LEGISLATIVE DEPARTMENT
Offices of City Council & Clerk
City Hall – Suites 304 & 307
350 South Fifth Street
Minneapolis, Minnesota 55415
Phone : 612/673-2216
FAX: 612/673-3812

December 18, 2012

Commissioner Spencer Cronk
Minnesota Department of Administration
c/o Information Policy Analysis Division
201 Administration Building
50 Sherburne Avenue
Saint Paul, Minnesota 55155

Dear Commissioner Cronk:

As directed by formal action of the City Council at its regular meeting on Friday, December 14, 2012, I am submitting on behalf of the City of Minneapolis a request for temporary classification of license plate data captured by the Minneapolis Police Department using Automated License Plate Readers (ALPR). The MPD uses the data captured by the ALPR system for law enforcement functions. The City is requesting a temporary classification of all such data obtained through the use of the ALPR system as not public data which, if not granted, could adversely affect public health, safety, or welfare.

The necessary documentation supporting this request is enclosed for your review. The City appreciates your attention to this important matter.

Regards,

Casey Joe Carl
City Clerk

Application for Temporary Classification of Government Data

The process for temporarily classifying government data was amended in 2010. The new requirements are in Minnesota Statutes, section 13.06.

Submission. Government entities can submit this application by mail or email to:

Commissioner of Administration
c/o Information Policy Analysis Division (IPAD)
201 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155

info.ipad@state.mn.us

Not public data. Once the Commissioner receives your application, the data are no longer public.

Public data. The application itself is public.

Commissioner's decision. The Commissioner has 45 calendar days to decide whether to grant the temporary classification. The Commissioner has 90 calendar days to make a decision if you request that the temporary classification apply to both your government entity and similar government entities, or the Commissioner decides the classification has statewide implications.

Name and Title of Responsible Authority

Casey Carl, City Clerk

Minnesota Statutes, section 13.06, subdivision 1, requires a government entity's responsible authority to authorize submission of the application.

Requesting Government Entity's Name and Address

City of Minneapolis

City Hall, 350 S. 5th Street

Minneapolis, MN 55415

Additional Contact Information

If entity staff or legal counsel helps prepare the application, please include that person's contact information.

Name: Caroline Bachun, Assistant City Attorney

Phone Number: (612) 673-2754

Email Address: caroline.bachun@minneapolismn.gov

Type of Application

☑ New Application

□ Amended Application

Classification Will Apply To (check one)

☑ Only the requesting government entity

□ All similar government entities

If applying on behalf of similar entities, identify all entities. You must provide documentation that the other entities agree to participate in the application and to be bound by the classification.

Describe Data to be Classified as Not Public

Describe the data you would like to be classified as not public. Be as specific as possible. Listing each data element is not necessarily required, but try to avoid general descriptions, such as "all files" or "all records maintained by this entity." It may be helpful to submit data collection forms. You should also identify data elements or types of data that are excluded from the temporary classification. If any of the data will become public at some point, describe the circumstances and/or timing. (*Please attach description.*)

Current Classification

Is there a Minnesota statute or federal law that currently classifies these data as not public?

☑ No

□ Yes *(If you are able to cite a state statute or federal law, there is no need to submit this application.)*

Is there a Minnesota statute or federal law that could be interpreted to forbid classification of these data as not public?

☑ No

□ Yes

If yes, cite the statute or law and discuss your interpretation. *(Please attach interpretation.)*

Data Sharing

Will you be legally required to share the data described in this application with persons outside of your entity during the time of the temporary classification?

☑ No

□ Yes

If yes, describe the required sharing, including statutory authority. *(Please attach description.)*

Justification

You must clearly establish that a compelling need exists for immediate temporary classification of the data as not public, which if not granted could adversely affect the public's health, safety or welfare, or the data subject's well-being or reputation. If relevant, include any past instances where release of the data had an adverse effect on the public or data subject. *(Please attach compelling need justification.)*

In addition to the compelling need justification, you must describe one or more of the following.

1. 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. *(Please attach similar data argument.)*

2. 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. *(Please attach render a program unworkable argument.)*

I affirm that all of the above statements are true to the best of my knowledge.

I am aware that a temporary classification expires August 1st of the year following its submission to the Legislature pursuant to Minnesota Statutes, section 13.06, subdivision 7, unless the Legislature takes action on the classification.

