State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-FIFTH
SESSION

HOUSE FILE NO. 3683

March 3, 2008
Authored by Hilstrom and Simon
The bill was read for the first time and referred to the Committee on Public Safety and Civil Justice
March 17, 2008
Committee Recommendation and Adoption of Report:
To Pass
Read Second Time

A bill for an act

relating to public safety; providing for an e-charging service; requiring fingerprinting; amending Minnesota Statutes 2006, sections 13.871, by adding a subdivision; 299C.10, subdivision 1; proposing coding for new law in Minnesota Statutes, chapter 299C.

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

Section 1. Minnesota Statutes 2006, section 13.871, is amended by adding a subdivision to read:

Subd. 11. **E-charging.** Data in e-charging is governed by section 299C.41.

Sec. 2. Minnesota Statutes 2006, section 299C.10, subdivision 1, is amended to read:

Subdivision 1. **Required fingerprinting.** (a) Sheriffs, peace officers, and community corrections agencies operating secure juvenile detention facilities shall take or cause to be taken immediately finger and thumb prints, photographs, distinctive physical mark identification data, information on any known aliases or street names, and other identification data requested or required by the superintendent of the bureau, of the following:

(1) persons arrested for, appearing in court on a charge of, or convicted of a felony, gross misdemeanor, or targeted misdemeanor;

(2) juveniles arrested for, appearing in court on a charge of, adjudicated delinquent for, or alleged to have committed felonies or gross misdemeanors as distinguished from those committed by adult offenders;

(3) adults and juveniles admitted to jails or detention facilities;

~~(3)~~ (4) persons reasonably believed by the arresting officer to be fugitives from justice;

~~(4)~~ (5) persons in whose possession, when arrested, are found concealed firearms or other dangerous weapons, burglar tools or outfits, high-power explosives, or articles, machines, or appliances usable for an unlawful purpose and reasonably believed by the arresting officer to be intended for such purposes;

~~(5)~~ (6) juveniles referred by a law enforcement agency to a diversion program for a felony or gross misdemeanor offense; and

~~(6)~~ (7) persons currently involved in the criminal justice process, on probation, on parole, or in custody for the offenses in suspense whom the superintendent of the bureau identifies as being the subject of a court disposition record which cannot be linked to an arrest record, and whose fingerprints are necessary in order to maintain and ensure the accuracy of the bureau's criminal history files, to reduce the number of suspense files, or to comply with the mandates of section 299C.111, relating to the reduction of the number of suspense files. This duty to obtain fingerprints for the offenses in suspense at the request of the bureau shall include the requirement that fingerprints be taken in post-arrest interviews, while making court appearances, while in custody, or while on any form of probation, diversion, or supervised release.

(b) Unless the superintendent of the bureau requires a shorter period, within 24 hours the fingerprint records and other identification data specified under paragraph (a) must be forwarded to the bureau on such forms and in such manner as may be prescribed by the superintendent.

(c) Prosecutors, courts, and probation officers and their agents, employees, and subordinates shall attempt to ensure that the required identification data is taken on a person described in paragraph (a). Law enforcement may take fingerprints of an individual who is presently on probation.

(d) Finger and thumb prints must be obtained no later than:

(1) release from booking; or

(2) if not booked prior to acceptance of a plea of guilty or not guilty.

Prior to acceptance of a plea of guilty or not guilty, an individual's finger and thumb prints must be submitted to the Bureau of Criminal Apprehension for the offense. If finger and thumb prints have not been successfully received by the bureau, an individual may, upon order of the court, be taken into custody for no more than eight hours so that the taking of prints can be completed. Upon notice and motion of the prosecuting attorney, this time period may be extended upon a showing that additional time in custody is essential for the successful taking of prints.

~~(d)~~ (e) For purposes of this section, a targeted misdemeanor is a misdemeanor violation of section 169A.20 (driving while impaired), 518B.01 (order for protection

violation), 609.224 (fifth degree assault), 609.2242 (domestic assault), 609.746 (interference with privacy), 609.748 (harassment or restraining order violation), or 617.23 (indecent exposure).

Sec. 3. **[299C.41] E-CHARGING.**

Subdivision 1. **Definitions.** (a) The definitions in this subdivision apply to this section.

