



Advisory Opinion 13-010

This is an opinion of the Commissioner of Administration issued pursuant to Minnesota Statutes, section 13.072 (2012). It is based on the facts and information available to the Commissioner as described below.

Facts and Procedural History:

On December 26, 2012, the Information Policy Analysis Division (IPAD) received a letter from Ian Bratlie, on behalf of the American Civil Liberties Union of Minnesota (ACLU-MN). In his letter, Mr. Bratlie asked the Commissioner to issue an advisory opinion about ACLU-MN's right to gain access to certain data the Minnesota Department of Public Safety (DPS) maintains. IPAD asked Mr. Bratlie to withdraw his request, pending the issuance of a report by the Office of the Legislative Auditor. Mr. Bratlie renewed his request on February 26, 2013.

IPAD, on behalf of the Commissioner, wrote to Ramona L. Dohman, DPS Commissioner, in response to Mr. Bratlie's request. The purposes of this letter, dated March 5, 2013, were to inform her of Mr. Bratlie's request and to ask her to provide information or support for DPS's position. On March 19, 2013, IPAD received a response, dated same, from E. Joseph Newton, General Counsel and Data Practices Compliance Official for DPS.

A summary of the facts as Mr. Bratlie provided them follows. He wrote:

The ACLU-MN is greatly concerned about racial profiling by law enforcement officers in Minnesota. We believe that law enforcement officials in Sibley County regularly run license plates of cars that they believe to belong to minorities. They can run license plates in two ways, they can either do it through dispatch or they can do it through on-board computers. When the searches are done through the on-board computer, the data stream is controlled by BCA. BCA and Sibley County Sheriff's Office have entered into a joint powers agreement to gather and store this information.

To combat this discriminatory practice, the ACLU-MN requested information relating to searches made by Sibley County Sheriff's Office (hereafter SCSO). Our first request was to SCSO itself. However, they told us the information was held by BCA. They made a request to BCA for the data but were told by ... BCA that they could not provide the information to SCSO.

According to Mr. Bratlie, ACLU-MN then asked BCA for access to the data SCSO did not maintain, namely three items of data: 1) license plate number queries run through on-board computers, by officer and date, 2) the data transmitted from BCA in response to those queries, and 3) the number of transactions per officer.

In response, BCA told Mr. Bratlie it had “no data responsive” to any of his requests. BCA “also suggested that information we were seeking might be protected by the Driver’s Privacy Protection Act [of 1994, or “DPPA”].” (18 U.S.C. section 2721.)

Mr. Bratlie objected to DPS’s position, and again asked BCA for access to the three items of data. According to Mr. Bratlie, BCA “now claimed” that the data were not accessible because data responsive to item 1) were “security information” per Minnesota Statutes, section 13.37, item 2) were protected by DPPA, and that BCA had no data responsive to item 3).

Issue:

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

Did the Minnesota Department of Public Safety respond appropriately to a request for the following data?

- Data showing all license plate numbers run through Sibley County Sheriff patrol cars on-board computer system, by officer and date, from January 1, 2012 to May 31, 2012.
- Data showing the response to those Sibley County squad car license plate initiated requests.
- Data showing the total number of transactions requested, by officer, from January 1, 2012 to May 31, 2012.

Discussion:

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

Mr. Newton described BCA’s “Archive Service” repository, which documents transactions made over its secure network to and from more than 20 repositories of data. According to Mr. Newton, the various repositories of data on individuals “include more than license plate data.” He wrote:

One type of transaction recorded in the Archive Service is a query that requests information maintained by the DPS Driver and Vehicle Services Division (DVS). An authorized criminal justice agency employee can retrieve DVS data by entering a license plate number. DVS returns data about the vehicle associated with the license plate and the registered owner. Those returned data elements are: the license plate, year and type of registration, the name, address and date of birth of the registered owner, the vehicle identification number or VIN, the year, make, model and color of the vehicle, the month the plate expires and the sticker number attached to the plate. Depending on the query used, driver’s license information for the registered owner may also be returned.