Signature of Responsible Authority

Dec. 17, 2012

Date

City of Minneapolis
Attachment to Application for Temporary Classification of Government Data

December 17, 2012

Describe Data to be Classified as Not Public:

The Minneapolis Police Department (hereinafter, "MPD") uses Automated License Plate Readers (hereinafter, "ALPR"). This is a new technology. These readers capture information on an average of 800,000 license plates per month. ALPRs are mounted on squad cars, traffic enforcement vehicles, or at stationary locations. After the ALPR reads the license plate number of a vehicle, the license plate number is run through various databases to determine whether there is a "hit." A hit could include, for example, that the vehicle or license plate is stolen, there is a warrant for the arrest of the owner of the vehicle, the owner of the vehicle is under a protection order, and the owner of the vehicle has a suspended or revoked driver's license.

The collected ALPR data can be displayed through a printed report. This report will generally show the location (longitude and latitude), date and time that was captured for a vehicle, the license plate number, a picture of the license plate, a picture of the vehicle, and any hits. The name of the owner of the vehicle is not collected through the ALPR system.

The City is requesting a temporary classification for all data obtained through use of the ALPR system, including but not limited to the following:

(1) Date and time of any report run from ALPR data, the name of the person running the report, and the date span of the report.
(2) The locations of any ALPR camera, whether mobile or stationary.
(3) License plate numbers.
(4) The device number for each ALPR camera.
(5) Date, time and location data on vehicles.
(6) Pictures of license plates, vehicles, and areas surrounding the vehicles.
(7) Number of times a vehicle was captured by the ALPR system for a period of time.
(8) Any hit information, including but not limited to, the following categories: stolen vehicle, Stolen license plate, wanted person, Canadian Police Information Center data, protection order, missing person, violent gang and terrorist organization, supervised release, convicted sexual offender registry, immigration violator files, Keep Our Police Safe ("KOPS"), Minnesota warrants, suspended driver's license, revoked driver's license, canceled driver's license, disqualified driver's license, Be On The Lookout (BOLO), Hotsheet (stolen vehicles in Minneapolis), and scofflaw (5 or more outstanding parking tickets).

The MPD uses the ALPR data as a tool for various law enforcement functions. Among other things, the data can be used to find stolen vehicles and track potential suspects in a homicide. The data can also be used to determine whether: (1) the vehicle owner has a warrant for his or her arrest; (2) the owner is driving with a revoked or suspended driver's license; (3) the vehicle is one involved with a missing person; or (4) a person may be subject to a protective order and may be violating that order. When officers are in a squad car on which an ALPR has been mounted, they can get valuable real time information while they are driving the squad car.

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 public's health, safety or welfare, or the data subject's well-being or reputation. The Commissioner of the Minnesota Department of Administration has not specifically issued advisory opinions related to ALPR data.

The MPD uses this new ALPR system technology to combat crime in the City. However, this new innovative tool is being used for data mining through massive data practices act requests. There have already been 14 requests for the entire public contents of the existing information in the ALPR database. One of those requests is a standing request for database data to be provided every 90 days. The MPD is also receiving an increasing number of individual license plate requests from persons other than the subject of the data.

A recently created blog tracks movements of police and law enforcement personnel vehicles: http://trackthepolice.tumblr.com. The owner of that site welcomes submissions of ALPR data from anywhere in the country where ALPR systems are being used and states, "If they want to watch us, we'll watch them back."

If the ALPR data remains public, the public can learn about people's movements in their vehicles. For example, victims of domestic abuse may be placed at risk because the abuser can request ALPR data to try to determine where the victim may be living or working. This undermines standard safety plans for domestic violence victims. This same risk is present for victims of stalkers and other harassment-related crimes. It is expensive, time consuming and unfair to ask crime victims to get a new license plate in order to avoid this risk. Moreover, even a new license plate number can be discovered by knowing the vehicle driven by the victim and seeing the vehicle on the street with the new license plate. Crime victim safety is being placed at risk by the availability of this data.

