COMMONWEALTH OF KENTUCKY
OFFICE OF THE ATTORNEY GENERAL

RUSSELL COLEMAN
ATTORNEY GENERAL

1024 CAPITAL CENTER DRIVE
SUITE 200
FRANKFORT, KY 40601
(502) 696-5300

24-ORD-044

February 21, 2024

In re: Phillip Hamm/McCracken County Sheriff's Office

Summary: The McCracken County Sheriff's Office ("the Sheriff's Office") did not violate the Open Records Act ("the Act") when it denied a request for certified copies of records or records that do not exist. The Sheriff's Office also did not violate the Act when it requested a resident of the county where the records are located to make an appointment to inspect records in person. The Act does not require the Sheriff's Office to comply with a request for electronic records in nonstandard format.

Open Records Decision

Phillip Hamm ("Appellant") submitted a request to the Sheriff's Office for records related to a criminal investigation. His request contained 11 subparts, but in sum, he sought the metadata associated with two deputies' personal cell phones, metadata associated with other electronic files, the internet search histories of the Sheriff's Office's employees that resulted in obtaining a specific photograph, certified copies of various records, and any policy "regarding the issuance of agency provided mobile devices." The Sheriff's Office timely responded and denied each part of the request for various reasons. This appeal followed.

The first four parts of the Appellant's request sought the metadata "created" on February 14, 2022, "from the cell phone used by" two deputies when they displayed a photograph to an inmate during a police interview and the metadata "associated" with the photograph. In subpart 6 of the request, the Appellant sought the internet search histories of any employees that resulted in them obtaining the photograph of the Appellant from his personal Facebook social media account. In subpart 10, the Appellant sought the metadata "from" a specific cell phone "used to take the photo" of a residence "which accompanied the application for a search warrant" at that location. The Sheriff's Office denied all of these requests because it claimed neither the metadata contained on the deputies' personal cell phones nor their personal internet search histories were "public records" under KRS 61.870(2), and therefore, none of these records are subject to inspection.

In subpart 8, the Appellant sought the metadata related to a specific file that was allegedly created on February 14, 2022, "at 4:16:08 pm" and "modified" at "10:23:17" the same day. The Sheriff's Office denied this subpart of the Appellant's request because it "previously supplied" the Appellant with the requested record. The Sheriff's Office further stated the Appellant could view the record again "by making an appointment" with the Sheriff's Office to inspect the record in person. Similarly, the Sheriff's Office invited the Appellant to make an appointment to inspect the search warrant for the residence, which the Appellant sought in subpart 9 of the request.

In subpart 5 of the request, the Appellant asked for a "certified copy of the original email" a deputy sent to a district court judge to obtain the search warrant. In subpart 7 of the request, the Appellant sought "certified copies" of three electronic files he identified by filename. The Sheriff's Office denied these requests because it is not required to provide "certified copies" of records in response to a request under the Act.

Finally, subpart 11 of the request sought a copy of any document or policy "regarding the issuance of agency provided mobile devices." The Sheriff's Office denied this request because no responsive records exist.

On appeal, the Appellant relies on the Office's decision in 23-ORD-057, which found that the photograph giving rise to all these requests is a public record because it was "used" for an official law enforcement purposes, *i.e.*, to obtain a witness's identification that was subsequently used to obtain and execute a search warrant. The Appellant argues the metadata related to the photograph is inseparable from the photograph itself, and thus, if the photograph is a public record, then the metadata must be as well. In response, the Sheriff's Office continues to assert that metadata contained on its employees' personally owned cell phones is not a "public record" under KRS 61.870(2). However, it also notes that the photograph at issue in 23-ORD-057 was destroyed, and therefore, any metadata associated with the photograph would have also been destroyed. Further, the Sheriff's Office claims that, even if the metadata still exists, its employees are unable to extract it. Rather, the Sheriff's Office would have to hire a private contractor at significant expense to perform the extraction. Relying on 19-ORD-091, the Sheriff's Office argues that, to the extent metadata could ever be considered a "public record," it exists in a nonstandard format. As such, it has discretion whether to comply with the Appellant's request. On this last point, the Office agrees. Thus, it is unnecessary to determine whether the metadata on the deputies' personal cell phones is a "public record" under KRS 61.870(2), because even if it is, the Sheriff's Office has discretion whether to provide it.

