

Legislative Commission on Data Practices Convenes

The creation of the [Legislative Commission on Data Practices and Personal Data Privacy](#) was one of this year's exciting information policy developments. The Commission is a bi-partisan effort to examine data practices issues more closely. The Commission's broad scope includes not only issues involving government data but also privacy and security concerns that the Legislature might address in the private sector.

The Legislature created the Commission to study issues relating to government data practices, individuals' personal privacy rights and to review legislation impacting data practices, data security, and personal data privacy. The commission will:

1. review and provide the Legislature with research and analysis of emerging issues relating to government data practices and security and privacy of personal data;
2. review and make recommendations on legislative proposals relating to the Minnesota Government Data Practices Act; and
3. review and make recommendations on legislative proposals impacting personal data privacy rights, data security, and other related issues.

The Commission has met six times since July and heard testimony from a variety of stakeholders, including government representatives, advocacy organizations and members of the public. IPAD provided a high level overview of the Data Practices Act and our division's functions at the first meeting. The Commission also discussed some high profile topics that have generated considerable media coverage – automatic license plate readers, police body cameras, data about health plans, and education data. Going forward, the Commission is likely to take up the issues of private sector data security, cellular phone tracking technology, and “big data” concerns.

Continued on Page 2.



Inside this issue:

Case Law 2
Update

Advisory 3 & 4
Opinions



(Continued From Page 1.)

The Commission set its meeting schedule for the remainder of the year for the following dates and times:

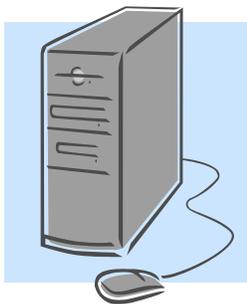
- Wednesday, December 17, 2014 at 9:00 am - Room 10, State Office Building
- Monday, December 22, 2014 at 10:00 am - Room 10, State Office Building

You may sign up for [email notification](#) of future meetings, view meeting materials and listen to hearing audio on the Commission's [website](#).

We look forward to following the Commission's work and participating in the resulting conversations about data practices. We will continue to keep our customers informed about the Commission as its activities and discussions progress.

Case Law Update

Gregerson v. Hennepin County, File No. A14-0487 (Minn. Ct. App, October 6, 2014, unpublished).



After Chris Gregerson won a copyright infringement lawsuit against a third party defendant, he sued the third party and the third party's lawyer for malicious prosecution, abuse of process and conspiracy, but was unable to procure enough evidence to win the suit. In an unrelated matter, one of the third party's companies was under criminal investigation and his computer hard drives were confiscated by police. Police received search warrants to conduct keyword searches to inspect the hard drives for evidence of specific criminal matters. Gregerson requested that the police run additional searches for terms that would lead to evidence related to his case. The police refused, and Gregerson brought suit against the county. He lost at the trial court, and appealed.

The Court of Appeals affirmed the trial court's decision, and ruled that the data on the hard drives were in the possession of a government entity, and as such were government data. However, the data were not public because the U.S. and Minnesota Constitutions protect against unwarranted searches. Citing *Riley v. California*, 134 S. Ct. 2473 (2014), the Court reasoned that under the Fourth Amendment, police cannot search beyond the scope of their warrant, even if the item is in their custody. The owner of the confiscated item still has a reasonable expectation of privacy in the item's contents that are unrelated to the permitted search. Any search beyond what was permitted in the warrant would be a violation of the owner's Fourth Amendment rights.

Driver's Privacy Protection Act Cases: Since June of this year, the U.S. District Court for the District of Minnesota has issued fifteen opinions concerning the federal Driver's Privacy Protection Act (18 U.S.C. § 2721) ("DPPA"). The DPPA cases allege that law enforcement illegally accessed an individual's driver's license data. The recent DPPA decisions were issued on motions to dismiss brought by defendants based on the tolling of the statute of limitations and failure to state a claim. In all cases, § 1983 claims (civil rights violations), invasion of privacy claims, and claims against the Commissioner of the Department of Public Safety were dismissed. Cases with claims that were not dismissed will continue on in the litigation process, while cases with all claims dismissed have the opportunity to appeal to the 8th Circuit.

Advisory Opinion Update

PROCUREMENT DATA

[Opinion 14-011](#): A requester asked for all data submitted in response to RFPs for third party auditors to conduct, or help conduct certain audits, and all resulting contracts. The request was denied based on the entity's conclusion that all of the data are not public data that "relate to an audit" under section 3.979, subdivision 3(a). Section 13.591, subdivision 3, generally classifies most of the data in question as public, once the selection/evaluation process is complete (except trade secrets), other than data "relating to an audit" under section 3.979, subdivision 3(a).

****Pursuant to Minnesota Statutes, section 13.072, subdivision 2, "[t]he commissioner ... shall indicate when the principles stated in an opinion are not intended to provide guidance to all similarly situated persons or government entities." The Commissioner does not intend for this opinion to be generally applicable.***

EMPLOYEE SURVEY DATA

[Opinion 14-012](#): A requester asked for the "raw data file" that contained de-identified employee responses to a survey. The request was denied based on section 13.43, subdivision 7(a), which classifies the data as private personnel data. Personnel data are defined as "data on individuals"; the data in question are not data on individuals because an individual cannot "be identified as the subject of that data" (section 13.02, subdivision 5). Therefore, the data are not personnel data, and are presumptively public. The city's contractor that conducted the survey said it would "sanitize" the raw data to remove the identity of *responders* before providing the "raw data file" to the entity; any data that could identify an employee who was the *subject* of a suggestion are private personnel data.

