information to the public quickly and with as little cost as possible.

While we support the goals of the task force, we have some concerns with some of the recommendations.

Recommendation #4 would prohibit an agency from charging the public for labor, overhead and development costs incurred by the agency in providing copies or maintaining the data. In general, Mn/DOT charges either nothing or only the marginal cost of providing copies of public data. However, there may be exceptional cases where the department has developed systems or information at significant cost to taxpayers and where the information has commercial value. It would be inappropriate to provide that kind of information free to those who intend to profit from the use of the information at the expense of taxpayers. Of greater concern is the cost of requests for data for ill-defined media investigations or from protesters opposed to agency actions who seek to use information requests as a way to shut down or obstruct normal agency business. An ongoing local media investigation has recently cost Mn/DOT $25,000 to $40,000 to locate documents, separate public from private data, and furnish copies of documents on which private information had been blacked out. The requester and Mn/DOT are still discussing the difficult part of the request, which requires Mn/DOT to review and remove private data from thousands of documents in about 160 employee files so that the documents can be inspected by the requestor. We have estimated that this will require 480 hours. Agencies are increasingly subject to very large and expensive requests. We feel that the agency should not be required to bear the expense of such requests.

Recommendation #22 would require agencies that contract out any of their functions to private sector persons to ensure that any data produced as a result of that function is subject to the Data Practices Act. Recommendation #6 would prohibit government entities from copyrighting any government data without specific legislative authority to do so. One of the functions of the Department of Transportation is to conduct transportation research. The Legislature appropriates money to Mn/DOT to carry out research and technology development. Frequently the Department contracts with private sector consultants or businesses to conduct research and cooperate in product development, particularly in the area of Intelligent Transportation Systems. In some cases the Department forms partnerships and contracts with a private sector partner to develop new systems or products (for example, computerized traffic management equipment and software) that Mn/DOT needs and from which the private partner can later profit in order to spur the development and application of innovative equipment and systems in transportation. A private sector partner will only undertake the development of innovative and expensive products or software which require a monetary investment of its own if it has the potential to profit from those activities in the future. This requires withholding product design or development information resulting from these contracts from competitors who have not undertaken the investments in partnership with Mn/DOT. We also fund research at the University of Minnesota where the U of M patents or copyrights the work product. Although it would be possible for Mn/DOT to seek authority to copyright the product of some partnerships and contracts, because of the number, variety and complexity of relationships that the department pursues in its research activities with the private sector and the University, these activities would be seriously impeded by Recommendations 6 and 22. Therefore, we urge the task force to carefully consider circumstances such as these, where it is appropriate to allow private sector parties carrying out functions contracted for by the public sector, to profit from those activities and to withhold product design information from competitors.

Mn/DOT takes very seriously its responsibility to protect the privacy of its non-public data. Recommendation #7 would require agencies to design data systems so that public data are easily accessible for electronic use and copying. It isn't possible for Mn/DOT to achieve this goal. Minnesota law requires agencies to maintain non-public data and to protect it from release. We are also required to provide public data to requesters.

We create and maintain electronic systems to collect, store, and use data in the most efficient and cost-effective way. In order to protect the security and the integrity of government data, on-line access must be restricted. Mn/DOT was recently warned by a security consultant that its network has vulnerable points where access should be restricted. We don't know of any technology that would allow Mn/DOT to provide on-line access to electronic data and to maintain the security and integrity of the data at the same time.

Recommendation #12 would require a government entity to report to the Commissioner of Administration the acquisition of any electronic device that would enhance its ability to conduct surveillance on citizens. It isn't clear what information would be required. Mn/DOT has thousands of computers and uses television cameras to monitor freeways and to manage traffic flow at intersections. Does the Task Force intend to allow the Department of Administration (DOA) to establish requirements for reporting each piece of equipment? What will DOA do with the information?

Thank you for considering our comments. Please feel free to contact Betsy Parker at 651-296-3002 if you have any questions.

