MINNESOTA DEPARTMENT OF ADMINISTRATION

FYi

From the Information Policy Analysis Division

Volume 11 Issue 1
Winter 2012

The legislative session begins—IPAD advances its proposal

A new legislative session started on January 24th and IPAD has put forward a data practices/open meeting policy proposal that addresses many different topics, with the focus on issues we hear from many of our customers. The proposal has gone through the executive branch's agency initiative process, and the language is now available for the public. IPAD also prepared a summary of the proposal.

On December 12, 2011, IPAD invited stakeholders to provide their feedback at a meeting open to the public. Language for the proposal was not available at that point so the meeting revolved around general principles the proposal hoped to address. Some examples of feedback from the meeting include:

- **Data Challenge Appeals**: IPAD's goal in the proposal is to address government using staff resources to respond to improper data challenges that are actually challenging a process, rather than the accuracy of data about an individual (see Minnesota Statutes, section 13.04, subdivision 4). A concern was expressed over whether the language change would remove an existing individual's right to challenge data about themselves, including one's opinion about another individual. We also heard from a government entity that a language clarification may be useful for government staff that deal with improper data challenges.

- **Security Information**: IPAD's goal in the proposal is to create consistency in the use of declaring data to be security information (see Minnesota Statutes, section 13.37). The proposal currently requires determinations of the classification of security data as not public to come from a Responsible Authority (RA), and requires a short description explaining the necessity for that classification. IPAD heard concerns about the potential difficulty in implementing these measures for larger agencies. IPAD also heard general concerns that security data is being used too broadly to classify data as not public.

- **Personnel data**: In the proposal, IPAD is attempting to address the current inconsistency across the state that some local governments consider their elected officials (i.e. city council members, school board members, county commissioners) to be government employees, and therefore subject to the personnel data section of the Data Practices Act (see Minnesota Statutes, section 13.43), while other local governments do not – making all data about their elected officials presumptively public. Some feedback on this change focused on concern in not having a specific "public data list" for local government elected officials if they are removed from the personnel data section.

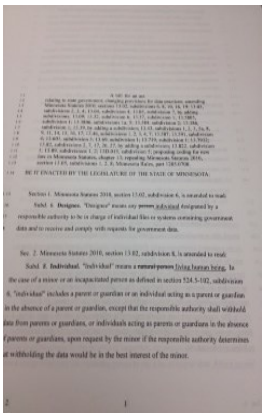
On January 23, 2012, IPAD also shared details of the policy proposal at a meeting sponsored by the Minnesota Coalition of Government Information (MNCOGI), which was streamed live and archived on The UpTake. The purpose of the meeting was an open discussion of potential data practices or open meeting legislative proposals.

Continued on Page 2

INSIDE THIS ISSUE:

IPAD's legislative proposal

Continued from Page 1



MNCOGI discussed their own policy proposal ideas, which include limiting how entities may use the classification of security data and requiring state budget negotiations between the Governor and Legislative leadership to be videotaped. MNCOGI had not found a sponsor for their proposals at the time of the meeting.

IPAD has already made a few changes to the proposal based on discussions at these meetings, as well as other customer suggestions and concerns. IPAD's ultimate goal is to foster conversation over ways we can promote clarity, readability, and an overall better understanding of data practices and open meeting laws.

We are always looking for feedback, which you can send to info.ipad@state.mn.us.

Caselaw update

Plaintiffs in a recent federal 8th Circuit Court of Appeals case argued that the Missouri Department of Revenue had violated the federal Driver's Privacy Protection Act (DPPA) by selling personal information about drivers to certain third parties.

The Court held that bulk obtainment of personal information for future use is not a per se violation of the Driver's Privacy Protection Act (DPPA). The Court also held that obtaining an entire database for the sole purpose of reselling the information does not violate the law because the Act specifically allows the resale and redistribution of the personal information.

