



Advisory Opinion 10-016

This is an opinion of the Commissioner of Administration issued pursuant to Minnesota Statutes, section 13.072 (2009). It is based on the facts and information available to the Commissioner as described below.

Facts and Procedural History:

On April 13, 2010, the Information Policy Analysis Division (IPAD) received a letter dated March 29, 2010, from Paul Hannah, on behalf of the St. Paul *Pioneer Press*. In his letter, Mr. Hannah asked the Commissioner to issue an advisory opinion regarding the *Pioneer Press*' access to certain data from the City of Saint Paul.

IPAD, on behalf of the Commissioner, wrote to Shari Moore, City Clerk, in response to Mr. Hannah's request. The purpose of this letter, dated April 23, 2010, was to inform her of Mr. Hannah's request and to ask her to provide information or support for the City's position. On May 12, 2010, IPAD received a response, dated same, from Reyne Rofuth, Senior Assistant City Attorney.

A summary of the facts as Mr. Hannah provided them is as follows. On July 7, 2006, the *Pioneer Press* requested certain data from the City:

A copy of the computerized incident-level data from your Computer-Aided Dispatch (CAD) system for all incidents from September 1, 2003 through June 30, 2006. We would like it to include all of the fields in the database, including but not limited to:

- CN [call number] number
- Cross reference CN number
- Console Number
- Incident Type
- Priority of Call
- Disposition of call
- Date/time call received
- Date/time call dispatched
- Date/time squad arrived
- Date/time squad cleared
- Occur date from
- Occur date to
- *Complete incident address, including house number, street name, suffix, direction and cross street*
- Sector and grid

[Emphasis added.]

The City responded:

... The St. Paul Police Department generates approximately 60,000 reports per year. The incident data from the CAD involves even more incidents. The data, whether in written report form or CAD system form, contains mixed data (public and not public data). Therefore, the Department would have to review each incident and redact not public data on over 170,000 incidents. It is unknown how long this would take, even given the reasonable time standard of [Minnesota Statutes, Chapter 13]. Therefore, our offer is to provide you with all the field data, except those fields that contain mixed data with the *last two digits of addresses, removed*. Below is a list of the always public data fields and the mixed data fields:

Always public data fields:

- Complaint number,
- Cross reference number,
- Console number,
- Incident type,
- Priority,
- Disposition of call,
- Date and time call received,
- Date and time squad dispatched,
- Date and time squad cleared call,
- Occur date (from), and
- Occur date (to).

Mixed data fields:

- Source of call,
- Site of call,
- Caller name,
- Caller location,
- Caller phone number,
- Call anonymity, and
- *Incident address.*

By removing the last two digits of all addresses, to protect not public data, you will be able to determine the incident location within a one to three block distance on any given street.

....

[Emphasis added.]

Issue:

Based on Mr. Hannah's opinion request, the Commissioner agreed to address the following issue:

Did the City of Saint Paul comply with Minnesota Statutes, Chapter 13, in responding to a request for data from the City's Computer-Aided Dispatch system?

Discussion:

Pursuant to Minnesota Statutes, Chapter 13, government data are public unless otherwise classified. (Minnesota Statutes, section 13.03, subdivision 1.)

Minnesota Statutes, section 13.03, subdivision 3, requires government entities to provide copies of public data upon request. Also, pursuant to section 13.03, subdivision 1, government entities must keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use.

Data that law enforcement agencies collect, create, and maintain are classified pursuant to Minnesota Statutes, section 13.82. Certain law enforcement data always are public, regardless of whether there is an active investigation. Such data are listed in Minnesota Statutes, section 13.82, sections 2 (arrest data), 3 (request for service data), and 6 (response or incident data). Most, if not all, of the time, when there is an incident involving a law enforcement agency, the agency collects and maintains the complete street address connected with the incident.

Although most law enforcement data are public, there are several exceptions. One that is applicable here is section 13.82, subdivision 17, which requires law enforcement agencies to withhold data that would identify certain individuals, including: victims or alleged victims of criminal sexual conduct; victims of or witnesses to a crime if the individual has requested not to be publicly identified, unless the agency determines that the safety or property of the individual would not be threatened by the release of data; paid or unpaid informants in certain situations; undercover law enforcement officers; and juvenile witnesses in certain situations.

In his opinion request, Mr. Hannah wrote:

The Department has refused to provide the last two digits of thousands and thousands of addresses to the *Pioneer Press*, even though complete addresses are public under Section 13.82. Its only argument is that some addresses might be protected from nondisclosure under Section 13.82. According to [the City], “[i]t is unknown which specific subdivision [renders this data as nonpublic], without having to look at each report or incident.”

