Greetings!

This is a commentary paper in which we as auditors hope to give some insights to the current statute, questions that have arisen and suggestions on possible changes to the existing structure.

BWCs (Body Worn Cameras):

We think the BWC statutes are well-designed, but the public notification and hearing requirements reflected concerns at the time that the public would potentially view BWCs as invasive. A decade later, BWCs have become not only ubiquitous, but an expectation of the public. There are obviously times when privacy concerns do come into play, especially on medical calls or anytime officers are entering someone's home, but many agencies use BWC policies that allow officers discretion in operating their BWC on calls that appear to be non-criminal in nature. The use of redaction technology – which has gotten quite good – also helps to address many privacy concerns. While transparency is always a plus, eliminating the public notification and hearing requirements would assist agencies that may have accidentally overlooked those requirements in years past, or that either missed one of the steps or failed to save documentation showing that all of the steps were followed exactly as required.

So far as the audit portion of the statute goes, in the absence of guidance as to what an audit should cover, we developed a compliance audit model that addresses all of the requirements and prohibitions of Minn. Stat. 626.8473 and 13.825. We identify any areas of non-compliance in our reports, but our emphasis is on helping agencies to bring their policies and procedures into compliance with statutory requirements. To that end, the most common issue we see is agencies not keeping up with statutory updates. In our experience, agencies want to be compliant but sometimes struggle to stay on top of changes as they occur.

One thing we would certainly like changed in statute, or that we would recommend, is clarifying that the ban on altering, data or metadata doesn't apply to correcting labels or classifications, or adjusting retention as needed (e.g., a traffic stop with a verbal warning as the outcome is set for 90-day retention, but then the driver comes in the next day to make a complaint against the officer. A CFS (call for service) turns into an ICR (Incident Case Report), resulting in a new label, the classification changes from Traffic Stop to Public Complaint and the retention is lengthened from 90 days to 1 year).]

We do have questions about how to handle BWC use by task force members. Should a task force be its own entity with its own policy, or should each of the individual members follow

his or her home agency's policy? If a task force is its own agency, does it also need to be audited separately? It is our opinion that it would be cleaner to apply the part of the statute about following your own agency's policy when acting under the command and control of another CLEO (Chief Law Enforcement Officer), even though a task force commander isn't technically a CLEO.

We strive to offer our audit clients guidance in resolving any areas of non-compliance we identify, which I believe helps to drive agency engagement. Most people in general panic when they hear the word "audit," but when agencies understand that the goal is to correct issues rather than punish mistakes, they tend to be very responsive. We do think there would be a lot of value in having a forum for agencies to address concerns to the legislature about certain statutory elements. (e.g., Large agencies sometimes struggle with the volume of redaction required for traffic stops, or small agencies may struggle with the agency device-only requirements when personnel must share BWCs due to budgetary constraints.) We're certainly happy to highlight these concerns within our audit reports, but inviting those agencies that have concerns to address the committee directly would help them to feel heard.

ALPRs (Automated License Plate Readers):

Our assessment of the ALPR statutes is that the legislature views ALPRs as a double-edged sword: Very powerful tools, but also very dangerous to privacy if used inappropriately. It's clear from the data logging and destruction requirements that there are a lot of concerns about the possibility of data being misused to track people without proper legal justification.

We're seeing a lot more uniformity in terms of the ALPR policies that different agencies are using (compared to our experience with BWC policies), which makes the audit process easier, but we're also seeing significant differences in HOW different agencies use ALPR data (traffic enforcement vs. an investigatory tool), which makes the audit process more difficult.

There are a number of points that could benefit from clarification:

1. How often should the public log of use be created? Daily? Weekly? Monthly? Some other interval?
2. Should the public log of use be posted publicly, or does it simply need to be available if requested?

3. Statute identifies the list of required elements for the public log of use, but doesn't provide any guidance as to the layout. Does the legislature have any recommendations?
4. How long should the public log of use be retained? The General Records Retention Schedule for Minnesota Cities recommends two years.
5. In addition to the list of permissible data elements contained in 13.824 Subd. 2, ALPR vendors are utilizing AI to attempt to identify additional vehicle traits, such as make, model, color, the state that issued the license plate, and various identifying marks (e.g., vehicle damage, stickers and accessories such as roof racks). They're "interpreting" these characteristics from the photos rather than actually "collecting" the data (i.e., pulling it from the MN License Plate file), but the license plate number "collected" under 13.824 Subd. 2(a)(1) is also technically an "interpretation" of the characters from the license plate image. Are these additional vehicle traits allowable, or do they exceed what is allowed under 13.824 Subd. 2?
6. Does the legislature have any guidance as to data sharing that occurs when multiple agencies utilize the same ALPR system? For example, if a sheriff's office and one or more police departments in the same county were to acquire the same ALPR system, could they utilize a shared ALPR database, or does each agency's data need to be directly accessible only to members of that agency? What about in a task force environment, where the member agencies could span multiple counties?
7. Related to the above, Minn. Stat. 13.824 Subd. 2 (c) states in part: "A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law." At what point would an ALPR data sharing arrangement constitute a de facto "central state repository"? We're aware, for example, that the Flock Safety ALPR system allows their clients to grant direct access to each other's ALPR data, making it possible to search multiple agencies' ALPR databases with a single query.
8. After a stationary/fixed ALPR is moved or removed, how long is an agency required to retain historical location data? (e.g., XYZ PD moves a camera from 2nd Street to 4th Street. How long after the move to 4th Street does XYZ PD need to retain records showing that the camera was previously located on 2nd Street?)
9. Up for discussion and comment is the question about chiefs or sheriffs verifying that data being held by third parties is being destroyed as required by MN statute, which third parties are being talked about? Other LE agencies? Or the BWC/ALPR vendors themselves? If it's other Law Enforcement agencies…we would NOT expect (or anticipate) that the department providing data would be doing follow-up checks to ensure data is being kept/destroyed, nor would it be practical. Like interagency sharing with, say, Department of Human Services forensic interviews or the courts

for that matter…there are just too many cases and numbers to make that reasonable conclusion. If it is regarding the third party software vendors, it is a similar issue. Statute is clear that it could be a crime to misuse or not comply with the rules when data is shared and would be more an "as needed" type of thing if concerns were raised or a complaint filed. We do conduct certain searches and tests to ensure the local data on an ALPR system is not being retained beyond the statutory maximums, but anything outside of that would be beyond the parameters of a biennial audit.

a. A possible note for consideration with the concerns about possible misuse of data by an ALPR vendor could best be addressed through some form of financial penalty and/or the possibility of being prohibited from conducting business with Minnesota law enforcement agencies.

We'd eventually like to be able to provide a standardized list of reports to be run for an ALPR audit so that the vendors could make sure their systems are able to generate them.

Thank you for your consideration and hearing our written comments.

Sincerely,

Auditors Chet Carlson and Daniel Gazelka

Rampart Audit LLC