Legislative Commission on Data Practices and Personal Privacy

Minnesotans for Open Government*
Written Testimony of Matt Ehling, Board Member - December 11, 2025

Co-chairs Feist and Scott, and members of the Commission,

Minnesotans for Open Government (MNOG) submits the following written comments as background for the agenda item identified below:

Minnesota v. Federal Privacy Laws
(Agenda Item #3)

Executive Summary

MNOG's written comments are specific to how privacy interacts with government records/ government data.

The State of Minnesota and the federal government took distinctly different approaches to addressing privacy issues as they developed their respective "government records" statutes. The federal Freedom of Information (FOIA) law contains broadly-worded privacy language that permits government agencies significant discretion to withhold information that would — in the assessment of the agency — impact personal privacy. Such agency assessments can be contested in court, and the specifics are ultimately determined by judicial interpretation.

In contrast, the Minnesota Government Data Practices Act (MGDPA) was created to "remove … discretion from government entities"** — including agency discretion related to privacy matters. This was done to ensure that government could not use privacy arguments as over-broad "cover" to withhold data that should correctly be categorized as "public." In contrast to FOIA, Minnesota has taken a proscriptive approach — one in which the legislature crafts MGDPA provisions that protect specific, defined data elements from public release, but which is also clear about what data elements remain "public." This differs significantly from the federal approach, which favors broadly-framed exemption language.

MNOG endorses the MGDPA's deliberative, proscriptive approach to addressing privacy in government records. This approach ensures that critical policy decisions about government transparency and privacy are vetted by the legislature through a broad participatory process, rather than flowing from insular administrative decisions made by government entities.

**Minnesotans for Open Government is a non-partisan, nonprofit organization with an all-volunteer board of directors that focuses on government transparency issues.*

***Minn. Comm'r of Admin. Adv. Op. 94-057 (Dec. 28, 1994).*

Extended Comments

MNOG is aware that the Commission's "privacy" agenda item (Item #3) may entail a broader discussion about privacy law, since various state and federal privacy regulations impact consumer data and related commercial activities that are distinct from government records issues. MNOG's comments, however, are specific to how privacy interacts with government records and data.

As an overall matter, MNOG stresses that privacy considerations which involve *government* actors are separate from those that involve *private sector* actors, since certain data about individuals held by the government can shed light on how the government *itself* operates.

For example, a wide variety of criminal justice-related data sets — such as arrest and trial records — pertain to individuals. At the same time, such data sets also illuminate governmental functions — functions that would be much harder to oversee if data about the involved individuals was kept from public view That is why arrest records, for instance, are classified as "always public" data in Minnesota. Converting such records to a "private" status would mean that Minnesota would be facilitating secret arrests (with all the oversight and civil liberties problems that would flow from that).

In Minnesota, the MGDPA regulates public access to government records, as well as privacy protections related to the same. The MGDPA is the state's analog to the federal FOIA statute, but each law handles privacy matters quite differently.

The U.S. Congress initiated the modern era of government records management when the federal FOIA law was passed in the mid 1960s. That law provides for public access to records held by federal agencies, except for nine broadly worded categories (or "exemptions"). Exhibit A to MNOG's comments is a copy of a U.S. Justice Department summary of FOIA's nine exemptions. Each broadly-written exemption describes categories of records that are exempt from disclosure under FOIA. Exemption 6, for instance, contains language stating that "information that would invade another individual's personal privacy" is exempt from disclosure under FOIA.

Likewise, Exemption 7 — FOIA's law enforcement provision — contains similarly broad language. Paragraph 7(c) states that information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy" is exempt from disclosure.

These broad exemptions are contained within a FOIA statute that is just a few pages long — one of which contains the nine FOIA exemptions. These exemptions are effectively the federal versions of Minnesota's "private" and "nonpublic" data classifications, but they function much differently. While the FOIA statute itself is brief, its few pages do not explain how the statute's terse exemption language applies to the myriad record sets held by the federal government. That is explained, instead, by thousands of pages of FOIA case law interpreting the exemptions in specific instances where plaintiffs have sued.

In Minnesota, the Legislature went in a much different direction when it passed the MGDPA in 1979. Rather than starting with broad, exempt categories, the framers of the MGDPA presumed that all government data was public, and then established specific "private" and "nonpublic" classifications around defined data sets. Their intention was that the Minnesota Legislature — rather than government agencies (and then courts, in adjudicating challenges) — should play the leading role in determining what government data would be public, and what would be "private" (or "nonpublic").***

An example of this approach is visible in Exhibit B, which is one page of the "law enforcement" section of the MGDPA (Minn. Stat. § 13.82). Unlike FOIA Exemption 7, which provides federal law enforcement agencies with broad discretion to withhold records in a variety of situations, Minnesota's law enforcement section mandates that some data elements will be public at all times — such as the "brief factual reconstruction of events" that appears in a police report. This ensures that the government cannot withhold key factual information about law enforcement operations that should be public for oversight reasons — a problem that often flows from broadly-framed statutory "exemption" language.

Where § 13.82 affords privacy, it does so in a specific and bounded way, such as by affording crime witnesses the ability to seek privacy protections in certain circumstances, and under a defined statutory threshold. Again, this affords privacy in specific situations, without resorting to overly-broad statutory language that can be used as "cover" for withholding important details about governmental actions.