In her comments to the Commissioner, Ms. Rofuth wrote:

It is true the SPPD [St. Paul Police Department] refused to provide full numerical addresses to the [*Pioneer Press*] in their requests for multiple year data dumps. It is the SPPD position [sic] they have the obligation to make the threat determination and other classification determinations under Minn. Stat. 13.82 at the time of the request because there are numerous situations in which the release of the address data fields would likely identify a protected individual, who’s [sic] identity is private data. ...

... everyone who professionally works with [Chapter 13] ... knows[s] and struggle[s] with the fact [that Chapter 13] is outdated in its application to electronic data. The legislature has failed to address this extremely important issue and correct the problem which leaves government entities to deal with unfair threats of noncompliance on a daily basis or, at the very least, with confusion in its application. The SPPD struggles with this dilemma and always acts in good faith in responding to media request [sic] with all the data it can provide without violating the statutory protections of individuals.

The Commissioner addressed a similar issue in Advisory Opinion 00-011:

In their correspondence with Mr. Anfinson, SLMPSD [South Lake Minnetonka Public Safety Department] representatives told him that it would be very expensive and time-consuming to review and remove the not public data from the thousands of log sheets generated each year ...

... If government entities neglect their obligations to maintain data in easily accessible formats, this is the kind of situation that can arise. SLMPSD might want to consider a redesign of the log sheet in order to "zone" the not public data, so that they are easier to remove for purposes of inspection of the public data.

... SLMPSD is obligated to provide free inspection of the public data in the log sheets, and it must bear the cost of separating the not public from the public data.

Although 00-011 involved data in paper format, the analysis in that opinion applies to the matter Mr. Hannah raised. The City argued it would have to review each of the 170,000 incidents in the database prior to making a determination about how the data are classified. This response illustrates the very reason that when a government entity creates and develops an electronic database, staff must consider how the entity will respond to data requests involving data in the database. Perhaps if the City's database had been developed differently, staff could include certain public/not public classifications at the time of initial data entry and flag certain fields for classification at a later point in time.

There is no dispute that some of the incident-related data the *Pioneer Press* requested are public and some are not public. Regarding address data, the Commissioner points out it is not necessarily the case that providing a complete street address connected to an incident identifies an individual whose identity requires protection under section 13.82. For example, if there is a shooting at a particular address and the witnesses to the incident (who requested that their identities be protected and the agency has followed the process outlined in section 13.82, subdivision 17) do not live at that address, the address is public. Or, for example, releasing the complete street address of an apartment building does not necessarily identify a witness (who has requested protection per section 13.82, subdivision 17) who lives in one of the units of the building.

Ms. Rofuth also asserted that Minnesota Statutes, section 13.82, subdivision 16, allows the City to withhold the complete address data from the *Pioneer Press*. Section 13.82, subdivision 16, provides:

When data is classified as public under this section, a law enforcement agency shall not be required to make the actual physical data available to the public if it is not administratively feasible to segregate the public data from the not public. However, the agency must make the information described as public data available to the public in a reasonable manner. When investigative data becomes inactive, as described in subdivision 7, the actual physical data associated with that investigation, including the public data, shall be available for public access.

As the Commissioner opined in Advisory Opinion 94-054, section 13.82, subdivision 16, states that, when it is not administratively feasible for a law enforcement agency to separate public data

from not public data, it is permissible for the law enforcement agency to not provide physical access to the data but to make the public data available to the public in some other reasonable manner. This provision is not a basis on which to deny access to public data. The Commissioner does not agree that it applies to the situation at hand.

Mr. Hannah asked the Commissioner to determine whether the City responded appropriately to the *Pioneer Press*' data request. Pursuant to sections 13.03 and 13.82, the City must provide the *Pioneer Press* with the public data in the database and also withhold the not public data. However, in fulfilling its obligation under Chapter 13 to provide public data upon request, it is not appropriate for the City to withhold complete address information related to an incident because there is a possibility that release of the data will identify an individual whose identity must be protected pursuant to section 13.82. The City must determine, on a case-by-case basis, whether certain data related to an incident must be protected.

Finally, Ms. Rofuth states that Chapter 13 has not been updated to reflect issues related to electronic data storage. Government entities are storing data in increasingly larger databases. If those databases are not designed to accommodate an entity's obligation to provide appropriate access to public data, it can be challenging. The Commissioner encourages government entities that house data in large databases, such as the City of Saint Paul, to raise their concerns with the Legislature.

Opinion:

Based on the facts and information provided, the Commissioner's opinion on the issue that Mr. Hannah raised is as follows:

In agreeing to provide the *Pioneer Press* with certain incident-related public data (data in the "always public data fields"), the City of Saint Paul did comply with Minnesota Statutes, Chapter 13. However, the City did not comply with Chapter 13 in refusing to provide complete address data when the City had not determined that the release of the complete address data would identify an individual whose identity must be protected under section 13.82.

Signed:



Sheila M. Reger
Commissioner

Dated:

June 1, 2010