Mr. Newton also stated:

In order to retrieve data over the secure network, authorized agencies identify the devices that submit and receive data. If the device is a fixed computer in the offices of the authorized agency, a unique value is assigned for each user of that device and that information is stored in Archive Service. For a mobile device like a laptop that connects to the secure network, only the device identifier is known or stored, no information about the identity of the mobile user is available. Because the mobile devices may be shared by agency employees, the joint powers agreement between the agency and BCA requires that the agency be able to tell BCA which employee was using a mobile device at a particular date and time, if that information is needed to evaluate usage or resolve some other issue.

Mr. Newton stated that BCA maintains “license plate” data only in the Archive Service, and that those data “are classified as private data on individuals or non public data by a security information declaration issued by the DPS responsible authority. The query and response data requested in the first two items are both covered by the declaration.”

Minnesota Statutes, section 13.37, subdivision 1 (a), in relevant part, defines security information as: “government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury.” Section 13.37, subdivision 2, classifies security information as not public.

Mr. Newton wrote to the Commissioner:

Recognizing the jeopardy that could result to law enforcement officers, victims of crime and the general public if this quantity of data concerning the activities of criminal justice agencies and their employees was available to the public, the BCA requested that the DPS Commissioner ... issue a security information declaration to protect the data in the Archive Service.

In her written determination classifying “all government data contained in the system log files and the audit trail” as security information under section 13.37, Commissioner Dohman stated:

The Department of Public Safety’s Bureau of Criminal Apprehension has a division whose primary responsibility is to facilitate the sharing of data among criminal justice agencies. The division is called Minnesota Justice Information Services or MNJIS.

As part of its operations, MNJIS stores system log files which are used primarily for internal troubleshooting. MNJIS also maintains an audit trail of queries and responses made by criminal justice agencies These files and audit trail, if accessible to the public, would permit those engaged in illegal activities to determine what investigations were underway as well as the data returned in response to queries made by criminal justice agencies.

Mr. Newton stated that the security declaration applies to all data in the Archives Services, but the declaration states only that the system log files and the audit trail data are protected.

In his comments, Mr. Newton correctly noted that the Commissioner has deferred to another entity’s expertise in making determinations about classifying otherwise public data as security information. However, per Advisory Opinion 02-014:

The Commissioner has previously opined that section 13.37, subdivisions 1(a) and 2, may not be employed as a blanket classification scheme

The Commissioner wants to emphasize that, in the exercise of this discretion, a government entity must have reason to believe that public disclosure of such data would likely lead to substantial jeopardy. The entity cannot simply protect data from disclosure under section 13.37 on an arbitrary basis, but must base the determination on reasoned analysis.

The Commissioner accepts, in general, Commissioner Dohman's reasons, as set forth in her written declaration, that there are times when *otherwise public* data in the Archive Service may be protected as security information. In addition to the rationale provided in the declaration that public access to system log files and audit trail data would "permit those engaged in illegal activities to determine what investigations were underway as well as the data returned in response to queries made by criminal justice agencies," the Commissioner (of Administration) is aware that a fundamental purpose to maintain audit trails is to safeguard access and use of those systems against both internal and external misuse and tampering. Audit trails also provide a means to verify system activity and the accuracy of the data. Public access to individual queries and resulting data returned from those queries, unless aggregated, may also reveal vulnerabilities in the robustness of a system's ability to prevent and track misuse and tampering. With that said, the Commissioner encourages DPS to reconsider whether any of the data ACLU-MN requested are not system log files and/or audit trail data, and therefore are not subject to the security information declaration.

As the Commissioner has stated in previous opinions, section 13.37 provides entities broad discretion to address security concerns. It is up to the Legislature to weigh those concerns with other sometimes competing interests, i.e., public accountability and data subjects' rights.

