

This Document can be made available in alternative formats upon request

State of Minnesota
HOUSE OF REPRESENTATIVES

EIGHTY-NINTH SESSION

H. F. No. 2323

05/12/2015 Authored by Quam, Lucero, Hertaus, Gruenhagen, Newberger and others
The bill was read for the first time and referred to the Committee on Civil Law and Data Practices

1.1 A bill for an act
1.2 relating to data practices; classifying body camera data; regulating storage and
1.3 access to body camera data; amending Minnesota Statutes 2014, section 13.82,
1.4 by adding a subdivision.

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

1.6 Section 1. Minnesota Statutes 2014, section 13.82, is amended by adding a subdivision
1.7 to read:

1.8 Subd. 31. **Body camera data.** (a) As used in this subdivision, "body camera data"
1.9 means any audio or video data collected by a device, worn by a peace officer and operated
1.10 pursuant to a written department or agency policy, that records the officer's activities and
1.11 interactions with the public or collects digital evidence as part of an investigation.

1.12 (b) Except for data classified as active criminal investigative data pursuant to
1.13 subdivision 7, body camera data, collected in a space or at a location where a data subject
1.14 is presumed to have a reasonable expectation of privacy under the constitution of the
1.15 United States or the state of Minnesota, is private data on individuals or nonpublic data at
1.16 all times and may only be shared or disseminated pursuant to court order. Notwithstanding
1.17 subdivision 7, body camera data that are part of an inactive investigation remain classified
1.18 as provided in this subdivision.

1.19 (c) Nothing in this section shall be construed to limit a court's authority to determine
1.20 the admissibility of evidence in a judicial proceeding.

1.21 (d) Direct access from the Internet to any system component containing body
1.22 camera data is prohibited. Before allowing access to any system component containing
1.23 body camera data, the user must be assigned a unique username and password. The use
1.24 of the same username by more than one person is prohibited. No person, other than the

2.1 individual assigned the username and password, may know the password. Use of a
2.2 username or password by a user who is not assigned that username is prohibited. Use of
2.3 a system account or service account to access any data or system component within the
2.4 body camera data environment is prohibited. All paper and electronic media containing
2.5 body camera data, including paper and electronic backups, must be stored in a physically
2.6 secure location. The use of a third party or hosted network, or system environment
2.7 or equipment, not directly owned by a law enforcement agency to store body camera
2.8 data is prohibited. The body camera data environment must be physically and logically
2.9 isolated on a dedicated network and on dedicated systems that are not shared with a data
2.10 environment that is not related to body camera data. This paragraph applies to purchases
2.11 of body camera data systems on or after January 1, 2016.