FYi

From the Information Policy Analysis Division

Volume 12 Issue 4
Fall 2013

When is a data breach notice required?

During the 2013 legislative session, Minnesota Statutes, section 3.971 was amended to require certain notifications to the Office of the Legislative Auditor (OLA) about the improper use of not public data. Specifically, subdivision 9, now requires:

> Subd. 9. **Obligation to notify the legislative auditor.** The chief executive, financial, or information officers of an organization subject to audit under this section ***must promptly notify the legislative auditor*** when the officer obtains information indicating that public money or other public resources may have been used for an unlawful purpose, or when the officer obtains information indicating that ***government data classified by chapter 13 as not public may have been accessed or used unlawfully***. As necessary, the legislative auditor shall coordinate an investigation of the allegation with appropriate law enforcement officials. [Emphasis added.]

In essence, this provision requires notification to the OLA each time a government entity subject to the OLA's audit authority has knowledge of improper access to or use of not public data. This is a very broad reporting obligation for the applicable entities.

In contrast, the data breach notification provision in Minnesota Statutes, section 13.055, subdivision 2, applicable only to state agencies, states:

> Subd. 2. **Notice to individuals.** A state agency that collects, creates, receives, maintains, or disseminates private or confidential data on individuals ***must disclose any breach of the security of the data following discovery or notification of the breach. Notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person.*** The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency as provided in subdivision 3; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data. [Emphasis added.]

This data breach provision requires notification to affected persons only when there is a breach of the security of the data and the data is reasonably believed to have been acquired by an unauthorized person.

Continued on page 2

Inside this issue:

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Data breaches, cont.

An **unauthorized person** is defined as, "…any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data."

Breach of security of the data is the "… *unauthorized acquisition* of data…that compromises the security and classification of the data. Good faith acquisition of government data by an employee, contractor, or agent of a state agency for the purposes of the state agency is not a breach of the security of the data, if the government data is not provided to an unauthorized person."

Unauthorized acquisition "means that a person has obtained government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes."

Reading the defined phrases of unauthorized person, breach of the security of the data, and unauthorized acquisition together, the breach notifications under section 13.055 are only required when there is an element of intent to use data for nongovernmental purposes. Thus, breach notifications are required in situations such as stolen government issued laptops and the knowledge of hacking into government databases.

Examples of when the OLA notification is required, but the section 13.055 data breach provision may not generally apply, include:

- Accidental access of a not public database by a government employee
- Incorrectly typing an email address and sending not public data to the wrong government employee
- Inadvertently reading a report with not public data without an appropriate work assignment

Each of the above situations requires corrective action at the government entity, and notification to the OLA, but not a data breach notification as required by section 13.055, because of the lack of wrongful intent.

The Legislature considered changes to the data breach provisions in section 13.055 (HF 183/SF 211) last session and likely will take the issue up again when it convenes for the 2014 session on February 24, 2014.

Advisory Opinion Highlights

Summary Data

Opinion 13-014: A government entity asked whether its method of creating summary data complied with Chapter 13. The data requester argued that the entity's method did not create a risk of uniquely identifying an individual. In concluding that the entity is in the best position to make these types of determinations, the Commissioner noted that entities must balance their duty to provide access to public data with their responsibility to protect private data.

Open Meeting Law

Opinion 13-015: A member of the public asked various questions about whether a township's park commission was subject to Chapter 13D, the Open Meeting Law (OML) and whether the township complied with various other provisions of the OML. The Commissioner concluded that the Park Commission was subject to the OML based on the ordinance creating the commission. The OML is silent with respect to whether public bodies should create agendas, but if an agenda was provided to commission members, a copy must be made available at the meeting pursuant to section 13D.01, subd. 6. To the extent that an email from the chairman was a one way communication, it did not violate the OML. Finally, because the Board changed the time and place of a regular meeting and the place of a previously-noticed special meeting, it was required to provide notice of a special meeting – three days notice, listing date, time, place, and purpose.

Caselaw Update

In ***Helmberger v. Johnson Controls, Inc.***, ___N.W.2d___ (Minn. 2013), [No. A12-0327 (Minn. Nov. 20, 2013)], Helmberger was denied a copy of a subcontract from Johnson Controls, Inc. (JCI), a government contractor, based on JCI's conclusion that its subcontractor was not subject to the Minnesota Government Data Practices Act (Minnesota Statutes, chapter 13), specifically the requirement in section 13.05, subd. 11.