(Note: In 2012, the Legislature amended section 13.37, subdivision 2, so that if an entity denies a data request based on the responsible authority's determination that the data are security information, then, "upon request, the government entity must provide a short description explaining the necessity for the classification." DPS should re-evaluate its declaration to determine whether the description provided fully articulates the necessity of the declaration in a manner that the public can understand.)

Mr. Newton discussed another justification for denying Mr. Bratlie's request:

The ACLU-MN is also not able to have access to the license plate data based on federal law. The license plate data maintained in the Archive Service are retrieved from the DVS repository. As noted in Minnesota Statutes, §168.346, subd. 1, license plate data, also known as vehicle registration data, are treated as provided in 18 United States Code § 2721. Pursuant to that federal law, the public is not allowed access to license plate data for individual registered owners. See §2721(a)(1). Because the registered owner can have access under the federal law, the closest state classification is "private data on individuals." Because the classification of the data "travels" with the data, DPS/BCA cannot disclose the data to a member of the public like the ACLU-MN.

According to DPPA, a "State department" of motor vehicles, such as DPS, is generally prohibited from disclosing to the public "personal information" about an individual obtained by DPS in connection with a "motor vehicle record." Section 2725 of DPPA defines those terms as follows:

- Personal information: information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

- Motor vehicle record: any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.

Furthermore, DPPA sets forth permissible uses under certain conditions. Pursuant to Minnesota Statutes, section 168.346, "data on an individual provided to register a vehicle shall be treated as provided [by DPPA] and shall be disclosed as required or permitted by that section." (Mr. Newton did not address how DPS can fulfill its obligation under this section to provide appropriate access to those data in light of DPS's security information declaration.)

The Commissioner respectfully disagrees that DPPA applies to data item 1. License plate numbers entered into the Archive Service by local law enforcement officers are not protected by DPPA, because the officer gained access to the number by looking at the license plate on a vehicle, not from the Archive Service.

Regarding data item 2), Mr. Bratlie wrote:

The information protected by DPPA, and cited in Minn Stat § 168.346, is personal information. Thus, at a minimum, BCA has given no explanation for why the ACLU-MN was not entitled to information on zip codes, vehicular accidents, driving violations, and driver's status that would have been in the replies.

The BCA has made an incorrect reading of Minn Stat § 168.346 which does permit them to share the data under the rules set up in the DPPA. DPPA permits information to be shared in 14 different scenarios. At least three of them apply here.

Mr. Bratlie discussed the permissible uses that he believes apply to ACLU-MN's request. The Commissioner acknowledges his position. However, per DPPA, it is up to Commissioner Dohman to determine whether any of the permissible uses apply to Mr. Bratlie's request.

Mr. Bratlie noted, and Mr. Newton concurred, that DPPA does not protect 5-digit zip codes. (In his comments, Mr. Newton stated, "[i]t is not clear what value zip codes have in determining whether racial profiling is occurring in Sibley County." Whether or not an entity believes public government data have "value" does not affect a person's access rights. See Minnesota Statutes, section 13.05, subdivision 12, and Minnesota Rules, part 1205.0300, subpart 2.)

Mr. Newton also stated that even if DPS "provided ACLU-MN with the zip codes for the license plates queried by Sibley County in early 2012, those are the only data they would be entitled to receive under the DPPA."

Mr. Newton also wrote:

The ACLU-MN also argues that BCA is somehow required by language in Minnesota Statutes, §168.346 to produce the data it has requested. This argument has no merit; chapter 168 directs the commissioner of public safety to take certain actions. See § 168.002, subd. 5. While BCA reports to the commissioner of public safety, BCA's operation of the Archive Service is not controlled by § 168.346. As was stated in BCA's November response to ACLU-MN, the part of DPS that controls access under the DPPA is Driver and Vehicle Services Division.