(b) "Auditing data" means data in e-charging that document:

(1) who took a particular action;

(2) when the action took place;

(3) the Internet Protocol address of the computer used to take the action;

(4) the identification number of the organization employing the individual taking action;

(5) what action was taken;

(6) the unique identification for the document against which the action was taken;

(7) the purpose for taking the action;

(8) the date and time the request was received by the e-charging system; and

(9) the identification number of the system from which the request originated.

(c) "Credentialed individual" means an individual who has provided credentialing data to a government entity or a court and has been authorized to use e-charging.

(d) "Credentialing data" means data in e-charging that document for an individual who is or was authorized to use e-charging:

(1) user identification;

(2) password; and

(3) jurisdiction identification.

For law enforcement officers, credentialing data also includes a biometric identifier. For notaries public, credentialing data also includes an e-notary digital certificate.

(e) "E-charging" means a service operated by the Bureau of Criminal Apprehension to provide communication and workflow tools for law enforcement, prosecutors, and the courts to use during the process of charging a person with a crime.

(f) "Government entity" has the meaning given in section 13.02, subdivision 7a.

(g) "Individual" has the meaning given in section 13.02, subdivision 8.

(h) "Workflow and routing data" means data in e-charging that document:

(1) the assignment or reassignment of a document to a person or place;

(2) any deadline for the action on the assignment; and

(3) validation that the needed action has been completed.

Subd. 2. **Data classification.** (a) Credentialing data held by a government entity are classified as private data on individuals as defined in section 13.02, subdivision 12, or nonpublic data as defined in section 13.02, subdivision 9.

(b) Auditing data and workflow and routing data maintained by the Bureau of Criminal Apprehension are classified as confidential data on individuals as defined in section 13.02, subdivision 3, or protected nonpublic data as defined in section 13.02, subdivision 13. The same data maintained by any other government entity are classified as provided by other law.

Subd. 3. **Data sharing authorized.** (a) Auditing data, workflow and routing data, or credentialing data must be disclosed to a credentialed individual to resolve issues about the integrity of data at issue in a pending criminal matter. No use outside the pending criminal matter is authorized and no recipient can redisclose the data that are received. To the extent that court rules make the data accessible to the public, they are accessible in the court records.

(b) Auditing, workflow and routing data, or credentialing data must be disclosed to a defendant in a pending criminal matter when the data are relevant to the individual's defense as defined in the Rules of Criminal Procedure. Relevance must be determined by the court using the standard set in Rules of Criminal Procedure, rule 9.01, subdivision 2(1). If the data are found to be relevant, the court must issue an order directing disclosure and send it to the Bureau of Criminal Apprehension. Disclosure cannot be made unless the court's order provides the full name and date of birth of the defendant, the law enforcement agency number, the law enforcement case number connected to the charge, and specifies the data to be disclosed. The bureau shall provide the data to the defendant's attorney and the prosecutor. The data may not be used outside the pending criminal matter and a recipient may not redisclose the data that are received. To the extent that court rules make the data accessible to the public, they are accessible in the court records.

(c) Auditing data, workflow and routing data, or credentialing data may be disclosed to an employee of a government entity or court who has been accused of inappropriate access to, or use of data in, e-charging and to the employee's employer. The data may not be used outside the pending employee disciplining case and a recipient may not redisclose the data that are received. To the extent that section 13.43 or court rules require the disclosure of the data as part of the final disposition of discipline against an employee, the data are public.

(d) Auditing data, workflow and routing data, or credentialing data may be disclosed as part of a criminal or civil matter against a person for unauthorized access to, or use of data in, e-charging. The data may not be used outside the civil or criminal case and

a recipient may not redisclose the data that are received. To the extent that the rules of public access to records of the judicial branch make the data accessible to the public, they are accessible in the court records.

Subd. 4. **Responding to data requests.** When the Bureau of Criminal Apprehension receives a request under chapter 13 for access to data in e-charging that are not auditing data, credentialing data, or workflow and routing data held by the Bureau of Criminal Apprehension, the Bureau of Criminal Apprehension shall direct the requester to all government entities that have created the requested data. As part of its response, the Bureau of Criminal Apprehension shall provide the requester with the name, address, and telephone number for the responsible authority for the government entity.