



Advisory Opinion 11-017

This is an opinion of the Commissioner of Administration issued pursuant to Minnesota Statutes, section 13.072 (2011). It is based on the facts and information available to the Commissioner as described below.

Facts and Procedural History:

On September 19, 2011, the Information Policy Analysis Division (IPAD) received a letter dated September 12, 2011, from Michael Ring. In his letter, Mr. Ring asked the Commissioner to issue an advisory opinion regarding his rights related to certain data collected by his employer, the Dakota County Attorney's Office. IPAD requested additional information/clarification, which Mr. Ring provided on October 5, 2011.

IPAD, on behalf of the Commissioner, wrote to James Backstrom, Dakota County Attorney, in response to Mr. Ring's request. The purposes of this letter, dated October 19, 2011, were to inform him of Mr. Ring's request and to ask him to provide information or support for the Office's position. On November 3, 2011, IPAD received a response, dated same, from Mr. Backstrom.

A summary of the facts as Mr. Ring presented them is as follows. He wrote in his opinion request:

... The Dakota County Attorney's Office required all professional and administrative staff to be fingerprinted recently. That process included collection of not only our fingerprints, it also included collecting names, gender, state [sic] of birth, height and weight. When I was fingerprinted on June 3, 2011, the deputy sheriff also requested my social security number for insertion on the fingerprint card. No Tennessee warning was given prior to collection of that data.

Issue:

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

Did the Dakota County Attorney's Office comply with Minnesota Statutes, Chapter 13, when it collected fingerprints from an employee and did not provide a Tennessee warning notice prior to collecting the data?

Discussion:

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

Data about employees are classified pursuant to Minnesota Statutes, section 13.43. Certain data about employees are public (section 13.43, subdivision 2) and certain data are private (section 13.43, subdivision 4).

When a government entity collects private or confidential data about an individual from that individual, the entity must provide a notice, commonly referred to as a Tennessean warning. (Minnesota Statutes, section 13.04, subdivision 2.) This notice must contain the following: (1) the purpose and intended use of the data; in other words, why the entity is collecting the data and how it will use the data; (2) whether the individual can refuse or is legally required to provide the requested data; (3) what the consequences are of supplying or not supplying the data; and (4) the identity of other persons or entities outside of the collecting agency authorized by state or federal law to receive the data.

In his comments to the Commissioner, Mr. Backstrom wrote that to carry out its statutory duty to prosecute crime, the County Attorney's Office requires access to the Criminal Justice Information System (CJIS). He explained that CJIS is a set of "state and federal electronic data bases that includes records of individuals that have been collected by state and federal law enforcement agencies engaged in the investigation and prosecution of crime."

Mr. Backstrom further wrote that CJIS is managed by the Minnesota Bureau of Criminal Apprehension (BCA), and that the BCA and the FBI impose personnel security policies and procedures on all law enforcement agencies as a condition of the BCA's providing electronic access to CJIS. He stated that one such requirement is that the "identity of all persons with direct access to a computer terminal that is linked to CJIS or the right to unescorted access to the area where the terminals are located must be verified by a national fingerprint-based record check." Mr. Backstrom wrote, "All employees and volunteers in my Office have either direct access to computer terminals that are linked to CJIS or unescorted access to the areas where these terminals are located."

Mr. Backstrom wrote that an email the office manager sent to all staff on May 18, 2011, constituted the Tennessean notice required by Minnesota Statutes, section 13.04, subdivision 2. Mr. Backstrom provided a copy of the email to the Commissioner and provided the following explanation:

... [The] email explains the purpose and intended use of the private data, states that the employees and volunteers are required to provide the data, states that failure to comply will result in termination of the agreement with the BCA that allows for access to CJIS and identifies that the data will be released to the BCA. The email directive constitutes managerial direction from the employer. Accordingly, the normal inference from such direction is that failure to comply with it would amount to insubordination and would warrant negative employment action.

Mr. Ring's question is whether the Office complied with Minnesota Statutes, Chapter 13, when it collected his fingerprints on June 3, 2011. The Commissioner has reviewed the May 18, 2011, email, and thinks it meets some requirements of a Tennesen notice. First, in stating that the fingerprints will be sent to BCA so it can conduct criminal background checks and that background checks are required because of new state and federal regulations, the email explains the purpose and intended use within the Office and that staff are legally required to provide fingerprints.

Second, in stating that fingerprints are going to the BCA, the Office informed Mr. Ring of outside persons or entities to which the Office has authority to release the fingerprints.

However, where the email notice falls short is in informing Mr. Ring of the consequences of supplying or not supplying his fingerprints. While the email states that failure to comply with the fingerprinting requirement means that the County Attorney's Office will no longer have access to CJIS, it does not explain the consequences to Mr. Ring, e.g., that failure to comply will result in negative employment action (as Mr. Backstrom described above). As the Commissioner has discussed in many previous advisory opinions, the purpose of the notice is to provide individuals with sufficient information to decide whether to provide the requested data.

In addition, going forward, it might be helpful to clearly label a Tennesen notice as such and explain that it is being supplied as required by Minnesota Statutes, section 13.04, subdivision 2. Nowhere in the May 18, 2011, email is it explained that the email constitutes a Tennesen notice.

It should be noted that both Mr. Ring and Mr. Backstrom discussed that in August 2011, almost three months after the Office collected Mr. Ring's fingerprints, Mr. Ring signed a consent form giving permission for the Office to release his fingerprints to the BCA. While this seems to indicate the Office can share the data with the BCA, it does not negate the obligation the Office had to provide a Tennesen notice at the time of collection. (See Advisory Opinions 95-028, 98-007, 04-009, 04-010, and 07-009.)

Finally, as the Commissioner previously has opined, if an entity is collecting an individual's Social Security number (SSN), federal law imposes some additional notice requirements. (See Advisory Opinions 01-040, 04-020, and 04-048.) (See also Federal Privacy Act of 1974, 5 U.S.C. § 552a note – Disclosure of Social Security Number.) The May 18, 2011, email does not meet all the federal notice requirements; therefore, the Office has not met its obligation under federal law. Mr. Backstrom did state that the Office ceased collection of SSNs but, apparently, not before it collected Mr. Ring's fingerprints. Mr. Backstrom wrote:

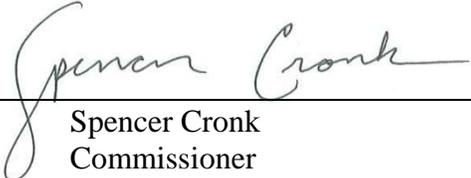
[The Sheriff's Office initially requested] that the employees and volunteers, at the time of fingerprinting, supply their social security number. However, that department subsequently learned that such information was not necessary in order to perform the national background checks. Accordingly, fingerprint cards with social security numbers on them were shredded ... the fingerprint cards were reprinted, and the affected employees had to sign the new fingerprint cards, which did not contain social security numbers.

Having learned the fingerprint cards with SSNs were collected in error, it is commendable that the Office disposed of them.

Opinion:

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

When the Dakota County Attorney's Office collected fingerprints from an employee, it provided some components of a Tennessee Warning notice, but not all. Therefore, it complied, in part, and did not comply, in part, with Minnesota Statutes, Chapter 13.

Signed: 

Spencer Cronk
Commissioner

Dated: November 23, 2011