FYi

From the Information Policy Analysis Division

Volume 12 Issue 1
Winter 2013

New legislative session brings both new and old data issues

The Minnesota Legislature convened on January 21, 2013. With a new legislative session, we've seen many new data practices related bills. Senate bills will go through the Committee on Judiciary chaired by Senator Ron Latz. The House Civil Law committee chair Representative John Lesch created a Data Practices Subcommittee chaired by Representative Steve Simon. The House bills will ultimately pass through Civil Law as well. Some data practices bills have made it through the committee stage in either the Senate or House, while others await a hearing. However, legislators from both sides of the aisle have expressed their commitment to addressing data practices during this year's session.

Here are some data practices issues that have already received attention this session.

Health Insurance Exchange Marketplace (HF5/SF1) The legislation creating the Health Insurance Exchange Marketplace (as part of the Federal Affordable Care Act) contains a number of data practices and open meeting law provisions. The House and Senate each passed their own versions of the bill and they await a conference committee to work out the differences. Both bills subject the Minnesota Insurance Marketplace Board to the Open Meeting Law (Minnesota Statutes, chapter 13D), and have provisions allowing for certain meetings to be closed (such as personnel negotiations or where certain not public data are discussed). Each bill also classifies certain data used within the Marketplace as not public, and provides for circumstances when data may be shared or disseminated outside the Marketplace.

Automatic License Plate Readers (ALPR) The Commissioner of Administration will soon approve or disapprove a temporary classification request by the City of Minneapolis for data captured by law enforcement using Automatic License Plate Readers (ALPR). In the meantime, bills on the collection, classification, and retention of ALPR data were introduced. **HF474/SF385**, as introduced, classifies ALPR data as confidential or protected nonpublic and requires law enforcement to immediately destroy data at the time of collection if not part of an existing law enforcement proceeding. The Senate version of the bill was amended by classifying ALPR data as confidential or protected nonpublic if the data are part of an active criminal investigation.

Continued on page 2

Inside this issue:

Advisory opinion highlights 3

Caselaw update 4

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Legislative update, cont.

All other ALPR data are private or nonpublic and must be destroyed 90 days from the time of collection, with certain exceptions for "Safe At Home" participants. Law enforcement will be required to maintain a log of its collection and use of ALPR data. The Senate bill has passed the Judiciary Committee and awaits a floor vote. **HF488/SF210** classifies data as private/nonpublic and requires data to be destroyed within 24 hours, with certain exceptions.

Government entity data breaches Currently under section 13.055, a state agency is required to provide notice to individuals when there has been a data breach or unauthorized access of not public data. **HF183/SF211** expands the breach notice requirement to include local government entities and requires a report on the findings of any investigation into a security breach. The bill, as introduced, also increases the potential criminal penalty for a willful violation by a public employee from misdemeanor to a gross misdemeanor. The Senate version, as amended, removes the gross misdemeanor provision and allows an individual to access the name of persons who have obtained access to private data on the individual, unless the data are part of an active investigation. SF211 was passed to the Senate floor.

Public employee settlement agreements and public officials **HF604/SF1143,** as introduced, creates an additional requirement for agreements settling any dispute that involve a payment of more than $10,000 to a public employee. In addition to the current requirement of providing the specific reasons for the agreement, entities must also describe the nature of the acts, omissions or other events that gave rise to the potential liability. The bill also clarifies the definition of a "public official" and expands the circumstances when all investigative data about a public official are public. The House version was amended by removing the settlement agreement provisions from the bill, but continues to clarify and expand the definition of a public official. The House bill passed the Data Practices Subcommittee and Civil Law Committee and will next be heard in the Education Policy Committee.

Personal contact information Currently, citizen contact information collected by government entities for electronic mailing lists (i.e. snow emergency or city council agenda notifications) are public data. **HF20/SF60** would classify the personal contact information collected for notification or information purposes as private data. The House version has been heard in the Data Practices Subcommittee and the Civil Law Committee and was amended to include protection for data related to an individual's online account or access procedures. The Senate version received a hearing in the Senate Judiciary Committee and was laid on the table to be heard again at a later date.

Stay tuned… Some of these bills may be incorporated into an omnibus data practices bill (likely to be **HF695** in the House). Be sure to check the Spring FYi for a complete legislative recap of all new laws that pertain to data practices and open meetings.

Advisory opinion highlights

Data about elected officials

Opinion 12-018 A member of the public asked whether an entity improperly released private data about a board member. At the time it released data to the public, the entity's human resources director considered board members to be entity employees. The board passed a resolution that members are not employees six weeks later, and there was no evidence in the record that the entity had taken any other affirmative action regarding their employment status before then. Accordingly, the data were personnel data about the board member, regardless of any action to the contrary the board took subsequently. The entity was obligated to determine the classification of data before releasing it to the public.

Communication on personal devices

Opinion 12-019 An entity asked whether communications sent by its board members from their personal accounts and equipment were government data and if so, how those data were classified. When the board members were acting in their official capacity in calling, emailing, or writing, the data were government data subject to Chapter 13. The communications are classified as public under the general presumption, and residential address and email or telephone number are public data as well, pursuant to section 13.601, subd. 3(b), as well.