The Minnesota Supreme Court held that private businesses under contract with the government are not required to comply with chapter 13 unless otherwise agreed to in contract. The Court found no language in chapter 13 that makes a contract between private entities public unless the parties otherwise contractually agree. Even if the private parties contract to perform a government function, they must agree to be bound by chapter 13 before they can be compelled by it.

The Court interpreted section 13.05 subd. 11, as "a notice provision that addresses the contractual terms that a government entity must include when contracting with a private business to perform a government function." This provision does not generally obligate any private party unless specifically agreed to in contract. Here, the subcontract Helmberger requested was an agreement between two private parties and neither party had contractually agreed to be bound by chapter 13.

Continued on page 4

Case update, cont.

The following federal district court summaries relate to data breaches of private data in the state Driver and Vehicle Services (DVS) database under the federal Driver's Privacy Protection Act (DPPA).

In ***Kiminski v. Hunt*, 13-185 (D. Minn. Sept. 20, 2013),** Kiminski received a notice from the Department of Natural Resources (DNR) that an employee (Hunt) had accessed her private DVS information without a legitimate reason to do so. Kiminski brought suit under the DPPA against Hunt and several DNR officials for violating her privacy. The state defendants (other than Hunt) filed a motion to dismiss for failure to state a claim against them under the DPPA. The DPPA allows for an individual to bring a suit against *the person who accessed the information*. The district court held that the state did not know the employee was accessing the database for an improper purpose, and that the DPPA only permits liability against the individuals who accessed the data. Therefore, the motion to dismiss the state employees was granted. The court also found that the DPPA does not create a private right of action under 42 U.S.C. § 1983 (in contrast to holdings in other circuits). The DPPA provides for its own restrictive private right of action, and thus precludes a right of action under § 1983.

In ***Kost, et al., v. Hunt,* A13-583, (D. Minn. Oct. 8, 2013),** plaintiffs received the same DNR letter as *Kiminski* and subsequently requested an audit to see how many times Hunt accessed their DVS information. Plaintiffs discovered that other employees had accessed their private data in what they believed was an unauthorized manner. They filed suit against Hunt, various DNR and Department of Public Safety (DPS) supervisory officials, and DNR/DPS "Does" in their individual capacity for the personal viewing of their DVS information. The Court dismissed the actions against the state supervisory defendants for the same reason as *Kiminski*—that the DPPA did not provide a cause of action against those who had not personally accessed the private data. The Court, however, refused to dismiss the "Doe defendants" because the plaintiffs properly alleged that each Doe defendant had accessed the information personally, which creates a right of action under the DPPA.

In ***Kost, et al., v. Hunt,* A13-583, (D. Minn. Nov. 15, 2013),** multiple county and city governments filed a motion to dismiss. Plaintiffs filed their complaint in March of 2013, and were seeking damages for violations going back to 2003. The Court dismissed all allegations prior to 2007 as time-barred, holding that while the DPPA did not have a specific statute of limitations, the default time limitation for all civil actions is 4 years, and this default applied to the DPPA. The Court also dismissed all the moving defendants from the suit, saying that the plaintiffs failed to allege facts in their complaint that showed impropriety on the part of the defendants. (Same case as above; different motion to dismiss.)

In ***Nelson v. Jesson et. al.,* A13-340 (D. Minn. Nov. 1, 2013),** a Department of Human Services (DHS) employee accessed plaintiff's DVS information without authorization to do so. After receiving a breach notification, the plaintiff filed suit against the employee, the employee's supervisors, and DHS. DHS and the supervisors filed a motion to dismiss. The Court granted the defendants' motion on the basis that the plaintiff failed to sufficiently allege an impermissible purpose under the DPPA. The plaintiff did not allege that DHS or the supervisors personally obtained his DVS information, nor did he allege that they gave database access to DHS employees for an impermissible purpose. The Court also dismissed plaintiff's § 1983 claim because the DPPA violation did not cause a "shocking degradation or an egregious humiliation" to plaintiff under the 14th Amendment to the U.S. Constitution, and furthermore, a DPPA claim precludes a claim under § 1983.