Sincerely,

Barbara Sundquist

Barbara Sundquist
Division Director
Finance and Administration

From: **"Linda K. Hopkins" <lkhopkins@intelliwareint.com>**
To: **"Michele Ford" <michele.ford@senate.leg.state.mn.us>, <michelef@senate.leg.state.mn.us>**
Subject: **Re: (Fwd) Information Policy Task Force Report, General**
Date sent: **Mon, 11 Jan 1999 10:36:24 -0600**

Comments on message from Lyno Sullivan reg. Information Policy Report:

From: Lyno Sullivan <lls@freedomain.org>
She said: "Alternatively, I recommend that the specific requests that are permitted, be specified in statute and by the agency, upon consultation with the Office of Privacy and Freedom of Information. This is necessary to protect the agencies from the costs of random requests. Further, a given request need only be honored on a periodic basis, perhaps once a year. If I request data today it is reasonable that I get it within ten days. However, it would be a form of harassment if I were permitted to request that same data every ten days.

WORKING DATA OF GOVERNMENT

Government creates much information within its internal processes that is public information. Every government worker must become aware of, and clearly label, which information transactions (email, documents, etc.) are public and which are private. These internal documents, that are public in nature, should be available for public inspection. This is one aspect of opening government to its citizens.

For example, it is reasonable that a citizen be able to inspect the internal public record of why a given decision was made. However, it would be inappropriate to open these working documents too soon, lest too much meddling occur. Perhaps a two year closure would be sufficient. After the period has expired, the working papers, email correspondence, etc. should be made available on the MPDN for public inspection."

I appreciate the comments and the time taken by Ms. Sullivan on this matter. However, I disagree with some of her suggestions. I chaired the Working Group on Intellectual Property and Public Access which developed, under the guidance of GIAC, the policy for public access to Government Information within the State of Minnesota. I believe, based on the original policy recommendations made by the Working Group under the GIAC, that some of Ms. Sullivan's proposals would be counter to the public policy functions of Government information. For example, to have public-accessible government information defined by statute means that a majority of the information produced by agency would be considered non-public. Generally, requirements of specificity result in a narrowing of the number of items of any kind becoming included named. In this case, then, the number of types of government information being cited by statute to be accessible by the public would likely be quite reduced in number. This is contrary to the goals of the Working Group; namely, that the majority of information would be releasable and only by falling into certain categories (containing much fewer amounts of information).

I also disagree with Ms. Sullivan that a significant period of time should go by before citizens can access working documents. One of the most

significant rights that citizens under our Constitution have is the right to challenge government's policies and actions. With access to internal public records by citizens being allowed only after two years have passed, the usefulness of such public records for court matters or discussion purposes would be severely diminished. For example, public discussion of a controversial highway or bridge construction could be irreleverant or of diminished value by lack of information about what the actions of the agency were or why they are being done at the time irreversible action is taken.

I would appreciate comments of the Task Force.
Thank you,
Linda Hopkins, J.D.
651-481-0177

For example, it is reasonable that a citizen be able to inspect the internal public record of why a given decision was made. However, it would be inappropriate to open these working documents too soon, lest too much meddling occur. Perhaps a two year closure would be sufficient. After the period has expired, the working papers, email correspondence, etc. should be made available on the MPDN for public inspection."

STATE OF MINNESOTA

OFFICE OF THE ATTORNEY GENERAL

MIKE HATCH
ATTORNEY GENERAL

SUITE 900
445 MINNESOTA STREET
ST. PAUL, MN 55101-2127
TELEPHONE: (651) 297-1075

January 11, 1999

Anne Barry, Chair
Information Policy Task Force
c/o Michele Ford
306 Capitol
St. Paul, MN 55155

Re: Comments of the Office of Attorney General on the Information Policy Task Force Report

Dear Ms. Barry:

I appreciate the opportunity to submit comments on the draft report of the Information Policy Task Force. As noted by Chief Deputy John Stanoch at the Task Force meeting on January 6, 1999, it was not possible to provide prior detailed written comments on each of the recommendations in the report because of the demands in completing the transition in administrations. I have now had a chance to review the report, consult briefly with members of my staff regarding the recommendations, and I have some thoughts that I would like to share with you.

