Attachment to Application for
Temporary Classification of Government Data

Describe Data to be Classified as Not Public:

Body worn cameras are portable video recording systems typically attached to the front of a law enforcement officer's outer uniform. Officers activate the body cameras during citizen encounters, including crimes in progress, priority responses, arrests, physical or verbal confrontations, rendering aid, providing problem-solving assistance and support, and when interviewing witnesses or victims. The place of encounter between and officer and community member is commonly dictated by a call for service or effecting and enforcement action. These officer citizen contacts can be highly dynamic and emotionally charged encounters occurring in public places, such as a public sidewalk or local retail store. In other instances these encounters occur in private such as caller's home, bedrooms, bathrooms, or in medical or social service facilities.

Based upon the limitations on temporary classifications, this application is narrower than what is needed. The applicants will petition the State Legislature to enact a more thorough law but in the interim this is needed to protect the public.

The applicants are requesting a temporary classification for the following data obtained through the use of body camera recording systems:

Definition

"Body Camera" means audio or video data collected by a device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others.

Temporary Classification Request

Body Camera recording system data which is not active or inactive criminal investigative data is private data on individuals or nonpublic data unless the incident involved the use of a dangerous weapon by a peace officer or use of physical force by a peace officer that causes bodily harm, as those terms are defined in Minnesota Statutes section 609.02.

If a subject of the data requests that the data be accessible to the public, the data is public provided that data on a subject who is not a peace officer and who does not consent to the release must be redacted, if practicable.

A law enforcement agency may withhold access to body camera data that is public to the extent that the data is clearly offensive to common sensibilities, which includes nudity, neighborhood

disputes, dead bodies, welfare checks, domestic disputes, and responses to medical and mental health crises.

Joint Application

The following government entities join in the application of the City of Maplewood for a temporary classification and agree to be bound by the classification:

1. City of Burnsville, City Council resolution attached.
2.
3.
4.

Justification:

There is a compelling need for immediate temporary classification of the data described above as not public, which if not granted, could adversely affect the privacy rights, health, safety, or welfare of the public, or the data subject's well-being or reputation.

The purpose of the Minnesota Government Data Practices Act ("Act") is "to reconcile the rights of data subjects to protect personal information from indiscriminate disclosure with the right of the public to know what the government is doing." *KSTP-TV v. Ramsey County*, 806 N.W.2d 785, 786-7 (Minn. 2011), citing *Montgomery Ward & Co. v. County of Hennepin*, 450 N.W.2d 299, 307 (Minn. 1990). Also, the Act attempts "to balance these competing rights within a context of effective government operation." *Id.* Pursuant to Minnesota Statutes, section 13.03, subdivision 1, all government data are presumed to be public unless otherwise classified by statute, federal law, or temporary classification.

Data that law enforcement agencies collect, create, or maintain are classified under section 13.82. This section provides that certain law enforcement data are always public, certain law enforcement data are never public, and certain law enforcement data may become public depending on the occurrence of certain events.

Those data falling within subdivisions 2, 3, and 6 of section 13.82 are always classified as public. Certain law enforcement data are never public, such as the identities of undercover law enforcement officers. See §13.82, subd. 17. Other law enforcement data, such as active criminal investigative data, are not public while an investigation is active. §13.82, subd. 7. Once the investigation becomes inactive, criminal investigative data, with certain exceptions, are classified as public.

Body cameras are a useful tool for law enforcement. However, the technology and growing calls for its use are advancing faster than the law. As a result, there are compelling concerns regarding citizen privacy.

In the March 2015 Final Report by Presidents Task Force on 21st Century Policing, considerable attention was given to advances in technology and the potential benefits that can be derived from appropriate implementation and use. The task force recognized the competing interests and discussed the need for considering human rights and civil liberties.

Body-worn cameras raise privacy concerns that have not to date been addressed by the legislature. Unlike the data typically generated as result of law enforcement response or action (i.e. narrative police reports), body cameras can simultaneously record both audio and video and capture clear, close-up images.

