House Research
Act Summary

CHAPTER: 163 **SESSION:** 2005 Regular Session

TOPIC: Omnibus Data Practices Bill

Date: June 17, 2005

Analyst: Deborah K. McKnight

Overview

This is the annual act that makes government data public or not public. It also restricts (1) inclusion of individuals in wireless phone directories and (2) certain entities' use of social security numbers.

Section

1 **Inquiry and inspection power.** Amends the statute on the legislative auditor's access to data for purposes of audits. Clarifies the auditor must be given "data of any classification."

2 **Investment data.** Designates as "nonpublic" financial, business, or proprietary data retained by the State Board of Investment (SBI) in connection with its venture capital, real estate, and resource investments.

Defines "financial, business, or proprietary data" to mean information the SBI executive director determines (i) is of a financial, business, or proprietary nature; and (ii) if released, would cause competitive harm to the SBI or the entity the SBI is investing in or has considered investing in.

Specifies SBI data in connection with these investments that is public, even if considered financial, business, or proprietary: the name and industry group classification of the investment entity; the SBI commitment amount and the funded amount of that commitment; the market value of the investment; the boards' internal rate of return; and the age of the investment in years.

3–7 Terminology change from state agencies, statewide systems, and political subdivisions to "government entities."

8 **Request for access.** Specifies that if 100 or fewer letter or legal size, black and white copies are requested, the fee is not more than 25 cents per page, rather than actual cost.

9–20 "Government entity" term change.

21 **State agencies; disclosure of security breach.** Requires a state agency to notify individuals if private or confidential data on them may have been acquired by an unauthorized person. Specifies how to provide notice. Allows delaying notice if prompt notice would impede a law enforcement investigation. Requires notice to consumer reporting agencies if over 1,000 individuals are affected by the security breach.

22 –31 "Government entity" term change.

32 **Education records; child with disability.** Relocates language that is in current law.

33 **Definitions.** Stricken language is moved to section 42.

34 **Classification.** Stricken language is moved to section 42.

35 **Data dissemination.** Authorizes a government entity to release security information to the public or any person or entity if the release would aid public health, promote public safety, or assist law enforcement. ("Security information" is defined in current law and can be found in section 33).

36 **Office of health facility complaints.** Adds a new subdivision to the government data practices act. Specifies that investigative data held by the Department of Health's Office of Health Facility Complaints are subject to the Vulnerable Adults Act data classifications, except that the identity of a substantiated perpetrator is public data. The new definition of substantiated perpetrator comes from the current human services licensing data statute.

37 -38 "Government entity" again.

39 **Applicant data.** Stricken language on applicant data moved to section 43.

40 **Licensing data.** Amends the human services licensing data provision of the government data practices act. It adds to the kinds of data that are public: a current or former licensee's record of training in child care and child development, and the number of serious injuries or deaths of persons reported about a licensed program to government agencies. Defines as a serious injury, one that is treated by a physician.

Relocates and expands current language that specifies that if a person (1) is a substantiated perpetrator of child or vulnerable adult maltreatment, (2) is subject to disqualification in connection with a license for family child care, child care center services, home foster care, or home adult foster or day care, and (3) the substantiated maltreatment is a reason for a licensing action, the identity of the perpetrator is public data.

Adds to data that is public in connection with human services licensure disqualification: the nature of a disqualification for which a variance was granted, and the disclosure that a person subject to a background study successfully passed it. (A variance can be granted to an individual who has a disqualifying crime in his or her background but there are conditions under which the individual could provide direct contact services that minimize the risk of harm to persons served.)

41 **Classification of evaluative data; data sharing.** Amends the statute that classifies data submitted to government entities by businesses. Adds a subdivision on data received as part of a selection or evaluation process regarding requests for proposals or bids. Makes data protected nonpublic (not available to the subject or anyone else) until the evaluation process is completed; then makes the data public, except for trade secret data (which is defined in current law and is not public). Allows sharing nonpublic data with employees of other agencies who are helping with the process; prohibits those employees from further disseminating such data.