The Act divides electronic records into two possible formats: standard and nonstandard. *See* KRS 61.874(2)(b). The "standard format" is "a flat file electronic American Standard Code for Information Interchange (ASCII) format." *Id*. Any format other than ASCII format is a nonstandard format. *Id*. Thus, "[i]f the public agency maintains electronic public records in a format other than ASCII, and this format conforms to the requestor's requirements, the public record *may* be provided in this alternate electronic format for standard fees as specified by the public agency." *Id*. (emphasis added). In other words, a public agency has discretion whether to provide electronic records in a format other than ASCII. In 19-ORD-091, the Office determined that metadata contained on public agency devices is a "public record" under KRS 61.870(2), but that such data is not maintained in ASCII format, and therefore, a public agency has discretion whether to comply with a request for metadata. Because the Sheriff's Office has discretion whether to comply with a request for metadata, it did not violate the Act when it denied the Appellant's request.[1]

Nor did the Sherriff's Office violate the Act when it denied the Appellant's requests for "certified copies" of various records or when it requested that he make an appointment to view records in person. *See* 11-ORD-201 (finding no violation when an agency required a person residing in the county to inspect records in person and comply with the agency's procedure for obtaining certified copies of records). No provision of the Act requires a public agency to certify copies of its public records. *See, e.g.*, 03-ORD-207. Rather, the Act only entitles a resident of the Commonwealth to receive "copies" of public records in exchange for a reasonable fee that does not exceed the actual cost of making the copies. *See* KRS 61.874(3).

Moreover, a "public agency shall mail copies of the public records *to a person whose residence or principal place of business is outside the county in which the public records are located* after he or she precisely describes the public records which are readily available within the public agency." KRS 61.872(3)(b) (emphasis added). Because a public agency is only required to mail records to a person who resides, or whose principle place of business is located, outside of the county, the Office has held that a public agency can require a person residing in the county where the records are located to exercise his right of inspection in person. *See* 11-ORD-201. Although any person has the right to inspect records in person at the public agency during normal business hours, KRS 61.872(3)(a), the Office has found that a public agency does not violate the Act when it merely attempts to plan ahead for the requester's

[1] In an attempt to prove the Sheriff's Office is capable of extracting metadata, the Appellant provides 1,500 pages of information he received from the Sheriff's Office in response to a request for metadata associated with body-worn cameras. However, cell phones are not body-worn cameras and there is no proof in this record that metadata contained in cell phones is stored in ASCII format or that it can be extracted in the same way metadata is extracted from body-worn cameras.

visit and have the responsive records readily available for his inspection.[2] *See, e.g.*, 20-ORD-013. Of course, a public agency cannot prevent a person from exercising the right of inspection by making appointments difficult. *See, e.g.,* 15-ORD-182 (finding a violation when an agency continually cancelled appointments); 93-ORD-48 (finding a violation when the agency limited the hours for inspection from 8:00 a.m. to 11:00 a.m. for all requesters despite the agency not closing until 4:30 p.m.). But here, the Sheriff's Office states it merely requested that the Appellant, who resides in McCracken County, schedule a time to inspect the requested records so they could be gathered and placed in a secure location for his inspection. There is no evidence that the Sheriff's Office has placed unreasonable restrictions on the Appellant's right to inspection or that it has a pattern of cancelling the Appellant's appointments.

