MINNESOTA COALITION ON GOVERNMENT INFORMATION
Informational brief on body camera data

Prepared by Matt Ehling,
Chair, MNCOGI Legislative Issues Committee

House Civil Law Committee, February 10, 2015

Executive summary: Under existing law, body camera data are generally presumed to be public, although many specific details contained in body camera data may be withheld as "private" or "nonpublic" data indefinitely. Under certain circumstances, all body camera data regarding a specific event can be temporarily withheld as "confidential" or "protected nonpublic" data.

Analysis of data status

1) All government data are presumed to be public unless otherwise classified. (Minn. Stat. 13.03 Subd. 1).
This public presumption is the baseline for all government data under Minnesota law. Exceptions to the public presumption stem from Minnesota statutes, temporary data classifications, or federal law.

2) Body camera video (in general) has no specific status under Minnesota law, so it is presumed to be public data.
Unless and until the legislature decides otherwise, body camera video (as a broad category) is presumptively public. In this regard, such data is akin to how squad car "dash cam" video is treated under Minnesota law, as well as many other government-created video recordings. For instance, according to IPAD Data Practices Advisory Opinion 01-090, video recordings captured by cameras at the City of Watertown's municipal liquor store are presumptively public data.

3) Under certain circumstances, body camera data can be classified as "confidential" or "protected nonpublic" data.
There are certain circumstances under which presumptively public body camera data could be temporarily changed to a "confidential" or "protected nonpublic" status. "Confidential" is a data status applying to individuals that does not permit the public or the individual data subject to see the data. "Protected nonpublic" data is data "not on individuals" that cannot be accessed by the public or by the data subject.

Circumstances under which this change could occur include the following:

a) The opening of a criminal investigation. Under Minn. Stat. 13.82 Subd. 7, data that are collected or created by a law enforcement agency in order to prepare a case against a person for the commission of a crime are "not public" while the investigation is active. Once the investigation becomes inactive, such data revert to their formerly public status, with some exceptions.

b) The opening of an investigation related to a civil lawsuit. Once the investigation becomes inactive, investigative data revert to their formerly public status, with some exceptions.

4) Certain elements contained within body camera data can always be withheld as "not public" data.

Images of certain persons and items recorded by body cameras can be withheld as "not public" data under any circumstance, including images contained on body camera data that were part of inactive investigative files.

These persons and images include, but are not limited to, the following specifics, which are set out in the "Comprehensive Law Enforcement Data" section of Chapter 13:

a) The identity of child abuse victims - including inactive investigative data - are private. (13.82 Subd. 8)

b) The identity of vulnerable adult victims - including inactive investigative data - are private. (13.82 Subd. 10)

c) Data that would reveal the identity of undercover officers can be withheld as private data - including inactive investigative data. (13.82 Subd. 17(a))

d) Data that would reveal the identity of a victim of criminal sexual conduct can be withheld as private data - including inactive investigative data. (13.82 Subd. 17(b))

e) Data that would reveal an informant's identity can be withheld as private data - including inactive investigative data. (13.82 Subd.17(c))

f) Data that would reveal the identity of a crime victim can be withheld as private data upon the request of the victim - including inactive investigative data. (13.82 Subd. 17(d))

g) Data that would reveal the identity of a deceased person removed from a cemetery can be withheld as private data - including inactive investigative data. (13.82 Subd. 17(e))

h) Data that would reveal the identity of a juvenile witness can be withheld as private data if police believe that release of the data would endanger the witness - including inactive investigative data. (13.82 Subd. 17(g))

i) Data that would reveal the identity of a mandated reporter can be withheld as private data - including inactive investigative data. (13.82 Subd. 17(h))

j) Data that describe stolen property are private or nonpublic data - including inactive investigative data. (13.82 Subd. 20)

k) Data that would reveal the customers of pawnshops, scrap metal dealers, and second hand goods dealers are private data - including inactive investigative data. (13.82 Subd. 27)

On a related note, photographs that are part of inactive investigative files that are "clearly offensive to common sensibilities" can be withheld as private data. (13.82 Subd. 7).

Other issues

Where is body camera data stored?

Storage of body camera data depends on the video system used, and the department utilizing it. In many cases, the vendors that sell body camera devices (such as Taser International) also sell video storage solutions. Such storage solutions can house body camera footage "on site" in servers, or remotely. Vendors that house body camera data "off site" are performing government functions, and are subject to Chapter 13 requirements to the extent of those functions. (See Minn. Stat. 13.05 Subd. 11).

Who can access body camera data?
Access to body camera data depends on the status of the particular data in question. Any person can make a request to inspect and/or copy public data (Minn. Stat. 13.03 Subd. 3). The subject of "private" data can access data that pertains to that individual, even though the public may not have access to it. Neither the public nor the subject of "confidential" data can have access to that data. Law enforcement personnel can access any category of body camera data, although such access must be pursuant to departmental regulations and existing law.

Court proceedings can take "not public" data and eventually present it to the public through its introduction into evidence. Access to such data is not governed by Chapter 13, but by rules adopted by the Minnesota Supreme Court.

How is "public" body camera data separated from "not public" data?
In general, public data is separated from "not public" data by removing (or "redacting") the not public data from the releasable, public data. In text-based data, this is done by "striking out" the not public data with black marks. In video, this could be accomplished in one of two ways:

a) "Cutting out" entire potions of video in which not public data is viewable;

b) "Blurring out" images of not public data, leaving the releasable, public video viewable.

Of the two, option b) ("blurring out") images is the more time consuming and costly of the two, as it generally requires frame-by-frame attention to redact the irregular movements of recorded persons and objects. Some attempts have been made to automate this process, including one made by the Seattle police department. Ultimately, even automated redaction would need to be checked by a person to ensure that the redacted material was, in fact, removed.