42 **Internal competitive response.** Relocates current law (see sections 33 and 34). Adds to it:

proposals solicited by a different government entity from the private sector. Makes data in an internal competitive response private or nonpublic until completion of the selection or evaluation process, at which time the data become public, other than trade secret data.

43 **Applicants for election or appointment.** Makes public the following data about applicants for appointment or election to a public body: name, city of residence, employment history, volunteer work, awards, prior government service or experience.

44 Technical; cross-reference.

45 **Animal premise data.** Classifies as private or nonpublic: Board of Animal Health data identifying livestock and the locations where they are kept. Allows the board to disclose the data to aid law enforcement or protect the public or animal safety.

46 **Design-build transportation projects.** Provides that certain information collected by the Department of Transportation for design-build transportation projects is protected nonpublic data with respect to data not on individuals, and is confidential data on individuals:

- statement of qualification evaluation criteria and scoring methodology
- statement of qualification evaluations
- technical proposal evaluation criteria and scoring methodology
- technical proposal evaluations

Provides that the first two items become public when the department announces its short list of qualified contractors, and that the last two items become public when the project is awarded.

Effective immediately.

47 **MnDOT data.** Provides that when the department determines that design-build is appropriate for a transportation project, the following are protected nonpublic data with respect to data not on individuals, and confidential data on individuals until the department publishes the data as part of the RFP process:

- relocation reports
- planimetric files
- digital terrain models
- preliminary design drawings
- commissioner's orders
- requests for proposals
- requests for qualifications

Allows the department to release design-build data to landowners, local governments, and other parties under contract to government entities, as part of the project development.

Specifies that data so released retains its status as protected nonpublic data with respect to data not on individuals and confidential data on individuals until the department publishes the information as part of the request for proposal process.

Effective immediately.

48 **Account information.** Makes the following data protected nonpublic data with respect to data not on individuals, and private data on individuals, when the data pertains to applicants for or users of toll facilities and high-occupancy/toll lanes:

- information contained in applications for purchase, lease, or rental of a transponder or other device for calculating tolls
- personal and vehicle identification data
- financial and credit data
- toll road usage data

Allows publication of summary data.

Effective immediately.

49 **Application.** Corrects a drafting error made in the 2004 session. The law enforcement data section of the Data Practices Act was amended to add a reference to the Department of Commerce's Division of Insurance Fraud Prevention. Inadvertently, this reference had the effect of denying the rest of the Commerce Department access to law enforcement data. This section restores the whole department's access rights so it can resume its various previously existing enforcement duties.

Effective immediately.

50 **Technical.**

Effective immediately.

51 **Technical.** Goes with the sections on requests for proposals and bids.

52 **Board meetings.** Allows the Agricultural and Economic Development Board to hold meetings by telephone or other electronic means if interactive television is impractical and all the following conditions are met:

- board members wherever their physical location can hear each other and hear all discussion and testimony
- members of the public at the regular board meeting can hear all discussion, testimony, and votes
- at least one board member is physically present at the regular meeting location
- all votes are conducted by roll call so each member's vote can be identified

Each member participating electronically is considered present for purposes of a quorum

and participating in proceedings.

To the extent practical, the board must allow a person to monitor an electronic meeting electronically from a remote location. The board may require the person making an electronic connection to pay for documented marginal costs the board incurs for the additional connection.

If a regular, special, or emergency meeting is held electronically, the board must give notice in the same manner required by the Open Meeting Law of: the regular meeting location, the fact that some members may participate electronically, and the fact that remote connection may be available and there may be a cost for it.

53 **Advisory board meetings.** Same as section 52 for the Small Business Development Center Advisory Board.

54 **Board meetings.** Same as section 52 for the Minnesota Job Skills Partnership Board.

55 **Council meetings.** Same as section 52 for the Governor's Workforce Development Council.

