Legislative Commission on Data Practices

January 2026

Summary of Meetings

October 15, 2025

Department of Administration – Data Practices Office (DPO)

- **Taya Moxley-Goldsmith (Director)** and **Casey Carmody (Assistant Director)** provided a structured overview of how Minnesota's data laws work together and how the DPO advises both government agencies and the public on the law.
- They described government data regulation as a lifecycle:
    - Creation of records under the Official Records Act,
    - Maintenance, classification, and access under the Minnesota Government Data Practices Act,
    - Retention and destruction under records management statutes.
- They explained that its primary day-to-day work consists of:
    - Answering questions from government entities about how to respond to data requests,
    - Assisting members of the public in understanding how to make requests or interpret responses,
    - Issuing advisory opinions and guidance.
- They reported:
    - Thousands of annual contacts from agencies and the public,
    - Demand for training, including in-person, webinar, and online formats,
    - That training demand can exceed staff capacity, even though training is the one workload area they can partially control,
    - Law enforcement data questions were identified as the single most frequent and complex category of inquiries.

Discussion

- Discussion centered around:
    - Data retention, minimization, and maintenance operate in a very different environment than in the 1970s, when initial statutes were written.
    - Digital communication tools (email, chats, collaboration platforms) have made it more difficult to determine what constitutes "records" and how long they should be kept.

November 20, 2025

1. Modern Data Privacy Best Practices Around Data Minimization, Retention, and Maintenance

- **Public testifiers** argued that Minnesota lacks a coherent, enforceable framework for data minimization. They warned that without clear statutory limits, agencies retain excessive drafts, metadata, and informal communications that increase privacy risk without improving accountability.
- **Government testifiers** acknowledged the value of minimization in principle but stressed that unclear retention rules make it risky for agencies to delete anything, since deletion may later be construed as unlawful destruction of records.
- **Commission members** discussed the difficulty between modern best practices and legacy approaches, noting that digital systems can now default toward over-collection and indefinite retention rather than intentional minimization. They noted that government agencies often retains data because it can, not because it should.

2. Current Challenges with Data Retention

- **Judy Randall (Legislative Auditor)** emphasized that retention is essential for audits and legislative oversight, especially for audits that routinely look back three to five years. She stressed that retention must include emails, chats, calendars, and collaboration tools, not just formal documents. She acknowledged agency burden and the difficulty of separating public from non-public data but warned that insufficient retention undermines accountability and legislative intent.
- **Public testifiers** described the current environment as a "Wild West," where digital records can be destroyed instantly without notice, review, or appeal. They argued that narrow interpretations of "official records" allow governments to erase decision-making trails.
- **Commission members** noted tension between operational limits and accountability expectations and that the retention rules are likely outdated.

3. Treatment of Geolocation Data

- **Public testifiers** suggested that geolocation data often exists as derivative or metadata, making it harder to classify under existing public/nonpublic frameworks. Speakers highlighted uncertainty over when geolocation data should be treated as private, especially when embedded in otherwise public datasets or operational logs.
- **Commission members** raised geolocation data as uniquely sensitive, noting that location information can reveal intimate details about individuals' lives even without traditional

identifiers. Members discussed the risk that geolocation data exposes a classification gap in Minnesota law: it is highly sensitive but not consistently treated as such, creating privacy risk and compliance uncertainty.

---

4. Intersection of HIPAA/HITECH, the MN Health Records Act, and the MN Consumer Data Privacy Act

- **Testifiers** noted that:
    - HIPAA/HITECH set federal baselines but do not cover all entities or data types.
    - The Minnesota Health Records Act imposes stricter requirements in some areas.
    - The MN Consumer Data Privacy Act introduces new rights and obligations that may overlap or conflict.
- **Government testifiers** expressed concern about compliance complexity and inconsistent obligations depending on who holds the data and for what purpose.
- **Commission members** discussed the confusion caused by overlapping state and federal regimes governing health data. Members also discussed that health data regulation in Minnesota is fragmented and difficult to operationalize, increasing the risk of both over-disclosure and over-restriction.

---

5. ALPR (Automated License Plate Reader) and Body Camera Reporting Requirements

- **Testifiers** highlighted:
    - Challenges with retention schedules,
    - Public access requests for large datasets,
    - The administrative burden of redaction,
    - Risks of secondary use beyond original law enforcement purposes.
- **Commission members** raised concerns about the volume and sensitivity of surveillance data generated by ALPR systems and body-worn cameras. Discussion emphasized that these technologies collect data incidentally and continuously, often involving individuals not suspected of wrongdoing. Members discussed the difficult tension between transparency, privacy, and operational realities.

---

6. Data Privacy and the Interplay of State and Federal Government

- **Public testifiers** emphasized that Minnesota's data practices framework historically requires notice to individuals about who will access their data. They raised concern that federal requests for state-held data may exceed what individuals were originally told,

potentially violating long-standing Fair Information Practice Principles embedded in Minnesota law. Speakers questioned whether Minnesota agencies meaningfully assess whether federal data sharing aligns with original collection notices.

- **Commission members** acknowledged the concern but noted the practical difficulty of reconciling state privacy promises with federal data demands. (Discussion continued December 11, 2025.)

December 11, 2025

---

1. Member Discussion on ALPR and Body Camera Reporting Requirements

- **Commission members** raised concerns about the scale, persistence, and secondary use of ALPR and body-worn camera data. They discussed how these systems generate large volumes of data about individuals who are not suspected of wrongdoing, raising questions about proportionality and privacy.
- Members noted that reporting and retention requirements are difficult to operationalize given:
    - Continuous data capture,
    - Mixed public/nonpublic content,
    - High redaction costs,
    - Long-term storage implications.
- There was discussion about whether current reporting mechanisms meaningfully support transparency.

---

2. Transparent Artificial Intelligence Governance Alliance (TAIGA) – MNIT Presentation

- **John Eichten (Deputy Commissioner)** described the creation of the Transparent Artificial Intelligence Governance Alliance (TAIGA) as a proactive response to the rapid adoption of AI tools by government agencies.
- Key elements emphasized:
    - Recognition that "AI-enabled" tools vary widely in function and risk.

    - Governance must go beyond traditional IT concerns (security, accessibility, sustainability) to include privacy, transparency, user-centered design, and accountability.
    - TAIGA is a cross-functional advisory group designed to guide responsible AI adoption across state agencies.
- MNIT outlined:
    - Guiding principles for AI use,
    - A public AI security standard allowing AI use with public data only,
    - Prohibitions on using AI with nonpublic data,
    - Explicit retention of human decision-making authority over AI outputs.
- **Public testifiers** questioned whether AI is properly regulated under state law, particularly regarding transparency and accountability.

---

3. Enforcement and Compliance with the Minnesota Government Data Practices Act (MGDPA), Including Public Input on Ideas for Improvement

- **Public testifiers** described enforcement of the MGDPA as uneven and often inaccessible to ordinary individuals. They emphasized that while rights exist on paper, practical barriers (like cost, complexity, and delays) limit meaningful enforcement.
- **Government testifiers** highlighted real-world consequences of noncompliance, particularly in criminal contexts where delayed or denied access to data can affect due process and discovery rights.
- **Other government testifiers** also emphasized that local governments strive to comply but face high request volumes, limited staff, and increasingly complex data environments. They warned that compliance failures are often driven by capacity rather than willful delays and stressed the need for clearer rules and realistic timelines.
- Speakers generally agreed that enforcement mechanisms do not scale well with modern data volume and complexity.