In illustration, the State has adopted what is called the "Safe at Home" Program. The program is administered by the Office of the Minnesota Secretary of State under Chapter 5B of the Minnesota Statutes. The Safe at Home Program is designed to help survivors of domestic violence, sexual assault, stalking, or others who fear for their safety by providing a mail forwarding system. Program participants use a PO Box address assigned to them. Safe at Home then forwards the participant's mail to their actual physical address. The actual physical address remains under security with the Safe at Home office. In addition to being the participant's agent to receive mail, the Office of the Minnesota Secretary of State is a participant's agent to receive service of process. **Access to the ALPR data can undermine this whole program.**

Concern from members of the public about the risks of allowing this data to remain accessible to anyone requesting the data is already being expressed. See the following site and the attached City Pages article:
http://blogs.citypages.com/blotter/2012/12/mpds_license_plate_data_allows_stalkers_to_track_their_victims_using_public_data.php

Other risks are also presented. By getting date, time and location data on vehicles, criminals might be able to determine the home location of a person driving the vehicle and could determine when a home might be vacant. A picture of a more expensive vehicle could also be an incentive to focus on a certain vehicle. When sufficient pattern information is obtained, criminals could burglarize the home of the vehicle owner. If another person is in the home and not visible from the outside, burglars could find themselves confronted by that individual.

Since license plates of disabled individuals can be distinguished from others, the owners of such vehicles may be placed at risk. Criminals may target the most vulnerable persons learning their patterns of movement and perhaps where they live.

The availability of this data might also impinge on an individual's welfare by inhibiting an individual from going to a local social service agency for financial assistance, a food shelf when low on funds, an HIV clinic or a divorce attorney's office if they believe they might be tracked at these locations.

The state's Criminal and Juvenile Justice Information Task Force has recommended to the Legislature that the data should be classified as private. In an August 10, 2012 Star Tribune article, a member of that task force, Bob Sykora, was quoted as saying, "I really believe there's a potential for somebody getting hurt or killed." The City is recommending at the 2013 legislative session that the ALPR data be protected, as well. Until the legislature has the opportunity to amend the data practices act to protect this type of data, a temporary classification should be adopted.

1. **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.**

Under Minnesota Statutes, Section 13.72, subd. 13, the toll road usage data of individuals who participate in the MnPASS program is protected. ALPR data could potentially include data on individuals on such toll roads if an ALPR camera is in the vicinity of the toll roads. Such ALPR data would be public, even though it would be private for the MnPASS participants under Section 13.72, subd. 13. Even if the ALPR cameras did not capture data from an individual using a toll road, ALPR data is similar to the MnPASS data, in that it tracks the whereabouts of a vehicle.

On December 29, 2010, the Minnesota Department of Transportation ("MN DOT") requested a temporary classification for data in the Mileage Based User Fee ("MBUF") program. The MBUF program was a pilot program to study whether a fuel neutral mileage charge should replace a state gas tax. Transponders and GPS tracking devices would be installed on the vehicles in the pilot program to track all movements of the vehicles. MN DOT argued, in its application, that revealing travel patterns of program participants could represent a significant danger to the safety and security of the participants in the same ways as concerns were expressed about the MnPASS program. MN DOT said those concerns included identifying unoccupied homes, possibly exposing property to criminal activities and possible tracking by those seeking to harm individuals.

On February 1, 2011, the Acting Commissioner of the Department of Administration granted the temporary application for vehicle identifying data and road usage data collected pursuant to the MBUF program, among other things. In granting the temporary application, the Acting Commissioner found as follows in Finding # 6:

> The applicant met the additional criteria in Minnesota Statutes, section 13.06, subdivision 3, by clearly establishing that a compelling needs exists for immediate temporary classification, which if not granted could adversely affect the health, safety, or welfare of the public, or the data subject's well-being or reputation for a portion of the data listed in the application.
>
> The applicant met the criteria indicated above in the following manner:
>
> The applicant met the criteria to establish a compelling need to temporarily classify as not public the vehicle identifying data, financial account data, road usage data, and participant home contact data collected and maintained pursuant to the MBUF program.

> The applicant argued that there is a compelling need to classify the program participants' travel and financial data. Exposure of the travel data (including home contact data) could subject program participants to criminal activities at their unoccupied homes and the tracking of participants by those seeking to harm the individuals. Exposure of the travel data could also alter program participants' ability to travel freely without fear of unwarranted intrusion into their private lives. Exposure of the financial data could increase the program participants' risk of identity theft.
>
> In addition, the applicant acknowledges that the temporary not public classification is being requested until legislation can be proposed during the 2011 Legislative Session to permanently classify the data.

Similar to the MBUF program, ALPR data could subject individuals to criminal activities in their unoccupied homes and could be tracked by those seeking to harm them. Individuals in Minneapolis should be free to travel without fear of unwarranted intrusion into their private lives by the general public. For the same reasons as the MN DOT application for the MBUF program was granted, the City's application for temporary classification of ALPR data should be granted.