First, it is apparent that many of the proposed recommendations are controversial and warrant further study. It is my strong suggestion to members of the Task Force to revise the report to reflect this. Only those recommendations that appear-- after public comment and deliberation-- to be noncontroversial and broadly supported should be recommended for legislative action during the 1999 session. Those recommendations that are controversial should be acknowledged to be so and only "recommended" for further study.

There are a number of Task Force recommendations which appear, based on the information that I now have, to be noncontroversial. They include clarifying that electronic records are covered by the Records Management Act; providing training to ensure proper disposition of electronic records; requiring publication of government procedures for accessing government data; recommending that government entities consider public access when creating electronic databases; eliminating inconsistent language or language errors in statutes which deal with data practices; funding the creation of model access policies, procedures and forms for state and local government; and providing funding for more data practices training for government employees.

The balance of the recommendations appear to be controversial for a number of reasons.

The recommendations for changing enforcement and remedies for violations of the Act raise the most concern. If adopted, the Task Force would be recommending that the legislature make radical changes to the existing enforcement scheme. The recommendations suggest *both* that a government superagency be established with the power to issue binding opinions on the law and to sue other government agencies which disagree with its interpretations, *and* that private litigation against government be facilitated by the creation of a system that removes standing and damages requirements and that mandates awards of attorney fees and presumptive damages. Putting aside the significant legal and fiscal questions raised by such proposals, it is unclear to me that the record before the Task Force supports such drastic changes. Although I understand that the Task Force heard some testimony regarding noncompliance with the Act, other evidence and testimony submitted suggests that most state agencies and local governmental units are handling the vast majority of data requests successfully. In fact, I understand the Task Force members gave governmental units a "B" grade on their responses to the Task Force's Secret Shopper Survey. On this record, radical changes are not justified, particularly before additional training, model procedures, and alternative dispute resolution options are tried. Moreover, the superagency and damages recommendations do not seem to respond to what both citizens and government entities told the Task Force members they wanted-- quick, fair and inexpensive ways to avoid and resolve data practices disputes.

The recommendations in the report that deal with management and access to electronic data are controversial because they do not deal with the practical and fiscal impacts of increasing direct public access to electronic data bases. Until those impacts are adequately identified and the fiscal and security implications fully understood, no legislation mandating changes to the way electronic access is provided should be recommended.

Several of the recommendations in the report are directed towards eliminating cost barriers, although the Task Force received little direct evidence that the cost of copies represented a significant barrier to citizen access to data. These recommendations are controversial because they do not address how the services will be funded in lieu of the current systems. If data search and retrieval costs cannot be charged back to users as is currently allowed, it is unclear how the cost of government employees providing this service will be paid for. The impact of this recommendation, if adopted, might be worse public access, not better. Similarly, if a portion of the cost of database development can no longer be recovered from those who financially benefit from that data, it will be difficult for state and local government to create and maintain such databases without direct funding from the legislature. Taxpayer interests would also appear to be harmed by limiting the ability of government entities to copyright materials paid for with public funds in a timely manner. Until the fiscal impacts in this area are adequately identified and solutions to the funding problems created, no legislation should be recommended.

A number of other recommendations should be reconsidered. For example, the recommendation to register "surveillance" technology is problematic because it appears to define such technology so broadly that numerous systems would require registration, and also because

the proposal fails to address the main issue, which is not the existence of such technology but abuse of the information collected. For another example, it is unclear whether the recommendation that government be prohibited from asking for identifying information from data requesters is necessary or reasonable. Under current law, access to the data cannot be conditioned on who the data requester is. As other commentators have suggested, there are legitimate reasons for government to collect such information, including insuring compliance with the Data Practices Act, improving information services, and insuring the security of government data and personnel.

Finally, my staff and I have not been able to do a detailed analysis of the draft legislation to determine whether it adequately translates each recommendation into law. However, I note that the draft legislation for recommendation 10 does not appear to implement the recommendation, which seeks to limit the application of the Tennessen Warning in public employment and education contexts. My staff's concern is that the draft language will still require that a Tennessen Warning be given in virtually any routine questioning of a government employee or student.