56 **Board meeting.** Same as section 52 for the Urban Initiative Board.

57 **Explore Minnesota Tourism Council.** Same as section 52 for the Explore Minnesota Tourism Council.

58 **Personal information on vehicle owners.** Makes changes in the law governing privacy of vehicle registration data.

Subd. 1. Federal compliance. Repeals the law that allows vehicle owners to request that their address be classified as private data on individuals (replaced by new subdivision 3). Requires the Department of Public Safety (DPS) to disclose this data if permitted by 18 U.S. Code, section 2721.

Allows data on the registered owners of a vehicle to be disclosed to someone who makes a written request if the owner consents in writing to the department disclosing personal information that is not protected by federal law.

Deletes requirements that vehicle owners must be informed at time of registration that their personal information may be used, rented, or sold for marketing purposes. Substitutes provisions that allow such use only if authorized by the owner.

Subd. 2. Disclosure. Repeals existing law that makes vehicle registration data on individuals public data to the extent permitted by federal law, and replaces it with new language in the section.

Subd. 3. Privacy classification for personal safety. Allows an owner to request that the residence address or name and residence address be classified as "private data on individuals" (data that identifies an individual and that is available only to the subject of the data). Requires the department to grant the classification if the request is accompanied by a signed statement that the classification is necessary for safety reasons. Allows such data to be disclosed to law enforcement, probation, parole, and child support enforcement authorities.

59 **Alternate mailing address.** Provides that if the post office will not deliver mail to the residence address of a vehicle owner listed on the vehicle title application, the owner must provide post office verification that mail will be delivered to a specified alternate mailing

address. Requires the department to use the alternate mailing address when so provided by the owner.

60 –72 **Accident reporting.** Makes technical changes and corrections in the laws governing accident reporting.

73 **Commissioner as agent.** Recodifies into traffic law the provision repealed under section 89 that makes the commissioner of public safety an agent for service of process.

74 **Information; vehicle owners.** Provides that if persons involved in an accident prepare a report when no law enforcement officer report was prepared, the vehicle owners have the same access as law enforcement officers would have to Department of Public Safety (DPS) information about the vehicles, owners, and drivers.

75 **Continuance of court proceeding.** Allows a court in which an accident is pending to order a continuance to allow the defendant up to 90 days after the date of filing of the action to defend the action. Requires the fee paid by the plaintiff to the commissioner at the time of service of the proceedings to be taxed in the plaintiff's cost if the plaintiff prevails.

76 **Address on driver's license.** Provides that if the post office will not to deliver mail to the residence address of a licensed driver listed on the license, the owner must provide post office verification that mail will be delivered to a specified alternate mailing address. Requires the department to use the alternate mailing address when so provided by the licensee.

77 **Address on ID cards.** Makes a change similar to the prior section for Minnesota ID cards.

78 **Privacy of driver's license data.** Makes changes in the law on privacy of driver's license data comparable to the changes in vehicle owner data under section 58.

79 **Taxpayer identity.** Amends the statute governing Department of Revenue data. Makes public: the state taxpayer identifying number of a business entity.

80 **Who may inspect.** Reorganizes and modifies the list of persons who have access to a tax return filed by a business entity.

81 **CIBRS.**

Subd. 1. Definitions. The Comprehensive Incident-Based Reporting System is located in DPS and managed by the BCA.

Defines the Minnesota law enforcement agencies that can submit data to CIBRS: police, sheriffs, Metropolitan Transit Police, Metropolitan Airports Police, University of Minnesota Police, the BCA, and the state patrol.

Subd. 2. Purpose. CIBRS data must be made available to law enforcement agencies to prepare a case against a person known or unknown for the commission of a crime or other offense or for purposes of law enforcement personnel background checks.

Subd. 3. Data practices act governs CIBRS.

Subd. 4. Data classification; audit trail. Specifies that data in CIBRS keeps the same classification it had in the agency that provided it to CIBRS. If CIBRS is the only source of public data, the data must be public in CIBRS.

