FYi

From the Information Policy Analysis Division

Volume 12 Issue 2
Spring 2013

Legislative Update: 2013 Session

This summary highlights changes to the Government Data Practices Act (Minnesota Statutes, Chapter 13) and other data practices related laws. This year's data practices omnibus bill changed provisions in Chapter 13 and in other data practices related laws (see 2013 Session Laws, chapter 82). *All chapter references are to the 2013 Session Laws and the effective date for provisions is August 1, 2013, unless otherwise noted*.

Changes to Chapter 13

Safe At Home Data – 13.045 (new); 13.82, subd. 24: Allows individuals to notify a responsible authority of their participation in the Secretary of State's Safe At Home address confidentiality program; governs the exchange of information among law enforcement. *Effective July 1, 2013.* (Ch. 76)

Personal Contact Information – 13.356 (new): Classifies as private data, personal contact information (phone number, email address, username/password) collected by government entities for notification (i.e. snow emergency alerts) or for an entity's electronic periodic publication (i.e. newsletter); Tennessen warnings are not required; specifies that data may only be used for purposes provided by the individual. *Effective the day following final enactment and applies to data collected, maintained, or received before, on, or after that date*. (Ch. 82, sec. 1)

Security Information – 13.37, subd. 1: Adds electronic addresses and GPS locations of volunteers in crime prevention programs as private or nonpublic security information. (Ch. 82, sec. 2)

Biological Specimens and Health Data – 13.386: Clarifies newborn screening and other activities under chapter 144 are not subject to the informed consent requirements in section 13.386, subd. 3(a). *Effective July 1, 2013.* (Ch. 82, sec. 3)

Personnel Data and Public Officials – 13.43, subd. 2: Clarifies "public official" positions in local government under section 13.43. *Effective the day following enactment*. (Ch. 82, sec. 4)

Personnel Data and Child Maltreatment Data – 13.43, subd. 14: Allows release of private personnel data to a parent/guardian upon report of alleged maltreatment of a student. (Ch. 82, sec. 5, 38)

Continued on page 2

Inside this issue:

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Legislative Update, cont.

Office of Higher Education; Employment and Training Data – 13.47, subd. 3: Allows the Commissioner of Employment and Economic Development to disseminate employment and training data to the Office of Higher Education for certain purposes. (Ch. 99, art. 2, sec. 1)

Business Data – 13.591: Updates language relating to requests for bids and proposals to allow for electronic submissions. (Ch. 142, art. 3, sec. 14)

Assistive Technology Devices – 13.64, subd. 2: Classifies as private the data that identify individuals with disabilities (or family members) who are accessing certain services from the System of Technology to Achieve Results (STAR) program within the Dept of Administration. (Ch. 82, sec. 7)

Transportation Service Data – 13.72, subd. 10: Classifies as private the name of the applicant or user of transportation services for the disabled or elderly. *Effective the day following enactment*. (Ch. 82, sec. 8)

Construction Manager/General Contractor Data – 13.72, subd. 19: Details data classifications related to the construction manager/general contractor contract process at the Dept. of Transportation. (Ch. 82, sec. 9)

Transit Customer Data – 13.72, subd. 20: Classifies as private, data on applicants/users/customers of the Metropolitan Council's web services or regional collection systems. *Effective the day following enactment*. (Ch. 82, sec. 10)

Private Donor Gift Data – 13.792: Classifies as private or nonpublic, certain Destination Medical Center Corporation (established pursuant to section 469.41) donor data. Names of donors and gift ranges remain public. (Ch. 143, art. 10, sec. 1)

Release of Confined Person; Automated Notification Service – 13.854 (new): Classifies as private, identifying data about an individual requesting notification on change in custody status of a confined person from the Dept of Corrections or other custodial authority made through an automated electronic notification system. (Ch. 34, sec. 1)

Data Practices Changes Outside Chapter 13

Legislative Auditor Data Security Audits and Notification – 3.971: Grants authority for the legislative auditor to audit information and data systems supported with public funds; requires certain entities to notify the legislative auditor when not public data may have been accessed or used unlawfully. *Effective the day following enactment*. (Ch. 142, art. 3, sec. 6-7; art. 5, sec. 14)

Online Government Information Services; E-Government Advisory Council – 16E.07, 16E.071 (new): Allows MN.IT (formerly Office of Enterprise Technology) to contract with a private entity to maintain certain online government information services; allows a convenience fee of $2 provided there is no fee for viewing or inspecting data; provides for an E-Government Advisory Council established to improve online government information services. (Ch. 142, art 3, sec. 24-25)

Electronic Geospatial Data – 16E.30: Requires electronic geospatial data sharing with other government entities at no cost. (Ch. 95, sec. 3, 4)

Minnesota Insurance Marketplace Act – 62V.06 (new): Creates the Minnesota Insurance Marketplace (MNsure); subjects MNsure to all provisions of chapter 13; provides classifications, certain sharings, and other requirements. *Effective day following enactment*. (Ch. 9, sec. 8)

Vital Records – Chapter 144: Governs how the Dept of Health must maintain, use, and secure vital records. (Ch. 108, art. 12, sec. 16-29)

Criminal Justice Data Communications Network – 299C.46, subd. 3: Describes access to the criminal justice data communications network and criminal justice information system; provides for certain criminal history background checks. (Ch. 82, sec. 29, 30)

Advisory Opinion Highlights

Written Data Access Prcoedures Required

Opinion 13-007: A member of the public requested a school district's data practices access policies and procedures required by sections 13.025 and 13.03. The district replied that it did not maintain a single written document that details its public data access procedures, but that it follows the procedures set forth in statute. The district did not fulfill its obligation to produce a "written data access policy" that "is easily available to the public."