There are other instances in which data, which is similar to ALPR data at issue, is deemed not public. Some of those examples are as follows:

- Under Minnesota Statutes, Section 13.37, security information is protected. Participants of the Safe at Home Program take precautions to avoid public disclosure of their home address through use of the state's mail forwarding system. The Safe at Home Program participants can request of a governmental entity that certain public information on them be private under Section 13.37. The ALPR data can track one's whereabouts, showing a pattern of movement. If an ex-abuser requests data on a license plate number of a Safe at Home Program participant, that ex-abuser may be able to track the Safe at Home Program participant to their home, work or other location. Such a release of ALPR data could render the Safe at Home Program unworkable.

- Welfare benefit data is private under Minnesota Statutes, Section 13.46. One could track the movements of an individual to the Department of Human Services or a local services agency, which could indicate that the individual is receiving welfare benefits.

- Under Minnesota Statutes, Section 13.82, subd. 17, the identity of victims or witness can be protected. That protection could be lost if an individual could request data around the time of a crime to see what vehicles were tracked going to a police station near the crime. The movement of the vehicle could indicate that the individual was a potential victim or witness of a crime. Obtaining further ALPR data for selected license plates could indicate where the individual might be living, thereby placing the life of the victim or witness or their families, at risk. Making ALPR data not public could ensure that the protected identity of witnesses or victims would not be made available to the public.

- Section 13.82, subd. 25 provide protection for data that reflect investigative techniques of law enforcement agencies. With a mass mining of ALPR data over time, the investigative techniques of MPD officers could be revealed to criminals and others.

- Data on people who use ride share is private. See Minn. Stat. secs. 13.72, subd. 9 and 13.201. Such private data includes beginning and ending work hours and current mode of commuting to and from work. With ALPR data, one could determine through a pattern of movement whether an individual is driving to work, and the approximate times that an individual begins and ends work, which would be private under Section 13.72, subd. 9.

- Under Minnesota Statutes, Section 13.548, the name and address and other identifying information on persons who enroll in recreational and other social programs is private. With ALPR data, one could determine through a pattern of movement whether an individual is going to a recreational or other social event.

- Under Minnesota Statutes, Section 13.37(a), data on volunteers who participate in community crime prevention programs, such as their home addresses, is protected. With ALPR, an analysis of an individual's movements can give information on where a block club meeting is being held and where the volunteers live. Block club volunteers and their property could be at risk. Making such data public could hamper the MPD's ability to assist block club leaders with recruiting and keeping block club volunteers.

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

The MPD uses the ALPR data as a tool for various law enforcement functions. Internally, use of the data can be valuable in combatting crime. However, external access to the data can be used to commit crimes against a person or property or to intrude on someone's privacy. If the data remains public, the MPD's ability to fight crime could be hampered.

As explained in more detail above, the release of ALPR data could also render the following programs unworkable:

- The Safe at Home Program
- Statutory protections for welfare benefit data recipients
- The criminal prosecution system if witnesses and victims of crimes can be targeted
- The ability of the MPD to combat crime using certain investigative techniques
- Recreational and other social programs offered by a government entity
- Block Clubs

MPD's license plate data allows stalkers to track their victims using public data