RFP process and re-solicitation

Opinion 13-001 A member of the public sought access to data related to a request for proposal (RFP) under the process in section 13.591, subd. 3(b). The entity cancelled procurement for the original contract prior to completion of the evaluation process, and three weeks later, re-solicited two new RFPs for the project. The entity's decision to cancel the RFP did not mean it "abandon [ed] the purchase" (at which point data that are otherwise protected become public), even though the scope of the re-solicited RFPs differed from the original, the project that is the subject of the RFPs is unchanged.

Access to actual data

Opinion 13-002 A member of the public asked whether an entity responded properly to a request for certain personnel data it maintained. The requester asked for copies of the job application and supplement of a current employee. The entity responded by creating a list of public data elements but did not make copies of the actual documents. The entity did not respond appropriately; it should have provided access to the actual data after redacting not public portions of the documents. The plain language of section 13.03, subdivision 3, states that requesters "shall be permitted to inspect and copy public government data."

Request for property inspection data

Opinion 13-003 A member of the public asked whether an entity responded appropriately to a request for property inspection data. The requester made her original request in December of 2011, after which the entity stated that she had received all data related to that request. She subsequently received data she considered responsive to that request in June 2012. Due to the nature of the correspondence between the requester and the entity, the Commissioner was unable to come to a conclusion as to whether the entity responded appropriately, though it appeared it acted in good faith throughout the communications.

Definition of 'public official'

Opinion 13-004 A member of the public asked for access to data related to the departure of a director in a city, pursuant to 2012 amendments to section 13.43, subdivision 2(e)(iii). Although the director worked in a management capacity for the city, which has a population of more than 7,500, he did not report to "the chief administrative officer or the individual acting in an equivalent position." Therefore, under the plain language of section 13.43, subdivision 2(e)(iii), he is not a public official, and neither are the City's police and fire chiefs, among others in City management positions.

Continued on page 4

Caselaw update

The Court of Appeals denied a request to have case records sealed in ***In re Opela*, No. A11-2063 (Minn. Ct. App. July 2, 2012, unpublished).** An Administrative Law Judge (ALJ) originally denied the request based on a lack of legal authority. The Court of Appeals ruled that although Chapter 13 classifies certain data about applicants for licenses as private under section 13.41, subd. 2, the classification of data must change to comply with judicial or administrative rules (see section 13.03, subd. 4). Because the data became part of the hearing record before the ALJ, the decision to seal the record was left to the ALJ's discretion. In general, case records on appeal are presumed public (Minn. R. Pub. Access to Recs. of Jud. Branch 4, subd. 1) and may only be sealed in extraordinary situations and only after the moving party demonstrates the need for doing so and sets forth the efforts made in maintaining confidentiality prior to bringing the action (Minn. R. Civ. App. P. 112.01, subd. 2). Thus, there was no abuse of discretion in the ALJ's declining to seal the entire record in the administrative proceedings.

In ***O'Keefe v. Carter*, A12-0811 (Minn. Ct. App. December 31, 2012, unpublished)**, the Court of Appeals determined the claims for violations of the Open Meeting Law (Minnesota Statutes, chapter 13D) are subject to a two-year limitations period under section 541.07(2), as supported by the plain language of Chapter 13D that provides for remedies of penalty and forfeiture under section 13D.06, subds. 1 and 3(a).

The Court also found that an exchange of email messages was not a "meeting" as contemplated by Chapter 13D, based on reasoning that a "meeting" only occurs when officeholders assemble in person and written communications are not a "meeting" under the law. The Court noted that even if the exchange of email messages could be established as a "meeting," the messages did not have the content required for a "meeting" because the subject of the messages was not both "important" and "controversial."

Advisory opinion highlights, cont.

RFP process and re-solicitation, cont.

Opinion 13-005 Note: this opinion relates to 13-001. A member of the public sought access to data related to a request for proposal (RFP) under section 13.591, subd. 3(b) and 4(a). The entity cancelled procurement for the original contract prior to completion of the evaluation process, and three weeks later, re-solicited two new RFPs for the project. Although the entity plans to issue more RFPs in connection with the project, the evaluation process for the two re-solicited RFPs is complete, and all data submitted in response to the original RFP are now public (except trade secret) under section 13.591, subd. 3(b). For the same reasons, "evaluative data," are also public, pursuant to section 13.591, subd. 4(a), except trade secret data.

Classification of grades and GPA

Opinion 13-006 An entity asked about the classification of grades and GPAs on undergraduate and graduate transcripts provided to the entity. Section 13.43, classifies "education and training background" data as public, but does not define "education and training background." Previous opinions have addressed the scope of those terms only as it relates to dates, specific institutions of learning, and places of employment. Using common dictionary definitions, grades and GPAs are not "education and training background." A specific grade or GPA is not part of the general education and training background of an employee or applicant and does not describe the knowledge, development, or experience that an applicant or employee has achieved. Accordingly, those data are private.