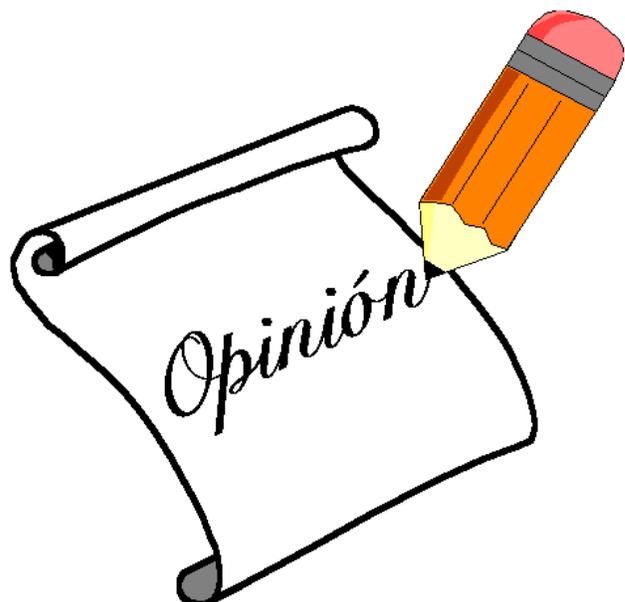
LAW ENFORCEMENT DATA

[Opinion 14-013](#): A requester asked for service and response or incident law enforcement data made public pursuant to section 13.82, subdivisions 3 and 6. The entity cited section 13.82, subdivisions 7 (active investigative data) and 13 (victim access to investigative data) and section 260B.171, subdivision 5 (peace officer records of children) to deny access to all data. The provisions cited by the entity are not applicable to the requests; the entity should have provided the requester with all public data that was responsive to her request.

OPEN MEETING LAW

[Opinion 14-014](#): A member of the public asked whether a public body properly closed two meetings to discuss the purchase of property, pursuant to section 13D.05, subdivision 3(b)(3). At the meetings, both the Mayor and the City Attorney made comments preceding the closing of the meetings. The statements were insufficient under the OML because the statement must be given by the public body, include the grounds permitting or requiring the meeting to be closed, and specifically describe the subject of the meeting. Additionally, for sale or purchase of property, the statement must identify the particular properties.

Continued on Page 4.



Advisory Opinion Update, cont.

OPEN MEETING LAW

[Opinion 14-015](#): A member of the public asked whether a city council's conduct under the OML was proper on eight different occasions. The council's "work sessions" were special, not regular meetings, but the Commissioner could not determine whether the council complied with the special meeting notice requirements under section 13D.04, or held an improper meeting via email. The council did not properly close meetings and discussed impermissible topics in closed session, per section 13D.01, subdivision 3, and section 13D.05. The council also improperly excluded members of the public who were not disruptive. It did not comply with section 13D.05, subdivision 3 (a), because it did not provide the required summary of a performance evaluation. It did not comply with section 13D.01, subdivision 6, because a public copy of members' materials was not available.

DECEDENT DATA

[Opinion 14-016](#): An entity asked whether it could release private data about a decedent to the decedent's sister, who was not the personal representative within the meaning of section 13.10, subdivision 1(c). However, she is a trustee for purposes of a wrongful death action under section 573.02, subdivision 3. The county may release "appropriate" data (however classified) without a court order to the decedent's sister, as a trustee in a wrongful death action as provided in section 13.10, subdivision 3.

OPEN MEETING LAW

[Opinion 14-017](#): A requester asked whether a public body properly closed two meetings on the basis of attorney-client privilege pursuant to section 13D.05, subdivision 2(b). In applying the balancing test required by the Minnesota Supreme Court, the first meeting was improperly closed because the body had not yet decided to act upon

an underlying issue, which barred the body from initiating legal action. The potential opposing party attended a portion of the second meeting, so the attorney-client privilege exception does not apply because those circumstances do not dictate the need for absolute confidentiality. However, the remainder of the meeting at which the attorney for the body discussed legal options and strategies with the body was properly closed.

CONTRACTS/NON-DISCLOSURE AGREEMENTS

[Opinion 14-018](#): A requester asked for access to copies of contracts and non-disclosure agreements for cell phone exploitation equipment. The entity said it could not redact the documents because they contained inextricably intertwined trade secret data (section 13.37, subdivision 1(b)), and "deliberative process/investigative techniques" data (section 13.82, subdivision 25). Contracts and non-disclosure agreements contain standard clauses that are presumptively public. Accordingly, the entity must redact any data that are properly classified under sections 13.37 and/or 13.82, and release the remaining public data.

INTERNAL AUDIT DOCUMENTATION

[Opinion 14-019](#): A state agency asked about its classification of data determination related to an internal audit of one of its grantees, including supporting documentation and other documents collected as part of the audit. The grantee is a political subdivision, subject to Chapter 13. The documentation includes data about employees, members of the public, and credit card, bank account, and Social Security numbers. In addition, it includes the grantee's response to the internal audit report, copies of the grantee's audit reports, and copies of some board minutes. Some of the data are classified as private pursuant to sections 13.43, 13.355, and 13.37. The remainder of the data in question are presumptively public, per section 13.03, or expressly public personnel data under section 13.43.