In general, the aim of the MGDPA has been to engender ongoing policy discussion about where public access should be afforded, and where privacy should be afforded, in a more nuanced way than federal law often allows. Over time, this has resulted in a statute that is much longer than the FOIA law. However, when one considers that FOIA cannot truly be understood without evaluating applicable case law, one realizes that the complexity of government data management will live somewhere — whether in statute, or in the common law.

MNOG's perspective is that the MGDPA — with its close connection to the legislative process — adds significant value by making determinations about data access and data privacy recurring issues that occur before an interactive, public body.

****The MGDPA still provides a role for courts, through a private right of action (§ 13.08) and an administrative remedy (§ 13.085). Those avenues are designed for MGDPA enforcement (§ 13.08 and § 13.085 can be used to challenge failures to provide public data, while § 13.08 can also be used to challenge privacy violations). In MGDPA cases, courts still become involved in interpretive debates, but the number of interpretive issues is significantly limited by the specificity of the MGDPA's statutory structure.*

EXHIBIT A
FOIA Exemptions (U.S. Dept. of Justice overview)

What are the 9 FOIA Exemptions?
Not all records are required to be released under the FOIA. Congress established nine exemptions from disclosure for certain categories of information to protect against certain harms, such as an invasion of personal privacy, or harm to law enforcement investigations. The FOIA authorizes agencies to withhold information when they reasonably foresee that disclosure would harm an interest protected by one of these nine exemptions.

The nine exemptions are described below.

- **Exemption 1:** Information that is classified to protect national security.
- **Exemption 2:** Information related solely to the internal personnel rules and practices of an agency.
- **Exemption 3:** Information that is prohibited from disclosure by another federal law.
- **Exemption 4:** Trade secrets or commercial or financial information that is confidential or privileged.
- **Exemption 5:** Privileged communications within or between agencies, including those protected by the:
    1. Deliberative Process Privilege (provided the records were created less than 25 years before the date on which they were requested)
    2. Attorney-Work Product Privilege
    3. Attorney-Client Privilege
    4. Presidential Communications Privilege
- **Exemption 6:** Information that, if disclosed, would invade another individual's personal privacy.
- **Exemption 7:** Information compiled for law enforcement purposes that:
    - 7(A). Could reasonably be expected to interfere with enforcement proceedings
    - 7(B). Would deprive a person of a right to a fair trial or an impartial adjudication
    - 7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy
    - 7(D). Could reasonably be expected to disclose the identity of a confidential source
    - 7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law
    - 7(F). Could reasonably be expected to endanger the life or physical safety of any individual
- **Exemption 8:** Information that concerns the supervision of financial institutions.
- **Exemption 9:** Geological information on wells.

EXHIBIT B
Portion of Minn. Stat. § 13.82 (Law Enforcement Section of MGDPA)

Subd. 4. **Audio recording of 911 call.** The audio recording of a call placed to a 911 system for the purpose of requesting service from a law enforcement, fire, or medical agency is private data on individuals with respect to the individual making the call, except that a written transcript of the audio recording is public, unless it reveals the identity of an individual otherwise protected under subdivision 17. A transcript shall be prepared upon request. The person requesting the transcript shall pay the actual cost of transcribing the call, in addition to any other applicable costs provided under section 13.03, subdivision 3. The audio recording may be disseminated to law enforcement agencies for investigative purposes. The audio recording may be used for public safety and emergency medical services training purposes.

Subd. 5. **Domestic abuse data.** The written police report required by section 629.341, subdivision 4, of an alleged incident described in section 629.341, subdivision 1, and arrest data, request for service data, and response or incident data described in subdivision 2, 3, or 6 that arise out of this type of incident or out of an alleged violation of an order for protection must be released upon request at no cost to the victim of domestic abuse, the victim's attorney, or an organization designated by the Office of Justice Programs in the Department of Public Safety as providing services to victims of domestic abuse. The executive director or the commissioner of the appropriate state agency shall develop written criteria for this designation.

Subd. 6. **Response or incident data.** The following data created or collected by law enforcement agencies which document the agency's response to a request for service including, but not limited to, responses to traffic accidents, or which describe actions taken by the agency on its own initiative shall be public government data:

(a) date, time and place of the action;

(b) agencies, units of agencies and individual agency personnel participating in the action unless the identities of agency personnel qualify for protection under subdivision 17;

(c) any resistance encountered by the agency;

(d) any pursuit engaged in by the agency;

(e) whether any weapons were used by the agency or other individuals;

(f) a brief factual reconstruction of events associated with the action;

(g) names and addresses of witnesses to the agency action or the incident unless the identity of any witness qualifies for protection under subdivision 17;

(h) names and addresses of any victims or casualties unless the identities of those individuals qualify for protection under subdivision 17;

(i) the name and location of the health care facility to which victims or casualties were taken;

(j) response or incident report number;

(k) dates of birth of the parties involved in a traffic accident;

(l) whether the parties involved were wearing seat belts;

(m) the alcohol concentration of each driver; and

(n) whether the agency used a portable recording system to document the agency's response or actions.