Written testimony for the 12/11/2005 Meeting of the Commission.

The following is my testimony on Agenda items 3, 4, and 5 of the Agenda. This testimony is not from MNOG but is from me as a data practices professional and advocate.

SUMMARY.

Agenda Item 3 - Interplay between state data privacy and federal activity. The method used by the MGDPA to protect the privacy of Minnesota citizens should create a conflict with the federal attempts to get data on Minnesota citizens and residents.

Agenda Item 4 - Artificial Intelligence.
The legislature should carefully consider all of the implications of the use of AI, described by some computer scientists as a threat to humankind, by Minnesota governments. This should include MNIT's development of an AI system that collects and uses data on all Minnesota's citizens.

Agenda Item 5 - Compliance with and enforcement of the MGDPA.
There is a long history of attempts by the legislature to improve compliance and enforcement. The most effective method to do so has been rejected on at least three occasions.

3. Interplay between state and federal law.

Minnesota actually got into the data privacy "business" before the federal government. Our "Data Privacy Act": was enacted before the Federal "Privacy Act of 1974", our Medical Records Act predates HIPAA by several years and protects patients better in far fewer words; and, our Data Privacy Act was enacted about the same time and provides greater rights for parents than the Federal Educational Rights and Privacy Act of 1974.

The most significant issue that results from the interplay between federal and state laws comes from how the Minnesota Data Practices Act, hereafter "Act", protects individual privacy from intrusions by the government.

Since 1974, the Act has required that all Minnesota Government entities, when they ask individuals to supply personal data, to inform those individuals of, among things, the purpose and intended use of the data, any consequences of providing the data, and the identity of other persons or entities authorized by state or federal law to receive the data. (Minnesota Statutes Section 13.04, subd. 2,commonly known as the "Tennessen Warning".)

This requirement to provide the notice is then enforced by language in Section 13.05, subdivision 4, that says that any personal data collected after the notice is given can only be used or disseminated for those purposes communicated in the notice. The legislature has stated some exceptions to this rule.

The interplay of this important privacy protection comes into play at the point when a federal agency asks a state or local Minnesota entity to provide data that was collected after the notice was given. The simple logic of the language cited above says that the data in question can only be disseminated to the federal agency if the individual subject (s) of the personal data were informed that the data they provided would be disseminated to that federal agency. Disseminating data to a federal agency in violation of the DPA could subject a Minnesota entity to liability under the remedies section of the DPA.

The current attempts by the federal government to get voter, human services, public safety, and other personal data clearly puts this interplay
issue before the legislature. It should become an important issue in any litigation brought by the federal government. I am not aware if the Attorney General or other government attorneys are raising this issue with the federal government. If not, they should be doing so.

<u>4. Artificial Intelligence.</u>

Some commentators, including computer scientists who did the groundwork for the creation of AI, have called it a great threat to the existence of human kind. This is one argument among many that hopefully will cause the legislature to take a very exhaustive and long look at how AI is and will be used in Minnesota governments.

The Commission might want to take notice of an historical event that is relevant. In the late 1960's, agencies of the federal government proposed a linkage of all federal government computers into one system. The bi-partisan reaction from Congress was strongly negative. This discussion led to the influential federal study of data privacy, the results of which were published in a 1974 report titled "Records, Computers, and the Rights of Citizens". This and other activities were the basis for the passage of the federal "Data Privacy of 1974".

<u>5. Enforcement and Compliance with the MGDPA, i.e. "Act".</u>

After some years of experience with the Act, it became clear to the legislature and others that lack of compliance and the ability of citizens to enforce the Act were clearly a problem. Of and on throughout the Act's history there have been numerous attempts to improve both compliance and enforcement. Often those attempts were met by strong opposition from both individual government entities and the government associations.

The "successful attempts" included the following: assessing damages for willful violations of the Act; establishing the right to bring an action to compel compliance; allowing a court to assess a civil penalty; giving the Commissioner of Administration the authority to issue opinions in Section 13.072; the establishment of the Administrative Remedy in Section 13.085; and directing the Commissioner to develop and operate a data practices training program in Section 13.073. (Even though I refer to these changes as successful, that does not mean the attempts actually achieved the legislative objectives that drove them.)

The most significant failure (s) in attempts to better enforce compliance with the DPA would have required the establishment of an ombudsperson like office in state government. Three different groups composed of citizens and mixed citizen and government officials studied compliance issues in the last thirty plus years. They included the Government Information Action Council and the Information Policy Advisory Task Force. Each of those groups recommended the establishment of a state government office that would be responsible for ensuring compliance, and when necessary, enforcing compliance. (If memory serves me well, this was also a recommendation made by Jim Nobles when he worked for House Research in the 1970's.) The citizen and citizen/official groups suggested that such an office should be modeled after the Data Privacy and Freedom of Information Commissioners that function in Canadian provinces like British Columbia and Ontario. Bills were introduced to implement those recommendations but they were never enacted. The government associations opposed these attempts at reform. The cost of such an office was cited by some legislators as the reason not to forward.

As a person responsible for working with both government entities and citizens in working with and using the DPA, I continue to support the establishment of a Commissioner type office in Minnesota state government. Offices like this tend to be the model used, not only in Canada, but in other places in the world. My experience of knowing personnel in those offices and seeing the results of their work, has told me that their operations are a far better way to achieve compliance and enforcement.

As always, if I can be of assistance to the Commission, feel free to call on me

Don Gemberling, Retired attorney, civil servant, and data practices advocate since 1973.