Body cameras accompany officers, and collect data, inside homes and other private spaces protected by the Fourth Amendment of the United States Constitution, as well as non-private places retaining some level of privacy protection, such as schools, health care facilities and public locker rooms and bathrooms. But the nature of the contact between officer and citizen regularly occurs even in public spaces where the expectation, on the part of the citizen is that the information they discuss or share will be held with some modicum of privacy. For instance, a parent discusses concerns about a child's behavior or expected and wishes to explore options. Or the case of person has safety concerns about a property in their neighborhood. While they are purposeful in their willingness to share that information with an officer, certainly they would not expect that information to be shared publically.

Body worn camera technology presents privacy concerns of a nature not previously anticipated or foreseen. At the same time, calls for increased levels of police accountability and transparency especially around the use of force are being demanded. As such, existing law is inadequate to balance the competing interests or to protect data subjects against unwarranted intrusion into their private lives. The public's right to have access to data about the government needs to be balanced against the individual's constitutionally protected right to privacy. This balancing test begs the question: Is public purpose served by allowing unfettered public access to body worn data showing a victim in distress, a person experiencing traumatic stress, vulnerable or mentally ill person in a comprised state due to their life circumstances or the nature of their victimization? If the answer is "yes", then does a citizen's constitutionally-protected right to privacy outweigh the public's right to access the body camera data? At present, mechanisms to assert privacy rights within Chapter 13 are limited.

For example, victims of domestic abuse, criminal sexual assault and other crimes involving sensitive issues may be reluctant to provide statements on camera for fear of retaliation or some other potential negative consequence. Body-worn cameras capture images in real time and the subjects are often people in the midst of traumatic circumstances. Body camera data may reveal personal, intimate details of victims in a vulnerable state. Emotions may be intense and the experience may be very personal to the individual involved. The possibility that the body camera data may be disclosed to the general public and published over the internet for the entire world to see would negatively impact the welfare of the data subject. We live in a world where video clips can "go viral" in a matter of hours. The rapid and wide-spread dissemination of this data could result in the re-victimization of the victim, and damage the victim's mental and/or physical health. In addition, public disclosure of this data has the potential impact of chilling victim cooperation with law enforcement. It may even discourage the request for law

enforcement assistance from victims of certain types of crime. This would be detrimental to the safety of the individuals involved as well as the general public, as criminal behavior would go unpunished.

If the body camera data are classified as public, the general public would be able to gain "virtual" entry into the homes of victims and witnesses. This could undermine the safety of victims and witnesses. For example, this virtual entry may enable domestic abusers to locate their victims and cause them additional harm. It may also enable suspects to locate and intimidate potential witnesses, thereby discouraging witness cooperation with the criminal prosecution function.

Further, by gaining access to this data, criminals may be able to target homeowners who are elderly or vulnerable. This data may also reveal valuables or firearms located in a home, which may put that home at risk of being burglarized.

The same negative consequences could result where the body camera captures a person involved in a medical or mental health emergency, be it a heart attack, drug overdose, or attempted suicide. The privacy interests under these circumstances should prevail over the public's hunger for sensationalism or gossip. This privacy interest is recognized to a limited degree by section 13.82, subd. 17(f), which classifies as not public the data that would reveal the identity of a person or subscriber who placed a call to a 911 system and the object of the call is to receive help in a mental health emergency. However, this provision protects only the identity of the person placing the call. It does not protect the data revealing the identity or other circumstances of the person needing help in a mental health emergency or other medical emergency.

Balancing individual privacy interests with the presumptively public classification of government data under chapter 13 is proving challenging under the best of circumstances, and may be fertile ground for lawsuits from proponents on both sides of the spectrum. On the one hand, data subjects may bring an action against the government, claiming invasion of privacy. And, on the other hand, members of the public denied access to the data may bring an action against the same government, claiming a violation of chapter 13 amid allegations of police misconduct or cover-up. In addition, chapter 13 sets forth powerful civil remedies for violations, including money damages, injunctive relief, civil penalties and criminal charges. *See* Minn. Stat. §§ 13.08, 13.09.