By Aaron Rupar
Published Tue., Dec. 11 2012 at 7:03 AM

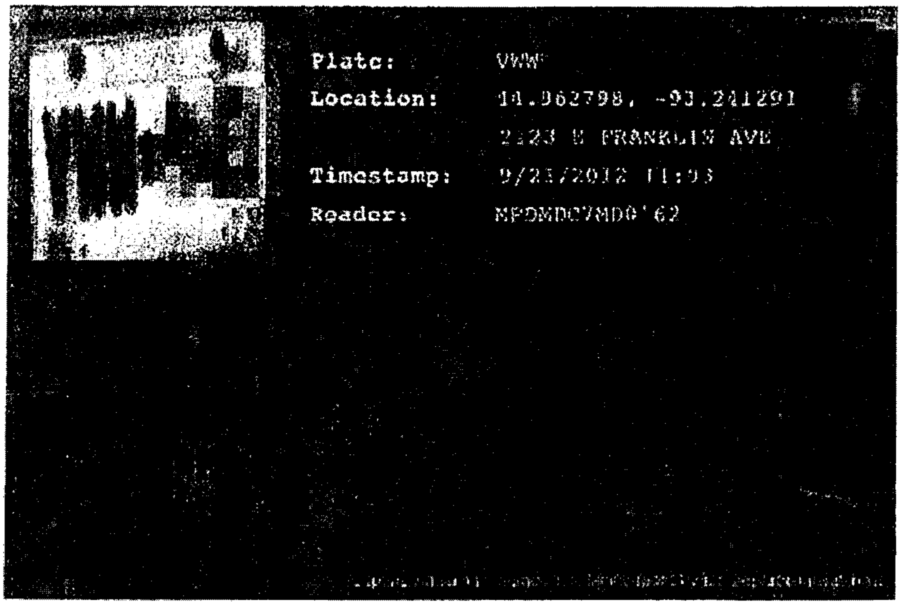


Plate: VWW
Location: 44.962798, -93.241291
2323 E FRANKLIN AVE
Timestamp: 9/23/2012 11:53
Reader: MPDMDC7MD0'62

Tony Webster's blog

The above image and information was captured by an MPD squad car's plate scanner.

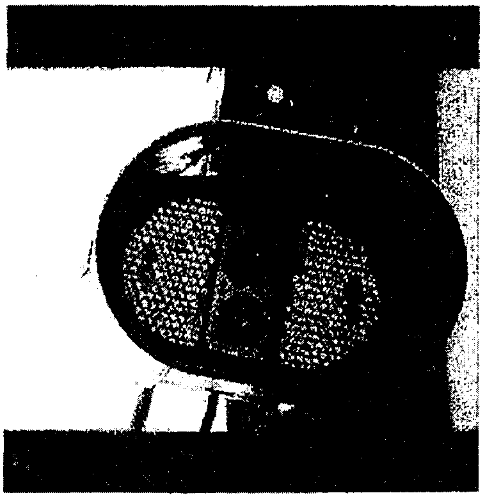
For $5.91, Tony Webster obtained data about the location of 2.1 million Minneapolis-area cars from August 30 to November 29. But for less than that, you can request information about where any particular car has been spotted in the last three months.

SEE ALSO: ***Melissa Hill's new blog allows you to "Track the Police" using public data***

The Automatic License Plate Reader data has uses most probably wouldn't find objectionable -- for instance, finding where a fugitive drove after committing a crime -- but it also has applications many would deem problematic.

Webster lists some of those problematic applications in his "Minneapolis Police release 2.1 million license plate records" report:

> -- A victim of domestic abuse's daily activities could be monitored, and their places of safety could easily be made known to their abuser;
>
> -- Elected officials, diplomatic cars, and government workers could be tracked as they go around the city;



Track the Police

One of Minneapolis' stationary license plate cameras.

-- Disability License Plates follow a special formatting, and an attacker or thief could target disabled persons' homes;

-- ALPR systems are turned on in police station parking lots, capturing police officers' personal vehicle license plates -- those license plates can easily be cross-checked and found outside of the officers' homes or their favorite restaurants;

-- An armored vehicle delivering cash or a hazmat truck's usual route can be tracked;

-- Or... just every-day surveillance of when you leave and come back to your home.

Similar concerns were raised by Minneapolis Police Department Deputy Chief Robert Allen in a recent Star Tribune report.

"If, for example, a stalker wants to see where their prey has been, they can do a public records search and we are required to provide them with information about where that vehicle has been seen by our system," Allen said.

The Strib reports that the MPD used to store license plate data for a year, but now clears the database after three months. St. Paul stores license plate data for two weeks; the State Patrol keeps it for only two days.

More changes to Minneapolis' policy are in the works -- new MPD Chief Janeé Harteau wants the legislature to change statute next session so license plate data is private for everybody other than a particular car's owner.

But that timeframe isn't quick enough for Webster, a self-described designer, hacker, and "data nerd." He calls upon the city to request that the state temporarily reclassify the information as non-public, which would alleviate concerns about plate information being used for nefarious purposes until the legislature gets around to working on a comprehensive solution.

Regarding his USB drive packed with 2.1 million license plate scans, Webster writes: "There's a lot of data here to analyze, but it comes down to this: there is no valid reason for Minneapolis Police to save information on anyone not wanted for a crime."

Name and Title of Responsible Authority

Elizabeth Parker, Chief Counsel/Responsible Authority

Minnesota Statutes, section 13.06, subdivision 1, requires a government entity's responsible authority to authorize submission of the application.