"Definition of "Public Official"

Opinion 13-008: Each administrator of a Minnesota Veterans Home is a "public official" for purposes of section 13.43, subd. 2(e)(3), because under section 198.005, each administrator acts as the administrative head for his/her veterans home.

Use of Skype at Open Meeting

Opinion 13-009: A city council held a meeting using Skype to include a council member at a remote location outside of Minnesota, meeting all requirements in section 13D.02. The council complied with section13D.02, because it used Skype as it might have used interactive television to conduct its meeting in a manner that allowed it to meet its obligations. Further, the plain language of the statute does not forbid a member of a public body from "attending" a public meeting at a location "open and accessible to the public" outside of the entity's geographic area, as long as all other conditions of that section are met.

Access to License Plate Data

Opinion 13-010: A member of the public sought access from the Minnesota Department of Public Safety/ Bureau of Criminal Apprehension (DPS/BCA) Archive Service Repository to certain license plate data. BCA and the local law enforcement agency have a joint powers agreement that governs the collection and maintenance of the data; however, neither DPS/BCA nor the agency maintains all of the data that together were responsive to the request. The Commissioner also discussed whether any of the requested data are system log files and/or audit trail data subject to a DPS security information declaration under section 13.37, as well as the applicability of the federal Driver's Privacy Protection Act to the classification of the data.

Adequacy of Tennessen Warning

Opinion 13-011: A school district interviewed a student about his/her alleged involvement in an incident off school property. The district gave the student an oral Tennessen warning, which did not meet the full statutory notice requirements. The oral notice was not adequate because the district did not clearly state the consequences *to the student* of providing or not providing the requested data when it knew of at least one consequence to the student if he/she provided data that confirmed his/her involvement in the incident. Also, the district did not identify those persons outside the district to whom it was authorized to disseminate the data, regardless of its intention to do so.

Caselaw Update

In ***Carlson v. Ritchie*, No. 12-2780 (D.Minn. June 3, 2013)**, a federal district court concluded that email addresses are not part of the public information list and that the plaintiff did not have a protected property interest in obtaining them. Registered voters may provide their email addresses as part of their registrations. The plaintiff purchased the public information list, pursuant to Minnesota Statutes, section 201.091, subd. 4, believing that the email addresses would be included, but they were not. He argued that email addresses should be public as part of the public information list pursuant to language in subdivision 9 and Advisory Opinion 12-016. The district court found that the public list is only required to include the elements listed in subdivision 4 (name, address, year of birth, and voting history, telephone number if provided, and it may include information on voting districts). The court further found that no property interest exists where statutory language is permissive.

In ***State v. M.D.T.*, A11-1285, ___ N.W.2d ___ (Minn., May 22, 2013)**, the Minnesota Supreme Court reversed, in part, a district court's expungement order of M.D.T.'s aggravated forgery and controlled substance crime convictions. The Court recognizes the judiciary's inherent authority to expunge criminal records for the serious infringement of constitutional rights and to perform judicial functions, but the Court has never extended the judiciary's inherent authority to expunge executive branch records. The Court relied on separation of powers doctrine and clear legislative policy in Minnesota Statutes, chapters 609A and 13, that these types of criminal records are public in the executive branch. Here, M.D.T. never argued that expungement was necessary to protect a constitutional right and the Court determined that expungement of the executive branch records is not necessary to perform a unique judicial function.

In its second expungement case, ***In re Welfare of J.J.P.*, A11-1146, ___ N.W.2d ___ (Minn., May 22, 2013)**, the Minnesota Supreme Court held that the judiciary has statutory authority under Minnesota Statutes, section 260B.198, to expunge "adjudication of delinquency" records held by the executive branch, but only the order adjudicating the juvenile delinquent and any record referencing the same; nothing preceding that record. Under section 260B.198, courts must weigh the benefit to the petitioner against the determinant to the public and burden on the court. The judiciary's authority to expunge adjudication of delinquency records is based in statute; therefore, this analysis differs from the Court's "inherent authority" analysis in *State v. M.D.T.*, eliminating separation of powers concerns. In addition, the applicable balancing test for expunging adjudication of delinquency records differs because juvenile records are not treated as criminal records.

The Minnesota Court of Appeals held in ***State v. Johnson*, A12-1248, ___ N.W.2d ___ (Minn. Ct. App., June 17, 2013)** that a person does not have a reasonable expectation of privacy in the contents of a computer hard drive and data once seized pursuant to a legal search warrant.

The U.S. Supreme Court issued a decision on June 17, 2013, **Maracich v. Spears, 570 U. S. ____ (2013)**, holding that it is not a permissible use under the federal Driver's Privacy Protection Act, 18 U.S.C. §§2721—2725, for attorneys to use state motor vehicle records to solicit clients.