The recent appearance of body camera use by law enforcement personnel is not unique to Minnesota. Law enforcement agencies in other states are also examining whether to use body-worn cameras. Those that have invested in this new technology are confronted with balancing the benefits of using the technology with the privacy interests at stake. Indeed, the question of whether or not body cameras should be used by law enforcement has generated a national debate. Public opinion appears to be heated and divided on the issue of whether body camera data should be accessible to anyone upon request.

Scott Greenwood, attorney with the American Civil Liberties Union, has expressed concern regarding video recordings taken while officers are inside a person's home:

> An officer might be allowed to go into the residence and record, but that does not mean that everything inside ought to be public record. The warrant is an exception to the Fourth Amendment, not a waiver. We do not want this to show up on YouTube. My next-door neighbor should never be able to view something that happened inside my house without my permission.

Miller, Lindsay, Jessica Toliver, and Police Executive Research Forum 2014, *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*, Washington, D.C., Office of Community Oriented Policing Services, p. 15.

The important and immediate competing interests at stake merit both local and state-wide discussion and resolution. Therefore, it's imperative that the body camera data at issue be protected by a temporary private or non-public classification to provide the legislature, local governments, and law enforcement executives an opportunity to appropriately address the issues within the legislative process.

Establish that data similar to that which the temporary classification is sought are currently classified as not public. Include the Minnesota statute citation to the similar data's current classification. Discuss similarities in the data, in the functions of the entities which maintain similar data, and in the programs/purposes for which the data are collected and used.

A. Under Minnesota Statutes section 13.82, subd. 17(b), the identity of a victim or alleged victim of criminal sexual conduct is protected and law enforcement agencies shall withhold public access to such data. Likewise, body cam data of such a victim being assisted or questioned by law enforcement responding to the scene of the crime should be protected from public access. For instance, even if the victim's face is pixilated on the body camera video and the voice is disguised, the body camera data could contain information from which the victim's identity could be ascertained, whether it be something that identifies where the victim lives or perhaps even the vehicle the victim drives. What particular piece of data included within the body camera video could be a clue to the victim's identity is likely beyond human capability to recognize and redact. Something as inconsequential as a unique piece of furniture or a family photograph inadvertently caught within the frame of the camera lens could be used to identify the victim.

The privacy and safety concerns surrounding body camera data of the victim that don't necessarily disclose the victim's identity, are equally if not more compelling, than the concerns justifying the withholding of the victim's identity. If the video of a victim's narrative regarding the details of the assault were publicly disclosed, each re-play of the video, whether by the media or others, would re-victimize the victim. The victim would be helpless to stop the video from being aired on television, shared on social networking sites, or uploaded onto any number of other public sites on the internet, whether "YouTube" or a similar site. Once data is in cyberspace, it is effectively there forever.

B. Under Minnesota Statutes section 13.822, sexual assault communication data are classified as private data on individuals. This section protects all persons who consult with a sexual assault counselor. Again, the underlying policy is to protect victims of sexual assault. Consistent with this policy is section 13.823, which exempts from the scope of chapter 13 a "program that provides shelter or support services to victims of domestic abuse or a sexual attack". And, personal history information collected, used, or maintained by a designated shelter facility is private data on individuals. *See* Minn. Stat. § 611A.371(3). Finally, personal history information and other information collected, used, and maintained by an Office of Justice Programs in the Department of Public Safety or a grantee thereof, from which the identity and location of any victim may be determined, are private data. *See* Minn. Stat. § 611A.46.

Classifying body camera data as not public is consistent with the public policy supporting these statutes.