Otherwise, makes CIBRS data on individuals confidential; makes data not on individuals protected nonpublic. Changes the classification respectively to private and

protected:

(1) if a law enforcement agency notifies CIBRS that an investigation has become inactive (according to the definition in current law); or

(2) if data has not been updated by the submitting agency for 120 days.

Ten days before changing the classification of data, CIBRS must notify the submitting agency that the change will be made, unless the agency updates the data or notifies CIBRS that the investigation is still active.

Requires a law enforcement agency to notify CIBRS if an investigation becomes inactive within ten days after that happens, so the data can be re-classified.

Requires recording in the CIBRS audit trail: all queries, responses, and actions by which data is submitted to CIBRS, changes classification, or is disseminated to any law enforcement agency.

Subd. 5. Access by law enforcement agency personnel. Requires personnel to have BCA certification to enter, update, or access CIBRS data. Requires using purpose codes to limit particular individuals' ability to enter, update or access CIBRS data.

Subd. 6. Data subject access. Requires the BCA or a participating law enforcement agency, upon request of an individual, to state whether the individual is the subject of private or confidential CIBRS data. Lets the individual request data from the BCA or a participating law enforcement agency. Requires informing the individual which law enforcement agency submitted the data and providing contact information for the responsible authority for the law enforcement agency's data.

Subd. 7. Challenge to completeness and accuracy of data. Requires an individual to notify the responsible authority of the agency that submitted data the individual is challenging. Requires the agency to notify CIBRS if its data is challenged. Requires CIBRS to include this notification whenever it disseminates any data that is under challenge. If data is successfully challenged, requires submitting corrected data to CIBRS and disseminating only the corrected data afterward.

82 **Subscription service.** Defines "subscription service" to mean a process for law enforcement to get ongoing, automatic electronic notice of contacts an individual has with any criminal justice agency. Prohibits DPS from establishing a subscription service without prior legislative authorization.

83 **Definitions.** Terms used in new section of statute governing creation of wireless telephone number directories.

84 **Wireless directories.** Requires a provider of wireless phone service to give subscribers conspicuous notice that they will not be included in a directory assistance database without their prior express authorization. Requires authorization to be (1) affirmatively obtained separate from the service contract and by verifiable means and (2) clear about the fact that the consent allows the customer's number to be included in a publicly available directory assistance database. Lets a consumer who consents to inclusion revoke consent. Prohibits

charging a fee for not being listed.

Lets the attorney general sue to enforce. First violation: warning letter. Subsequent: $500 per violation ($100 of this is paid to each victim) to a maximum of $10,000.

Effective immediately.

85 **Use of Social Security numbers.** Restricts private entities, the University of Minnesota, and MNSCU use of Social Security numbers as follows:

- prohibits posting or publicly displaying them
- prohibits requiring unencrypted Internet transmission of them
- prohibits printing them on any card required to access products or services
- prohibits including them on mailed documents unless required by state or federal law and with other exceptions listed

Lets private entities that used Social Security numbers before July 1, 2007, in a manner prohibited by this section keep doing so on and after July 1, 2007, if (1) use remains continuous, and (2) individuals are told annually they have the right to stop the use in question. Individuals who opt out must not be charged or denied services for doing so.

86 **Reports to legislature.** Requires DPS to report to the legislature by January 15, 2006, on (1) possible use of CIBRS data for background checks required by law, (2) a process for criminal records expungement by the subject of CIBRS data, and (3) retention schedules for CIBRS data.

Requires DPS to report by the same date on the advisability of prohibiting possession or use of devices or chemicals to falsify results of drug and alcohol tests or to place false DNA evidence at a crime scene.

87 **Review of state handling of genetic information.** Requires the commissioner of administration to review laws, rules, and policies on whether state handling of genetic information protects individual privacy. Requires a report to the legislature by July 15, 2006.

88 **Instruction to revisor.** Recodifies some transportation provisions.

89 **Repealers.**