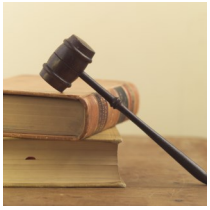
Cook v. ACS State & Local Solutions, Inc, et al, 663 F.3d 989 (8th Cir. 2011).

IPAD presents to AARP 'fraud fighters' on data practices issues

On December 13, 2011, IPAD presented data practices related information to the Fraud Fighter volunteers at a seminar of the American Association of Retired People (AARP). The presentation provided practical advice on the Data Practices Act, such as types of information the government collects about individuals that are presumptively public. It also highlighted a part of IPAD's legislative proposal classifying certain financial data in an inactive investigation as private. IPAD hoped to receive feedback on this portion of its a proposal from a group that is very active in preventing identity theft.

OAH issues data practices order

The Office of Administrative Hearings (OAH) issued its most recent data practices order under Minnesota Statutes, section 13.085. The ALJ dismissed the complaint.



Advisory opinion highlights

Tennessen warning requirements

Opinion 11-017: An employee asked if his rights were violated when his county employer collected his fingerprints and other private data, including Social Security number (SSN), and did not provide a Tennessen warning notice (see Minnesota Statutes, section 13.04, subdivision 2) prior to collecting the data.

The Commissioner discussed the contents of an email sent to all county staff prior to the data collection (which the county argued constituted the Tennessen notice) and found that it met some of the notice requirements. However, the notice did not adequately explain the consequences of supplying or not supplying the fingerprints. In addition, going forward, the Commissioner discussed that it would be helpful to clearly label a Tennessen notice as such. Finally, the Commissioner noted that if an entity is collecting an individual's SSN, federal law imposes some additional notice requirements.

Maltreatment data

Opinion 11-018: A minor student is alleged to have engaged in the maltreatment of another minor student; district employees filed a report under Minnesota Statutes, section 626.556. The district asked what data, including surveillance video from the hallways, written communication between district staff and the social services agency, and amongst district employees and administration, that it must provide to the parent about her/his child, who is the subject of the allegations of abuse.

The Commissioner discussed that it appears that the data in question are classified either by Minnesota Statutes, sections 13.32 or 626.556, subdivision 11. It is also possible that some of the data are classified by Minnesota Statutes, section 13.43. The parent of a minor student has the right to gain access to private data about him/her. The identities of the mandated reporters are confidential.

School board correspondence

Opinion 11-019: A school district asked about the classification of certain school board correspondence. Correspondence (email) sent from one individual to more than one school board member, or sent to one board member by more than one individual, is private data under Minnesota Statutes, section 13.601, subdivision 2, if neither the sender(s) nor board member(s) has previously made the email public. If such an email is classified as private data, the Commissioner opined that the school district is not required (in response to a data request) to seek a decision by the board member(s) or individual(s) senders as to whether s/he/they choose to make the email public. If such an email is classified as private data, it must be released in response to a data request if one board member or one individual sender chooses to make it public.

If any sender or recipient has forwarded an email or shared the contents of an email with a person or entity (other than the district), the email is public data.

Open Meeting Law

Opinion 12-001: An individual asked if a school district violated the Open Meeting Law (OML) when it conducted an open meeting (a 15-minute presentation by the superintendent with a quorum of school board members present) then broke in to small discussion groups where the board members were in separate locations and could not hear and/or see one another.

The Commissioner concluded that a quorum of the full body did not participate in any of those discussions and therefore the board did not violate the OML. The Commissioner also acknowledged the requester's concern that the Board violated a purpose of the OML as articulated by the Minnesota Supreme Court, i.e., "to afford the public an opportunity to present its views to the [public body]." *Prior Lake American v. Mader*, 642 N.W.2d 729, 735 (Minn. 2002). However, the OML does not provide the public with the right to speak at a public meeting.

In addition, the requester asserted that the board violated the OML because it did not create meeting minutes. The Commissioner noted that the OML does not require a public body to do so.