In conclusion, I would like to state the commitment of this office to represent the public interest of the citizens of this state. Under our constitution, the Attorney General's Office serves different roles. We are officers of the judicial branch, we represent the executive branch, and we are directly accountable to the legislative branch. We also have the *parens patriae* responsibility to represent the citizens of this state. These different responsibilities may appear to conflict from time to time, as when a citizen sues a government agency that the Attorney General is charged with defending. However, I want to assure the Task Force that, while working within the requirements of the law, the members of my staff will work to resolve any conflict in the area of Data Practices to promote the greater public interest, balancing the competing interests of providing public access to government data and preventing unwarranted intrusions on individual privacy.

Very truly yours,

MIKE HATCH
Attorney General
State of Minnesota

AG:174559 v1

Date: January 11, 1999

To: Ms. Anne Barry, Chair
Information Policy Task Force

From: Gail Ryan
Assistant Department Counsel
Minnesota Department of Agriculture

Phone: 296-3378

Subject: **Task Force Draft Report**

Following are some comments and concerns that the Department of Agriculture (MDA) has regarding the Information Policy Task Force's draft report (report). I distributed copies of your draft report to MDA's division directors and asked for their response. Several directors have expressed serious concerns.

1. Recommendation #4, recovery of costs, is a big concern. Our Information/Support Services Director provided me with the following comment: "The paper or diskette are the least of my costs! The labor, development and overhead to produce the requested date are very expensive. We respond to about 300 requests for computer data each year, and each one takes at least 3 hours, including time to estimate, do the report and send it. Since there is no funding in my budget to do this, I must recover these costs from the folks requesting the data. Also, it tends to eliminate frivolous requests." One of our regulatory service divisions has employed a full-time person to handle current data practices requests. MDA receives around 4,000-6,000 requests for data a year, 16-25 a day. Most requests can be handled quickly and with a minimum of expense, if any. However, a significant number of requests are costly.

We have received at least two requests in the past 6-8 months in the regulatory division referred to above that could be considered onerous or burdensome. Both requests were for voluminous amounts of data and could fairly be characterized as somewhat retaliatory for enforcement actions taken by the division. While most requests do not rise to that level of effort and expense, it is important to note that there is an increasing trend toward data requests that consume large amounts of employee time.

2. Recommendation #6 - Several MDA staff persons expressed their concern about possible loss of copyright protection for some of the department's projects. There was a concern that the integrity of the

data could be compromised or that the data could be used in ways or for purposes that were inimical to the intent of the legislation that established and funded the project. We also would be most concerned if it were possible for a member of the public to copyright data that the agency had developed and then be able to charge the agency for the use of that data. That issue must be addressed in any legislation regarding intellectual property rights.

I wonder if copyright authority couldn't be left intact but legislation proposed that would give the public an unlimited license to use the data for any purpose they chose. Copyright law is a specialized area of the law and you may want to establish a small ad hoc committee to look at the issue and make some recommendations. I believe the Attorney General's Office does have an attorney on staff with intellectual property expertise and there are others within the state agencies that have dealt with the issue in relation to professional/technical contracts that could be of help.

3. Recommendation #21 - The MDA is alarmed at the litigiousness that could result from this recommendation. The vast majority of civil servants want to comply with the data practices act and training could go a long way to make everyone more comfortable with its requirements. Rather than taking such a punitive approach, other ideas should be explored before to adversarial processes. The MDA recommends further exploration of the ombudsperson idea, perhaps on a trial basis, to deal with the problem situations. Funding a temporary position in the Public Information/Policy Analysis Section of the Department of Administration should be considered.

One final issue I'd like to comment on is regarding charging members of the public a reasonable fee on top of compilation costs for data with commercial value. I have been involved in many conversations on this subject and have come to the conclusion, as have others, that if data has involved the expenditure of a large amount of public dollars it is the public as a whole not just an individual member of the public that should reap the benefit of commercialization at least until the public dollars have been recouped.