C. Under Minnesota Statutes section 13.821, subd. (a), an individual subject of data may not obtain a copy of a videotape in which a child victim or alleged victim is alleging, explaining, denying, or describing an act of physical or sexual abuse without a court order under section 13.03, subdivision 6, or section 611A.90. Section 611A.90 provides that a custodian of a videotape of a child victim or alleged victim alleging, explaining, denying, or describing an act of physical or sexual abuse as part of an investigation or evaluation of the abuse may not release a copy of the videotape without a court order.

Additionally, body camera may capture data falling within the protections of section 13.821, whether or not the officer is aware at the time that the child is likely to describe an event of abuse. A child might blurt out something unexpectantly while the officer is in the home interviewing an adult on an unrelated matter. Or, it could develop through a casual encounter with an officer on a public sidewalk. Regardless, the body camera data involving the child should be afforded the same protection as videotape data specifically collected within the parameters of section 13.821. The fact that the officer did not intend to capture videotape of the child for the purposes contemplated by section 13.821 should not result in the data being unprotected.

It is important to note that section 13.821(a) precludes the ability to "obtain a copy of a videotape". It does not limit "other rights of access to data". *See* Minn. Stat. § 13.821(b).

D. Under Minnesota Statutes, section 13.82, subdivision 8, active or inactive investigative data that **identify a victim** of child abuse or neglect reported under section 626.556 are private data on individuals. Section 626.556 governs the reporting of maltreatment of minors. All records of the local welfare agency responsible for investigating the report of maltreatment are classified as private data. *See* Minn. Stat. § 626.556, subd. 11.

Subdivision 1 of section 626.556 states that, "The legislature hereby declares that the public policy of this state is to protect children whose health or welfare may be jeopardized through physical abuse, neglect, or sexual abuse." Classifying body camera data relating to child abuse or neglect as private or nonpublic is consistent with this public policy.

Further, under section 13.82, subd. 9, investigative child abuse data that become inactive because either the agency or prosecuting authority decide not to pursue the case or the statute of limitations expires, are classified as private data. However, such protection does not appear to apply where criminal charges are brought. In such a case, sensitive body camera data could end up in the public eye with devastating and harmful effects upon the minor child. Again, because video can be shared with the entire world in a matter of seconds, its negative impact upon the victim can be devastating and incapable of retraction. Such video is a favorite of cyberbullies. This is in sharp contrast to live testimony in a courtroom, where the public is invited, but typically does not attend, absent some relationship to the parties or connection with the proceeding. A child's classmates are likely to be unaware of a domestic abuse matter being heard in court. However, sensitive body camera video relating to such domestic abuse can be easily and quickly shared among classmates on any number of electronic devices, whether a high-tech telephone, tablet, or similar gadget. The potential harm that could result from publicizing victim and witness testimony or statements is recognized by the Minnesota court rules, which prohibit the photographic or electronic recording and reproduction of criminal proceedings absent the consent of all parties. *See* Minnesota General Rules of Practice for the District Courts, Rules 4.01-4.04. As a result, camera and microphones are rarely allowed in Minnesota trial courts.

E. Under Minnesota Statutes, section 13.82, subd. 17(b), the identity of a minor who has engaged in a sexual performance or pornographic work is protected from public access. *See, also,* Minn. Stat. § 617.246, subd. 2. For the reasons articulated above, body camera video that reveals either the identity of the minor or other sensitive details regarding the behavior should be classified as not public.

F. Under Minnesota Statutes, section 13.82, subd. 17(f), a limited privacy interest is recognized with regard to data that would reveal the identity of a person or subscriber who places a call to a 911 system and the object of the call is to receive help in a mental health emergency. However, this provision protects only the identity of the person placing the call. It does not protect the data revealing the identity or other circumstances of the person needing help in a mental health emergency or other medical emergency. Additional protection is needed for data subjects where the body camera captures a subject involved in a medical or mental health emergency, be it a heart attack, drug overdose, or attempted suicide. The privacy interests of the subject under these circumstances should prevail over the public's hunger for sensationalism or gossip.

