Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30</td>
<td>Welcome and Introductions</td>
</tr>
<tr>
<td>8:45</td>
<td>Law Enforcement Data Overview</td>
</tr>
<tr>
<td>10:00</td>
<td>Break</td>
</tr>
<tr>
<td>10:15</td>
<td>Protected Identities &amp; Morning Scenarios</td>
</tr>
<tr>
<td>11:00</td>
<td>Juvenile Justice Data Overview and Scenarios</td>
</tr>
<tr>
<td>12:00</td>
<td>Lunch (on your own)</td>
</tr>
<tr>
<td>1:00</td>
<td>Morning Recap &amp; Law Enforcement Video Discussion</td>
</tr>
<tr>
<td>1:15</td>
<td>Break</td>
</tr>
<tr>
<td>1:30</td>
<td>Additional Law Enforcement Provisions</td>
</tr>
<tr>
<td>2:00</td>
<td>Break</td>
</tr>
<tr>
<td>2:30</td>
<td>Afternoon Law Enforcement Data Scenarios</td>
</tr>
<tr>
<td>3:15</td>
<td>Final Debrief, General Q&amp;A, Evaluations</td>
</tr>
</tbody>
</table>

Law Enforcement Videos and Other Recordings
Police body-worn camera (BWC) video data
Minn. Stat. § 13.825 (A02)

• Most inactive BWC video data = private/nonpublic
• Active investigative data are confidential/protected nonpublic
• BWC data are public if there is:
  • Discharge of firearm in the course of duty
  • Incident results in substantial bodily harm
  • Data subject makes data public, with applicable redactions
  • Public employee disciplinary data

Body cam data requirements

• Data subjects include:
  • Anyone who can be seen or heard
  • Peace officer who collects the data
  • Peace officers who can be seen or heard

• Access by data subjects:
  • Data subject can access (inspect) unredacted video
  • Copies must be redacted, unless consent from other data subjects
  • On duty officers who are not undercover may not be redacted

• Access to data with no identifiable individuals:
  • Nonpublic data – need to determine subject of data, if any

Body cam data requirements, cont.

• Retention
  • Must retain for at least 90 days unless
    • Discharge of a firearm or use of force resulting in substantial bodily harm (must retain for 1 year)
    • Formal complaint against officer (must retain for 1 year)
  • After 90 days, follow retention schedule
  • Must allow for requests for longer retention

• Info page and FAQ:
  https://mn.gov/admin/data-practices/data/types/body-camera/
Body cam data requirements, cont.

• Inventory
• Authorized access
• Data sharing
• Audits – send to designated legislative committees
• Notice to BCA
• Vendor requirements
• Written policies and procedures, including public comment
• Increased penalties

Unmanned Aerial Vehicle (UAV) data (drones)
Minn. Stat. §626.19

• Generally private/nonpublic
• Active criminal investigative UAV data = confidential/protected nonpublic.
• Inactive criminal investigative = public
• Other not public data retain classification
• Can be disclosed as necessary in emergency situations as described in statute
• If no investigation, must be deleted no later than 7 days

Video discussion note

• We will be viewing actual law enforcement videos
• These videos do not contain violence – there is a gun drawn in one video
• Videos include:
  • A person in distress, a juvenile witness, and an arrest
Steps in determining access to videos

• What kind of video is it?
• Is there an active investigation?
• What section classifies the data?
• What is the classification?
• Who can view the unredacted video?
• Who can have a copy?
• Does public benefit data apply?

What type of video is it?

• Body camera video – § 13.825
• Drone data/video – § 626.19
• Other video: Squad video, taser camera, gun camera, cellphone video, etc. – § 13.82 or presumptively public

Public benefit data

§ 13.82, subd. 15

• Public benefit data may be shared to
  • Aid in the law enforcement process,
  • Promote public safety, or
  • Dispel widespread rumor or unrest.
• Applies to all confidential/protected nonpublic active investigative data (not protected IDs) AND any not public body camera or drone video data
Video #1: Emergency/rescue

Video #1: Classification

• What kind of video is it?
• Is there an active investigation?
• What section classifies the data?
• What is the classification?
• Who can view the unredacted video?
• Who can have a copy?
• Is there a public benefit?

