SENATE
STATE OF MINNESOTA
EIGHTY-EIGHTH LEGISLATURE

S.F. No. 211

(SENATE AUTHORS: DIBBLE, Hoffman, Jensen, Limmer and Osmek)

DATE	D-PG	OFFICIAL STATUS
01/31/2013	132	Introduction and first reading Referred to Judiciary
02/04/2013	147	Author added Osmek
03/05/2013		Comm report: To pass as amended Second reading

A bill for an act

relating to data practices; enhancing certain penalties and procedures related to unauthorized access to data by a public employee; amending Minnesota Statutes 2012, sections 13.05, subdivision 5; 13.055; 13.08, subdivision 1; 13.09.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2012, section 13.05, subdivision 5, is amended to read:

Subd. 5. **Data protection.** (a) The responsible authority shall (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; and (2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that is not public is only accessible to persons explicitly authorized by law, and is only being accessed by those persons for reasons explicitly authorized by law.

(b) When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.

Sec. 2. Minnesota Statutes 2012, section 13.055, is amended to read:

13.055 ~~STATE AGENCIES;~~ DISCLOSURE OF BREACH IN SECURITY; NOTIFICATION AND INVESTIGATION REPORT REQUIRED.

Subdivision 1. **Definitions.** For purposes of this section, the following terms have the meanings given to them.

(a) "Breach of the security of the data" means unauthorized acquisition of or access to data maintained by a ~~state agency~~ government entity that compromises the security and classification of the data. Good faith acquisition of or access to government data by an employee, contractor, or agent of a ~~state agency~~ government entity for the purposes of

the ~~state agency~~ entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a reason not explicitly authorized by law.

(b) "Contact information" means either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by the ~~state agency~~ government entity.

(c) "Unauthorized acquisition" means that a person has obtained or viewed 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. Intent to cause harm to a data subject is not a factor in determining whether an acquisition of data is unauthorized.

(d) "Unauthorized person" means any person who accesses government data ~~without permission or~~ without a work assignment that reasonably requires ~~the person to have~~ access ~~to the data~~, or regardless of the person's work assignment, for a reason not explicitly permitted by law.

Subd. 2. **Notice to individuals; investigation report.** (a) A ~~state agency~~ government entity 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.

(b) Upon completion of an investigation into any breach in the security of data, the responsible authority shall prepare a report on the facts and results of the investigation. If the breach involved unauthorized acquisition to data by a public employee, the report must at a minimum include:

(1) a description of the data that were accessed or acquired;

(2) the number of individuals whose data was improperly accessed or acquired;

(3) the name of each employee determined responsible for the unauthorized access or acquisition; and

(4) the final disposition of any disciplinary action taken against each employee in response, or if disciplinary action was determined to be unnecessary, the specific findings and reasons for that determination.

Notwithstanding any other provision of law, the full contents of this report shall be public at all times, provided to any individual required to receive a notice under paragraph (a), and posted on the affected government entity's Web site.

Subd. 3. **Delayed notice.** The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede an active criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 4. **Method of notice.** Notice under this section may be provided by one of the following methods:

(a) written notice by first class mail to each affected individual;

(b) electronic notice to each affected individual, if the notice provided is consistent with the provisions regarding electronic records and signatures as set forth in United States Code, title 15, section 7001; or

(c) substitute notice, if the ~~state agency~~ government entity demonstrates that the cost of providing the written notice required by paragraph (a) would exceed $250,000, or that the affected class of individuals to be notified exceeds 500,000, or the ~~state agency~~ government entity does not have sufficient contact information. Substitute notice consists of all of the following:

(i) e-mail notice if the ~~state agency~~ government entity has an e-mail address for the affected individuals;

(ii) conspicuous posting of the notice on the Web site page of the ~~state agency~~ government entity, if the ~~state agency~~ government entity maintains a Web site; and

(iii) notification to major media outlets that reach the general public within the government entity's jurisdiction.

Subd. 5. **Coordination with consumer reporting agencies.** If the ~~state agency~~ government entity discovers circumstances requiring notification under this section of more than 1,000 individuals at one time, the ~~state agency~~ government entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 6. **Security assessments.** At least annually, each government entity shall conduct a comprehensive security assessment of any personal information maintained by the government entity. For the purposes of this subdivision, personal information is defined under section 325E.61, subdivision 1, paragraphs (e) and (f).

EFFECTIVE DATE. This section is effective the day following final enactment and applies to security breaches occurring on or after that date.

Sec. 3. Minnesota Statutes 2012, section 13.08, subdivision 1, is amended to read:

Subdivision 1. **Action for damages.** Notwithstanding section 466.03, a responsible authority or government entity which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, or in the case of any violation resulting from a public employee's unauthorized access to not public data, the government entity shall, in addition, be liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under this chapter.

EFFECTIVE DATE. This section is effective the day following final enactment and applies to violations occurring on or after that date.

Sec. 4. Minnesota Statutes 2012, section 13.09, is amended to read:

13.09 PENALTIES.

(a)(1) Any person who willfully violates the provisions of this chapter or any rules adopted under this chapter is guilty of a misdemeanor.

(2) A public employee who acquires or accesses not public data in a manner not explicitly authorized by law is guilty of a gross misdemeanor if the employee:

(i) acquired or accessed data on a single data subject on more than one occasion; or

(ii) acquired or accessed data on multiple data subjects, regardless of the number of occasions on which the acquisition or access occurred.

~~Willful violation of this chapter by~~ (b) Any action subject to a criminal penalty under paragraph (a) by any public employee constitutes just cause for suspension without pay or immediate dismissal of the public employee.

EFFECTIVE DATE. This section is effective the day following final enactment and applies to violations occurring on or after that date.