Minnesota Statutes, section 168.346, subdivision 1(a), provides: “[d]ata on an individual provided to register a vehicle shall be treated as provided by United States Code, title 18, section 2721, ... and shall be disclosed *as required or permitted* by that section.” (Emphasis added.) The Commissioner respectfully disagrees with Mr. Newton’s position that DVS makes that determination. As noted above, DPPA regulates disclosure of data by a *State department* of motor vehicles. Per section 168.346, the Commissioner of Public Safety must determine if DPPA requires or permits disclosure of the data ACLU-MN requested.

As to data item 3), Mr. Bratlie wrote, “BCA claimed that there is no responsive data to this request. This reply makes no sense.” Mr. Bratlie asserted that per the Joint Powers agreement, section 2.11, BCA should maintain the data. He wrote:

As BCA stated ... they created the software for tracking “direct access” “indirect access” and “computer to computer interface.” Direct Access is done when a deputy uses SCSO equipment, such as a squad car computer, to access the BCA systems, such as entering a license plate number. Under the joint powers agreement with SCSO, there must be a method in the software for identifying which individual officers at SCSO conducted a particular transaction.

The BCA Data Inventory list confirms this as it requires BCA to have data showing who queried a BCA database and when that query happened. Even the determination form signed by Ramona L. Dohman states that information it holds will be shared with a criminal justice agency to discipline an employee who has misused the data system. Dohman stated that “resolution of allegations of misuse will promote public safety by helping to preserve the integrity of the criminal justice community.” Thus, as required by the FBI, joint powers agreement and even as BCA policy, there is a way to determine which deputy made requests to the BCA for information.

However, as noted above, Mr. Newton stated that BCA stores only the device identifier, not data that identify the officer who made the query. The joint powers agreement between the agency and BCA requires that the agency tell BCA which employee was using a mobile device at a particular date and time, if BCA determines “that information is needed to evaluate usage or resolve some other issue.” Accordingly, neither DPS nor SCSO maintains all of the data that together are responsive to ACLU-MN’s request.

In summary, apparently ACLU-MN cannot get access to the data it seeks from DPS, because BCA does not maintain the data *by officer* conducting the query via a mobile device, which is what ACLU-MN asked for. It may want to ask again for aggregate data, including zip codes, not by officer.

The Commissioner has an additional comment. Mr. Bratlie also asserted that the data he requested are public under Minnesota Statutes, section 13.82, subdivisions 6 (response or incident data) or 7 (inactive criminal investigative data):

BCA is incorrect to argue that this information is private driver data. It is, after being sought by a deputy, investigative data which makes it available to the ACLU-MN. Upon commencing an investigation, even one based on racial animus, the deputy has created a search that is presumed to be public. While the investigation may be short - finding out whether or not the car belongs to a minority - the deputy has made both incident data and criminal investigation data....

The Commissioner acknowledges Mr. Bratlie's position, but the problem here is that SCSO does not maintain the data in question. However, if, by virtue of running a license plate number query the local law enforcement officer creates response or incident or criminal investigative data, and those data are an official record for purposes of Minnesota Statutes, section 15.17, then the local law enforcement agency (here, SCSO) should maintain the data per Minnesota Statutes, section 138.17, and provide appropriate public access.

Note: References to footnotes and exhibits omitted.

Opinion:

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

The Minnesota Department of Public Safety responded appropriately to a request for the following data, because it does not maintain the data:

- Data showing all license plate numbers run through Sibley County Sheriff patrol cars on-board computer system, by officer and date, from January 1, 2012 to May 31, 2012.
- Data showing the response to those Sibley County squad car license plate initiated requests.
- Data showing the total number of transactions requested, by officer, from January 1, 2012 to May 31, 2012.

However, DPS may need to reconsider whether any of the data ACLU-MN requested are not system log files and/or audit trail data, and therefore are not subject to the security information declaration pursuant to section 13.37, subdivisions 1(a) and 2.



Spencer Cronk
Commissioner

April 11, 2013