Video #1: Classification, cont.

• What section classifies the data?
  • § 13.825
• What is the classification?
  • Private data on the individuals seen or heard
• Who can view the unredacted video?
  • Anyone seen or heard
• Who can have a copy?
  • Anyone seen or heard with redactions. Others must be redacted unless consent obtained, except on-duty peace officers
  • Any subject could ask to make it public. Others must be redacted unless consent obtained, except on-duty peace officers
• Is there a public benefit?
Video #2: Arrest

Video #2: Classification – active investigation

• What kind of video is it?
• Is there an active investigation?
• What section classifies the data?
• What is the classification?
• Who can view the unredacted video?
• Who can have a copy?
• Is there a public benefit?

Video #2: Classification - active investigation

• Dash cam video
  • § 13.82
  • Confidential/protected nonpublic
  • Those within entity and with statutory authority
  • No obligation to provide access to data requesters

• Body camera video
  • §§ 13.825/13.82
  • Confidential/protected nonpublic
  • Those within entity and with statutory authority
  • No obligation to provide access to data requesters
Video #2: Classification – inactive investigation

• What kind of video is it?
• Is there an active investigation?
• What section classifies the data?
• What is the classification?
• Who can view the unredacted video?
• Who can have a copy?
• Is there a public benefit?

Video #2: Inactive investigation dash video

• Classified by § 13.82
• Inactive investigative data = public
  • Probably not offensive to common sensibilities
• Juvenile witness determination
  • If the subject of the investigation warrants protection juvenile’s identity = private
  • Data presented in court as evidence = public

Video #2: Inactive investigation body camera

• Classified by § 13.825
• Private data on individuals in the video
• Passenger and officer can view unredacted
• Passenger can have unredacted copy
  • On duty officers cannot be redacted
• Officer can have redacted copy
  • Unredacted with consent of passenger
• Passenger can ask to make video public
5-minute break

Additional Law Enforcement Data

Automated License Plate Reader Data (ALPR)
Minn. Stat. § 13.824

- ALPR data are private/nonpublic
  - "Non-hit" data cannot be retained more than 60 days
  - Independent, biennial audits required
    - Audit guidance: https://mn.gov/admin/assets/ALPRaudit_tcm36-307907.pdf
  - Must send audit results to Commissioner of Administration and designated legislative committees
  - Limits on ALPR data sharing among LE

- Public data:
  - Public log of ALPR use
  - Whether an ALPR was used in arrest
  - Existence of recording technology is public

- ALPR procedures required
Traffic accidents
State Accident Report, Minn. Stat. § 169.09, subd. 13 (A03)

- Reports are confidential but shall release upon written request to DPS or any LEA:
  - Parties involved
  - Others suffering injury to person or property
  - Representatives of the estate or surviving spouse
  - Legal counsel and insurers for above
- Charging for copies
  - DPS can charge $5
  - LEA can charge per Ch. 13

Traffic accidents
Law enforcement data

- Local law enforcement traffic accident data are classified under section 13.82
- LEA must release data contained on DPS Report if necessary to comply with section 13.82, subd. 3 or 6

Driver’s license data

- Federal law: Driver’s Privacy Protection Act (DPPA), 18 USC 2721-2725
  - State DMV employee or contractor shall not knowingly disclose information in motor vehicle records
  - Certain permissible uses
- State law:
  - Minn. Stat. §171.12, subd. 7
    - Data used to obtain a driver’s license must be treated as provided in the DPPA
  - Minn. Stat. §171.07, subd. 1a (DVS photographs) – private, but do not have to be provided to the subject
Property complaint data
Minn. Stat. §13.44, subd. 1

- Identities of individuals making complaints about the use of real property
  - Violations of state law or local ordinance
  - Confidential
- What constitutes “use of real property”
  - Weeds in a neighbor’s yard?
  - Loud party next door?
  - Barking dog across the street?