Requesting Government Entity's Name and Address

Minnesota Department of Transportation
395 John Ireland Boulevard MS 140
Saint Paul, MN 55155

Additional Contact Information

If entity staff or legal counsel helps prepare the application, please include that person's contact information.

Name: Barbara Forsland, Data Practices Compliance Officer

Phone Number: 651-366-4822

Email Address: barbara.forsland@state.mn.us

Type of Application

● New Application

○ Amended Application

Classification Will Apply To (check one)

● Only the requesting government entity

○ All similar government entities

If applying on behalf of similar entities, identify all entities. You must provide documentation that the other entities agree to participate in the application and to be bound by the classification.

Describe Data to be Classified as Not Public

Describe the data you would like to be classified as not public. Be as specific as possible. Listing each data element is not necessarily required, but try to avoid general descriptions, such as "all files" or "all records maintained by this entity." It may be helpful to submit data collection forms. You should also identify data elements or types of data that are excluded from the temporary classification. If any of the data will become public at some point, describe the circumstances and/or timing. (*Attach additional pages if necessary.*)

Names of drivers/participants; vehicle identifying data; financial account data; travel routes, dates and times; payment data.

Current Classification

Is there a Minnesota statute or federal law that currently classifies these data as not public?

● No

○ Yes *(If you are able to cite a state statute or federal law, there is no need to submit this application.)*

Is there a Minnesota statute or federal law that could be interpreted to forbid classification of these data as not public?

● No

○ Yes

If yes, cite the statute or law and discuss your interpretation *(attach additional pages if necessary)*:

Data Sharing

Will you be legally required to share the data described in this application with persons outside of your entity during the time of the temporary classification?

● No

○ Yes

If yes, describe the required sharing, including statutory authority *(attach additional pages if necessary)*:

Justification

You must clearly establish that a compelling need exists for immediate temporary classification of the data as not public, which if not granted could adversely affect the public's health, safety or welfare, or the data subject's well-being or reputation. If relevant, include any past instances where release of the data had an adverse effect on the public or data subject. *(Attach additional pages if necessary.)*

See attachment.

In addition to the compelling need justification, you must describe one or more of the following.

1. 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. *(Attach additional pages if necessary.)*

   See attachment.

2. 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. *(Attach additional pages if necessary.)*

   See attachment.

I affirm that all of the above statements are true to the best of my knowledge.

I am aware that a temporary classification expires August 1st of the year following its submission to the Legislature pursuant to Minnesota Statutes, section 13.06, subdivision 7, unless the Legislature takes action on the classification.

Elizabeth M. Parker 12-29-10

Signature of Responsible Authority Date

Justification

There is a compelling need to classify the data described above (generally, personal identification data, vehicle tracking data, and finance/account data) because the Mileage Based User Fee (MBUF) program is scheduled to begin recruitment in January, 2011, and the legislative efforts to legally classify the data as other than public will not mature until later in the legislative session. If the data described above remain public, the risk to data subjects is serious and potentially dangerous. Exposure of travel routes and times could subject persons and property to criminal activities. Exposure of travel data could alter the ability of data subjects to travel freely without fear of unwarranted intrusion into their private lives. Exposure of account data increases risks of identity theft. These negative effects can be fully eliminated by classifying the data as other than public until the legislature has the opportunity to evaluate the matter.

If the risks to participants are not mitigated, it is likely that participation in the program will not achieve the numbers necessary to provide reliable test results, thus defeating the purpose of the pilot program.

Similar data

1. 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. *(Attach additional pages if necessary.)*

Data collection in the MBUF program is most similar to data collection in the MnPASS program. In the MnPASS program, transponders are attached to vehicles that trigger payment processes when vehicles travel in high-occupancy or toll lanes. MnPASS data are protected by Minn. Stat. 13.72 Subd 13, which was passed after legislative discussion about safety concerns and intrusion into the private lives of participants. Safety concerns included identifying unoccupied homes, possibly exposing them to criminal activities; possible tracking of individuals by those seeking to harm them; and identity theft concerns caused by exposing personal and financial data. Intrusion concerns included whether it was appropriate for a government to provide services accompanied by unnecessary exposure of personal life behaviors, such as travel routes, destinations and times. The conclusion was that protection of such data was required, and the following was passed:

> M.S 13.72 Subd. 13, **Account data.**
>
> The following data pertaining to applicants for or users of toll facilities, and high-occupancy vehicle lanes for which a user fee is charged under section 160.93, are classified as nonpublic data with regard to data not on individuals and as private data with regard to data on individuals: data contained in applications for the purchase, lease, or rental of a device such as an electronic vehicle transponder which automatically assesses charges for a vehicle's use of toll roads; personal and vehicle identification data; financial and credit data; and toll road usage data. Nothing in this subdivision prohibits the production of summary data as defined in section 13.02, subdivision 19.