Thank you for all of your hard work on the Task Force and thank you for your consideration of our comments.

MEMO:

To: Michelle Forde
From: Beth Hargarten
Re: Draft Report of the Information Policy Task Force
Date: January 12, 1998

Thank you for the opportunity to comment on the Draft Report. The Department of Labor and Industry endorses the Task Force's objectives of facilitating citizens' full and open access to government data in as easy a manner as possible. We propose that clarification of several of the recommendations set forth in the Report would facilitate the Task Force objectives.

We first suggest clarification of terms used in Recommendations 4 and 15. Recommendation 4 provides that the Data Practices Act should be amended so that "government agencies should only be able to charge for the actual costs of making the copies, and that those costs should not include labor, overhead and development costs incurred by the agency in providing the copies or maintaining the public data." Recommendation 15 provides that government entities should not be allowed to recover the "development costs for producing systems of data that have commercial value."

Our first concern about these recommendations and draft statutory language is that they could create the same confusion about costs that the Task Force is trying to avoid, because the term "development costs" is not defined. The use of that term in the draft language could be interpreted to require the agency to actually create systems of data through unfunded research. A clarification that "development costs" does not obligate an agency to create, analyze or research data would be helpful.

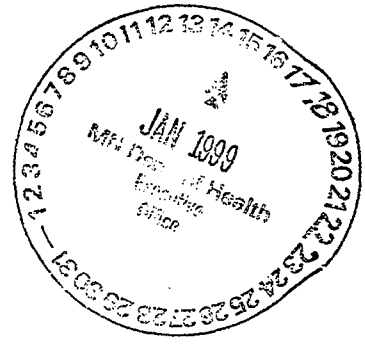
A second concern about Recommendations 4 and 15 is whether the provision that limits charges to the actual costs of copying has been adequately studied. On page 35 of the Draft Report, the Task Force acknowledges that the financial implications of this recommendation are difficult to compute, and that a survey of government entities about the projected cost was not done.

Our agency maintains private data on over a million injured workers, and hundreds of persons who have filed OSHA and other complaints about entities regulated by the Department. The importance of protecting data on individuals collected by the government is one of the principles expressed in the Report and shared by this Department. However, protecting private information in the context of a large data request could be very labor intensive. Therefore, we would like the opportunity to evaluate the cost of the recommendation before it is implemented.

Finally, we note that Recommendation 21 appears to impose "strict liability" on an agency who is not in compliance with the Act. As with any complex law, what is public data is not always clear under the law. We suggest that from a public policy perspective a more reasonable approach would be to impose the liability only after an agency has had the opportunity to obtain an opinion from the agency that enforces the Data Practices Act.

MINNESOTA DEPARTMENT OF PUBLIC SAFETY

Office of Technical Support Services
444 Cedar Street, Suite 140, St. Paul, Minnesota 55101-5140
Phone: 612.296.7589 FAX: 612.215.5792 TTY: 612.282.6555
Internet: http://www.dps.state.mn.us



Alcohol & Gambling Enforcement

Bureau of Criminal Apprehension

Capitol Security

Driver & Vehicle Services

Emergency Management / Emergency Response Commission

State Fire Marshal / Pipeline Safety

State Patrol

Traffic Safety

Ms. Anne Barry, Chairperson
Information Policy Task Force

January 12,1999

Dear Ms Barry,

Thank you for the opportunity to comment on the Information Policy Task Force's draft recommendations to the Legislature.

Attached are comments from the Department of Public Safety's Bureau of Criminal Apprehension. These comments reflect only one of the Department's program areas. However, they are representative of the issues the Department has about the recommendations presented in the draft report to the Legislature regarding changes in the Minnesota Government Data Practices Act as well as the general changes in the way data is handled by state departments.

Please take these comments into consideration in forming your final recommendations.