G. Under Minnesota Statutes, section 13.37, data on volunteers who participate in community crime prevention programs, including the lists of volunteers, their home addresses and telephone numbers are protected data. Also, under section 13.82, subd. 17(c), data that reveal the identity of a paid or unpaid informant being used by the agency if the agency reasonably determines that revealing the identity of the informant would threaten the personal safety of the informant. Additionally, under Minnesota Statues, section 13.82, subd. 4, the audio recording of a call placed to a 911 system for the purpose of requesting service from a law enforcement agency is private data on individuals with respect to the individual making the call. Moreover, section 13.82, subds. 8, protects the identity of reporters of child abuse or neglect. Finally, the law protects the identity of reports of maltreatment of vulnerable adults. *See* Minn.

Stat. §§ 13.82, subd. 8, 10; Minn. Stat. § 626.557. Clearly, these statutory provisions are designed to protect the anonymity of interested citizens willing to alert police to potential criminal activity, whether or not criminal charges are forthcoming. They also serve to encourage the reporting of crime, cultivate community participation in the battle against crime, and foster strong community relationships. All of these interests serve public safety. Likewise, similar types of data captured by a body camera should be classified as not public.

Establish that making the data available to the public would render unworkable a program authorized by law. Describe the program and cite the statute or federal law that authorizes it. If relevant, include past instances where release of the data rendered a program unworkable.

Police Departments are using the body-worn cameras as a tool for law enforcement functions. Use of the body camera data can be valuable for investigating and prosecuting criminal behavior. This, in turn, promotes public safety. However, unfettered public access to the body camera data may have detrimental and severe consequences for certain victims and witnesses, which in turn could hamper victim and witness cooperation with law enforcement. Also, access to the data could unintentionally aid future criminal behavior. Finally, public access to the data could result in Fourth Amendment privacy violations, thereby subjecting law enforcement agencies and political bodies to lawsuits.

Body cameras have been receiving a lot of interest and media attention recently. According to Chuck Wexler, executive director of the Police Executive Research Forum, the "recent emergence of body-worn cameras has already had an impact on policing and this impact will only increase as more agencies adopt this technology." Johnson, Kevin. "Police Body Cameras Offer Benefits, Require Training." USA Today, September 12, 2014. In 2014, President Obama announced that he favors more police utilizing body-worn cameras. To help bring this to fruition, he proposed a three-year, $263 million spending package to increase the use of body-worn cameras, among other objectives. Pickler, Nedra. "Obama Wants More Police Wearing Body Cameras". Associated Press, December 1, 2014.

However, some law enforcement agencies already using this new technology have been faced with suspending or eliminating the use of body cameras due to the exorbitant cost involved with responding to requests for the body camera data. Law enforcement agencies using this technology have been confronted with public data requests for the body camera video that police have described as burdensome.

Police Departments generates several thousand body camera videos per month. Some of these data, such as video of law enforcement activities occurring within a public place, would be classified as public data once the criminal investigation becomes inactive. Other data, however, would be a blend of data classified as public, private and/or confidential. Responding to a data request for such data would require a staff person to view the body camera video, determine its classification, and redact any data classified as private, confidential or not public. The redaction process could involve blocking out sound, blocking out faces or things, etc., while preserving for release that data classified as public. It's a layered process requiring time of staff members,

which translates into financial cost for the agency. Further, the agency decision to redact data that the agency classifies as not public is being challenged on an increasing basis, which adds another layer of staff time and expense. As the awareness of body camera video and demand for its release to the public increase, the cost to law enforcement agencies and local government in responding to these requests also increases. For local government has the sustainable resources to respond to broad, bulk or blanket data requests for body camera video. Such requests will effectively shut down the body camera programs, rending this useful and innovative technology unworkable.

III. Data Sharing:

The city of Maplewood will be legally required to share some of the data described in this application with persons outside of the city during the time of the temporary classification. That data which is relevant to criminal charges will be provided to the defendant or defense counsel pursuant to the discovery obligations under the Minnesota Rules of Criminal Procedure.