The MBUF program is a pilot program to demonstrate technologies that allow for future replacement of the state gas tax with a fuel neutral mileage charge. It is provided for in Transportations Appropriations Act, ch. 143, art. 1 § 3(a)(1), 2007 Minn. Laws Reg. Sess. 1584, 1587. MBUF program transponders and geographic tracking and recording equipment will be installed in participant cars to track every travel mile and calculate user fees based on the type of road travelled, distance travelled, vehicle characteristics, time of travel, etc. Participants will pay user fees based on periodic reports generated by the MBUF program. (Participants will receive "start-up funds" and incentive payments throughout the project for their participation.) The data will be used to compare actual user fees with the state gas tax generated by the same travel.

In both MnPASS and MBUF programs, data identifying individual participants are collected, including home address, contact information, vehicle type, etc. In addition, in both programs geographic data are collected to identify travel patterns. Mn/PASS is limited to noting travel patterns in high-occupancy vehicle lanes and toll road usage, while the MBUF program is considerably broader since it includes tracking all miles travelled by a particular vehicle. Both programs also collect financial and account data to allow assessment of charges and payments. In each program, we believe that providing protection for the data required to operate the program is necessary to persuade participants to join the programs.

The same concerns addressed by the MnPASS legislation exist for the MBUF program. Revealing contact information, travel patterns or financial account data in the MBUF program could represent a significant danger to the safety and security of participants in the same ways as concerns were expressed about the MnPASS program. Those concerns include identifying unoccupied homes, possibly exposing property to criminal activities; possible tracking by those seeking to harm individuals; and identity theft concerns caused by exposing personal and financial data. Additional concerns involve the appropriateness of providing government services if they are accompanied by unnecessary exposure of personal life behaviors, such as travel routes, destinations and times. Therefore, Mn/DOT is exploring proposing legislation that will provide data classifications for MBUF program data similar to those applied to MnPASS data. Since the MBUF program will begin soliciting participation in January, 2011, we are seeking a temporary classification to protect data until the legislation can be proposed, discussed, and potentially adopted. Legislation, if proposed, will likely be similar to this:

> Minnesota Statutes 2010, section 13.72, is amended by adding a subdivision to read:
>
> Subd. XX. Mileage based user fee data. The following data pertaining to users of navigation software and recording devices used to determine mileage based user fees are classified as nonpublic data with regard to data not on individuals and as private data with regard to data on individuals: data contained in applications for participation in the mileage based user fee program; personal identification data; vehicle identification data; financial and credit data; and field data including road usage data. Nothing in this section prohibits the production of summary data as defined in section 13.02, subdivision 19.

Program Workability

2. 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. *(Attach additional pages if necessary.)*

The MBUF program is authorized by Transportations Appropriations Act, ch. 143, art. 1 § 3(a)(1), 2007 Minn. Laws Reg. Sess. 1584, 1587. It is difficult to demonstrate that program participation will fail unless data protections are in place. What we do know anecdotally is that concerns about data availability were expressed by some potential participants in MnPASS and that the data classifications protecting certain data were sufficient to address their concerns. It is a reasonable assumption that more participation is likely to be achieved by removing possible concerns about data exposure. Mn/DOT notes that professional standards applied outside of the public sector would protect the data from public exposure to remove any barriers to participation. Mn/DOT believes it is appropriate to protect the data from public exposure to remove risks to participants and to ensure adequate participation to produce reliable project results.

STATE OF MINNESOTA
DEPARTMENT OF ADMINISTRATION

FINDINGS OF FACT AND CONCLUSIONS

REGARDING: Application for Temporary Classification of data pursuant to Minnesota Statutes, section 13.06, submitted by:

The Minnesota Department of Transportation

The Commissioner of Administration has examined the above application together with all comments received, and makes the following:

FINDINGS OF FACT

1. The application was filed pursuant to Minnesota Statutes, section 13.06, and was received by the Department of Administration on December 29, 2010.