Sincerely,

Janet M. Cain

Janet M. Cain
Chief Information Officer
(651) 296-9643

cc; Charles R. Weaver, Jr. Commissioner
Nicholas O'Hara BCA Superintendent
Karen McDonald BCA CJIS Section

DPS - Bureau of Criminal Apprehension
CJIS Section

GENERAL COMMENTS:

- These recommendations take an overly simplistic approach to supplying public data and how government agencies should do that.
- Government information systems built to serve a particular function of that agency, do not separate public and private data. Therefore, requests for public data are often difficult to compile.
- These recommendations do not address a very real problem with the Data Practices Act. Government agencies are held accountable for their dissemination of data and are, for the most park, fearful of committing a data privacy misdeed. Therefore, they may be overly conservative about sharing data. The public recipients of this data (individuals or private companies) are not held accountable and have no obligations for the use of the data.
- Government agencies are so conservative about sharing data that they often hamper their own ability to conduct their own business. As we build information systems to integrate criminal justice processes, the biggest problems encountered are not the technical issues but the data privacy issues. For example, even though Prosecution needs certain data to do their job, law enforcement may be hesitant to share the information for fear of violating data privacy. Necessary information is eventually gathered, but after much delay and confusion.
- As much as it seems desirable to have blanket policies for data, there needs to be a recognition of the difference between data on individuals and data not on individuals and even the different kinds of data on individuals and the impact of quick and easy access to that data.
- Unless a government agency's main function is providing public data, a request probably needs to go through a few people. First someone must get a clear picture of what they are requesting to make sure that the data they have and can supply meets their need. Second, a manager must decide who is going to do the job (i.e. which programmer is going to be pulled off a project) and third, a technical person might have to be called in to understand the request as that person will be the one extracting the data.

Recommendation #4:

- There are many more issues for state agencies relating to providing public data than simply providing it. Providing Public Computerized Criminal History (CCH), for example, results in many additional tasks for our staff: developing brochures on how to access & interpret data; answering numerous individual questions about the data; providing training to groups and associations that routinely access the data; working with individuals who have mistakenly been identified as having a criminal record when, in fact the record was on another individual.

- Many of the purchasers of public CCH data are resellers of the data.....companies that are in the business of conducting background checks for employment or apartment rental. They purchase public information from various sources. Their fees are higher than the background check fee charged at the BCA. Many of these companies are from other states and have no Minnesota ties.

- There is some data that government compiles for a specific purpose that does not directly reflect the activities of that government agency. For example, arrest information at a local law enforcement or conviction information at the court may reflect how they are doing their job, but by compiling that data at the state level to make it available to the criminal justice community so that they have the critical information necessary to do their job, may not a reflection how and what an agency is doing.

- Some public CCH data reverts to private data after a certain period of time. That change in classification will be adhered to by government agencies, but will not by private entities (citizens, Minnesota private companies, or private companies from other states) that receive the data. "Private" CCH data bases are being created by companies in the business of selling background check services. They have no obligation to honor the change in classification of that data nor do they have any obligation to correct data or verify identity.

Recommendation #5:

Allowing public access to government operational data bases raises two problems:

1) Operational systems are not always designed to separate the public and private data. While separate data bases can be created there are certainly additional expenses and problems with keeping separate data bases in synch.

2) Public access to operational systems could have a detrimental effect on the users of the systems. CCH, for example, is accessed thousands of times a day by criminal justice agencies throughout the country. Response time is a critical

factor in this system with the national standard being 25 seconds. Public browsing of the system could compromise these critical response times.

Recommendation #13:

The CCH database is one that is constantly changing. We process numerous court orders each month that order the sealing or expunging of the CCH data. Because we log every access to that data from the criminal justice community and from the non-criminal justice background checks that are conducted at the BCA, when we receive an order to seal/expunge data, we notify every entity that accessed that record in the last 3 years. We do not have that ability for data accessed via the public CCH data. Recipients of that data are never notified that data they received is now sealed/expunged and should not be used in decisions about that individual.

Recommendation #15:

- Many of the commercial users of Public CCH are companies from other states. Even those that are Minnesota companies are making money from information the taxpayers have paid to create.