With respect to the Appellant's request for a policy "regarding the issuance of mobile devices," the Sheriff's Office claims no such record exists. Once a public agency states affirmatively that a record does not exist, the burden shifts to the requester to present a *prima facie* case that the requested record does or should exist. *See Bowling v. Lexington–Fayette Urb. Cnty. Gov't*, 172 S.W.3d 333, 341 (Ky. 2005). If the requester makes a *prima facie* case that the records do or should exist, then the public agency "may also be called upon to prove that its search was adequate." *City of Fort Thomas v. Cincinnati Enquirer*, 406 S.W.3d 842, 848 n.3 (Ky. 2013) (citing *Bowling*, 172 S.W.3d at 341). Here, the Appellant has not established a *prima facie* case that the Sheriff's Office possesses a policy regarding the issuance of mobile devices. Rather, he merely asserts that one should exist in light of Sheriff's Office employees using mobile devices to conduct law enforcement business. The Office's role in these disputes is to determine whether a public agency has complied with the Act, KRS 61.880(2)(a), not to pass judgment on the prudence of enacting any particular policy. Because the Appellant has not made a *prima facie* case that the requested policy exists, the Office cannot find that the Sheriff's Office violated the Act by not providing the requested policy.

Finally, the Sheriff's Office denied the Appellant's request for its employees' internet search history for the Facebook photograph because data on privately owned devices are not "public records." On appeal, the Sheriff's Office states the "search was performed on a private mobile phone on a private Facebook account. Therefore, no record exists within custody [*sic*] of the agency." The Sheriff's Office further states it "does not even know if a search record would exist in the possession of Facebook or Meta ([the] parent company of Facebook)." The Act defines "public record" as "all

[2] Indeed, given that the Act allows a public agency up to five business days to determine whether to comply with a request, and to determine whether any exemptions apply to responsive records, KRS 61.880(1), there is no basis to conclude that a person can demand immediate entry into a public agency and start perusing its files at will. It stands to reason, therefore, that the public agency may first ascertain when a requester plans to come and exercise his right of inspection so that the records are readily available and any other internal security controls can be established.

books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained *by a public agency*." KRS 61.870(2) (emphasis added). As explained in 23-ORD-057, the *photograph* was "used" to obtain an identification and, subsequently, a warrant. An internet search history is not a photograph. Assuming, without deciding, that "internet search history" could be considered "documentation regardless of physical form or characteristic," there is no evidence here that the deputies' search histories on their privately owned devices are "prepared, owned, used, in the possession of or retained by a public agency." KRS 61.870(2). The deputies did not show their search history to the suspect to obtain an identification—they showed him the photograph that was obtained as a result of the search. Therefore, unlike the photograph, the search history was not "used" by the Sheriff's Office for an official law enforcement purpose.

Moreover, to the extent a search history was "prepared," it would have been prepared by a private company, such as an internet service provider, Meta, or some other private company. The Sheriff's Office, after all, does not log every search performed by its employees on private devices into a document it possesses or retains.[3] Simply put, the deputies' internet search histories on their privately owned devices are not "public records," and therefore, are not subject to inspection. Accordingly, the Sheriff's Office did not violate the Act when it denied this part of the Appellant's request.

A party aggrieved by this decision may appeal it by initiating an action in the appropriate circuit court pursuant to KRS 61.880(5) and KRS 61.882 within 30 days from the date of this decision. Pursuant to KRS 61.880(3), the Attorney General shall be notified of any action in circuit court, but shall not be named as a party in that action or in any subsequent proceedings. The Attorney General will accept notice of the complaint emailed to OAGAppeals@ky.gov.

Russell Coleman
Attorney General

/s/ Marc Manley
Marc Manley
Assistant Attorney General

[3] In contrast, a public agency might choose to monitor its employees' internet traffic on the agency's equipment using specialized software for productivity analysis or other legal reasons. To the extent such an agency possesses a log of that activity, then the log could potentially be a "public record" subject to inspection unless an exemption applies.

#35

Distributed to:

Phillip Hamm
Cade Foster
Ryan Norman