Security information
Minn. Stat. §13.37, subd. 1(a)

- Likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury
- Private/nonpublic
  - RA can provide if access will aid public health, promote public safety, or assist law enforcement
- Not a blanket classification – case-by-case determinations
  - RA must explain upon request

Personnel data in law enforcement agencies
Minn. Stat. §§ 13.43, 626.8457

- Arrest, request for service, and response or incident data regarding agency staff are always public
  - No exception even if used in personnel/internal affairs investigation
  - Can never be withheld as private personnel data
- Certain data must be shared with POST Board
  - LEAs must share public and private data on individual officers for peace officer database
  - Reporting obligation is ongoing; must be updated within 30 days of final disposition
## Criminal background checks

- **Examples required by law**
  - Law enforcement officers (Minn. Stat. §626.87)
  - School employees, coaches, volunteers (Minn. Stat. §123B.03)
  - Human services licensees (Minn. Stat. Ch. 245C)
- **Private data (data subject has access)**
- **What should law enforcement provide in response to a request?**
  - Only public data or private with consent
  - No active criminal investigative data
  - Juvenile data issues

## Domestic abuse data

**Minn. Stat. § 13.80**

- Data collected pursuant to the Domestic Abuse Act = confidential
  - Once a temporary court order is executed or served – data classified by section 13.82
  - Must provide public data and certain reports to victim, victim’s attorney, or an organization designated by the OJP for free.
  - Victims can also access active investigative data upon written request to the prosecutor (section 13.82, subd. 13)

## Maltreatment investigations

**Minn. Stat. §§ 260E.20, 260E.35, and 626.557**

- Maltreatment of minors, sections 260E.20 and 260E.35
- Maltreatment of vulnerable adults, section 626.557
- Broad authority to share not public data with other agencies responsible for investigating reports, including active criminal investigative data
  - Local welfare agencies
  - Department of Health
  - Department of Human Services
  - Department of Education
  - Vulnerable adult review panel
Medical information

• **HIPAA:** complete an internal legal analysis to determine if meets the definition of “covered entity”
  - Generally, LEAs are not subject to HIPAA privacy rule
  - Possible covered entities: EMT services, group health plans
  - DPO’s HIPAA guidance for government entities: https://mn.gov/admin/data-practices/data/types/patient/hipaa/

• **Minnesota Health Records Act** (Minn. Stat. §144.293, subd. 2)
  - Health records received directly from a provider may not be disclosed without consent/specific authority
  - Health information recorded or collected by law enforcement is presumptively public

Welfare data and mental health data

• Welfare data, section 13.46, subd. 2(c)
  - Data provided to LEA by welfare system (food assistance, general assistance, MFIP)
  - Confidential active investigative data or private inactive investigative data
  - Except, if inactive because appeals rights exhausted, data are public.

• Mental health data, 13.46, subd. 7(c)
  - Data given to LEA by a community mental health center, county mental health division, or mental health provider
    - Private
    - Must inform subject that mental health data was obtained

Chapter 13 Check!

During an investigation, police officers photograph the contents of an individual’s medicine cabinet. Ultimately, the prosecutor declines to pursue the case and the photographs become inactive criminal investigative data.

How are the photos classified?
### Data on Decedents

Minn. Stat. §13.10

- Minn. Stat., section 13.10 classifies not public data about data subjects who have died
  - Private data become private data on decedents
  - Confidential data become confidential data on decedents
- Data become public when:
  - 10 years have elapsed since death or presumed death; and
  - 30 years have elapsed since creation of data
- Representative of decedent can exercise access rights
  - Personal representative of decedent during administration period
  - If none, then surviving spouse or any child of decedent
  - If no spouse or children, then parents of the decedent