2. The application was filed on a form provided by the Department of Administration.

3. The application requested the not public classification of the names of participants; vehicle identifying data; financial account data; travel routes, dates, and times; and payment data collected, created, maintained, and disseminated by the Minnesota Department of Transportation (MNDOT) pursuant to the Mileage Based User Fee (MBUF) program established by 2007 Minnesota Laws Regular Session, chapter 143, article 1, section 3(a)(1).

4. The applicant met the criteria in Minnesota Statutes, section 13.06, subdivision 3, by clearly establishing that no statute currently exists which either allows or forbids classification of the data as not public.

5. The applicant met the criteria in Minnesota Statutes, section 13.06, subdivision 3, by clearly establishing that data similar to that for which the temporary classification is sought have been classified as not public by other government entities, or public access to the data would render unworkable a program authorized by law.

   The applicant met the criteria indicated above in the following manner:

   Similar Data
   The applicant argued that the MBUF program data are similar to the MnPASS program data, a program also administered by MNDOT. The MnPASS data were classified as not public by the Legislature in 2005. The classification is codified in Minnesota Statutes, section 13.72, subdivision 13:

   > The following data pertaining to applicants for or users of toll facilities, and high-occupancy vehicle lanes ... are classified as nonpublic ... and as private ... data

> contained in applications for the purchase, lease, or rental of a device such as an electronic vehicle transponder which automatically assesses charges for a vehicle's use of toll roads; personal and vehicle identification data; financial and credit data; and toll road usage data. ....

According to the applicant, the MBUF program is a pilot program to demonstrate technologies that allow for future replacement of the state gas tax with a fuel neutral mileage charge. In both the MnPASS and MBUF programs, individual participant contact information, travel patterns, and financial data are collected. Similar concerns about the safety and security of the potential MBUF participants exist as do with the MnPASS participants.

Program Workability

In addition, the applicant argued that data protection is necessary to address concerns from potential participants about data availability of their personal contact information, vehicle identification information, and financial account information. Data protection would ensure adequate participation in the program to produce reliable results.

6. The applicant met the additional criteria in Minnesota Statutes, section 13.06, subdivision 3, by clearly establishing that a compelling need exists for immediate temporary classification, which if not granted could adversely affect the health, safety, or welfare of the public, or the data subject's well-being or reputation for a portion of the data listed in the application.

   The applicant met the criteria indicated above in the following manner:

   The applicant met the criteria to establish a compelling need to temporarily classify as not public the vehicle identifying data, financial account data, road usage data, and participant home contact data collected and maintained pursuant to the MBUF program.

   The applicant argued that there is a compelling need to classify the program participants' travel and financial data. Exposure of the travel data (including home contact data) could subject program participants to criminal activities at their unoccupied homes and the tracking of participants by those seeking to harm the individuals. Exposure of the travel data could also alter program participants' ability to travel freely without fear of unwarranted intrusion into their private lives. Exposure of the financial data could increase the program participants' risk of identity theft.

   In addition, the applicant acknowledged that the temporary not public classification is being requested until legislation can be proposed during the 2011 Legislative Session to permanently classify the data.

7. The Commissioner did not receive any comments on this application.

Based upon the foregoing findings of fact, the Commissioner makes the following:

CONCLUSIONS

1. Based upon information in the application and the statutory requirements, the Commissioner concludes that the applicant has met the criteria in Minnesota Statutes, section 13.06, to temporarily classify certain data requested in the application.

2. For the reasons set forth above, the following data are approved by the Commissioner as not public data:

   Vehicle identifying data, financial account data, road usage data, and home contact data collected and maintained by the Minnesota Department of Transportation (MNDOT) pursuant to the Mileage Based User Fee (MBUF) program established by 2007 Minnesota Laws Regular Session, chapter 143, article 1, section 3(a)(1).

3. For the reasons set forth below, the following data are disapproved by the Commissioner as not public data:

   Names of participants and payment data collected, created, maintained, or disseminated by MNDOT pursuant to the MBUF program.

   The applicant did not clearly establish the compelling need to classify as not public the names of participants in the MBUF program or the payment amounts provided to program participants as required by Minnesota Statutes, section 13.06, subdivision 3.

   Therefore, these data are public pursuant to Minnesota Statutes, section 13.03, subdivision 1.

By: ______________________ Date: February 1, 2011

Ryan Church
Acting Commissioner