STATE OF MINNESOTA
IN COURT OF APPEALS
A14-0487

Chris Gregerson,
Appellant,

vs.

Hennepin County and Tracey Martin,
Respondents.

Filed October 6, 2014
Affirmed
Rodenberg, Judge

Hennepin County District Court
File No. 27-CV-13-10910

Chris Gregerson, New Richmond, Wisconsin (pro se appellant)

Michael O. Freeman, Hennepin County Attorney, Toni A. Beitz, Assistant County Attorney, Minneapolis, Minnesota (for respondents)

Considered and decided by Schellhas, Presiding Judge; Worke, Judge; and Rodenberg, Judge.

U N P U B L I S H E D O P I N I O N

RODENBERG, Judge

Appellant Chris Gregerson challenges the district court's grant of summary judgment in favor of respondents Hennepin County and Tracey Martin and its denial of appellant's request to access data under the Minnesota Government Data Practices Act (MGDPA). We affirm.

FACTS[1]

Appellant maintains a website of stock images that can be licensed or purchased as prints. In 2005, appellant discovered that Vilana Financial, Inc. had used one of his photographs without permission. Appellant sued Vilana Financial, Vilana Realty, Inc., and the companies' principal shareholder, Andrew Vilenchik, for copyright infringement. In 2008, the federal district court awarded appellant $19,462 in actual and statutory damages for the unauthorized use of his photographs. *Gregerson v. Vilana Financial, Inc.*, No. 06-1164, 2008 WL 451060, at *10 (D. Minn. Feb. 15, 2008).

In 2009, appellant sued Vilana Financial, Vilenchik, Vladimir Kazaryan (a Vilana employee), and their attorneys and law firms, alleging malicious prosecution, abuse of process, and conspiracy. Hoping to uncover evidence to support his claims of malicious prosecution against attorney Boris Parker, appellant settled his claims with Vilana and Vilenchik, in exchange for Vilenchik's promises to waive his attorney-client privilege and to turn over correspondence with Parker. The district court later dismissed appellant's remaining claims. We affirmed the dismissal of appellant's claims. *Gregerson v. Vilana Financial, Inc.*, No. A10-0863, 2010 WL 4451820, at *1 (Minn. App. Nov. 9, 2010), *review denied* (Minn. Jan. 26, 2011).

In 2010, the Crystal police department obtained two search warrants to investigate alleged criminal activities of Vilenchik and the Vilana corporations unrelated to appellant's claims. The first search warrant was issued on probable cause to believe that

[1] We provide a detailed factual history leading up to the operative facts giving rise to appellant's claims to enable the reader to understand the context of appellant's claims in this case.

Vilana's premises were being used as an unlicensed massage parlor and authorized a search for massage therapy equipment, advertising materials related to massage therapy, and "computers and peripherals used to place online advertising, produce advertising materials or schedule client appointments." The second search warrant was issued on probable cause to believe that Vilenchik had engaged in theft by swindle in the sale of a fake diamond and authorized a search for financial and other records relating to diamonds and "computers and peripherals used to maintain financial transaction records of the diamond sale or used in the production of fictitious . . . papers."

When executing the two search warrants, Crystal police officers seized several computers. A Hennepin County forensic computer examiner "imaged the hard drives of sixteen of the seized computers so that [he] could conduct forensic analysis of their contents, within the parameters specified in the search warrants."[2] The examiner then used 35 key words provided to him by Crystal police officers to determine whether the hard drives contained evidence relevant to the theft-by-swindle and unlicensed-massage-parlor investigations. The key words did not include "Christopher Gregerson, Boris Parker, Vladimir Kazaryan, Michael Walker, Michael Zubitskiy, McShane, or the topics 'malicious prosecution,' or copyright." The examiner downloaded the results of his analysis onto a disc and gave it to the Crystal police department.

In April 2011, appellant sent a subpoena to the Hennepin County Sheriff's Office (HCSO) requesting copies of the hard drives. In response, Assistant Hennepin County

[2] Complete copies of the hard drives were made for examination and remain in evidence storage at the Hennepin County Sheriff's Office. The seized hard drives were then returned to their owners.

Attorney Toni Beitz informed appellant that the subpoena was improper and that the HCSO would not release a copy of the hard drives without a court order. Appellant then informed Beitz that he "wished the HCSO to deem [his] subpoena to be a request pursuant to the MGDPA." Beitz denied appellant's request to access the hard-drive images because the Crystal police department's criminal investigation was "still formally not closed" and "all data is technically still confidential." But Beitz also explained that the HCSO would not provide appellant with the hard-drive images even after the investigation was final.

In June 2012, appellant contacted Beitz to ask whether the criminal investigation was complete and when the statute of limitations would expire. He narrowed his request to any documents regarding Boris Parker, Morgan Smith, or himself, including e-mails and recorded conversations between Vilenchik and Parker. Beitz responded that "the criminal investigation still has not been officially closed" and that the statute of limitations was "three years or longer." Beitz also advised appellant to address any future requests to the Crystal police department or to the HCSO's responsible authority, respondent Major Tracey Martin.

In September, appellant contacted Martin to request access to "any documents (email, letters, etc.) contained on the seized hard drives which are to, from, or mention Boris Parker" and "any audio recordings tha[t] include the voice of, or mention, Boris Parker." Appellant also requested any documents or recordings that mentioned himself, Kazaryan, Walker, Zubitskiy, McShane, malicious prosecution, or copyright. Martin denied appellant's request for data and told appellant to address all future inquiries to the

City of Crystal because the HCSO "will not release any data without authorization from the City of Crystal."

In December, appellant made another request for data and requested "to be informed if [he was] the subject of any of the data on the hard drive images identified in [his] previous letter." Martin again denied appellant's request.

Appellant then sued respondents, alleging that "[he] is entitled to access or receive, on an expedited basis, documents [he] requested from [respondents] under the MGDPA." Appellant requested the district court to (1) compel compliance with the MGDPA, (2) grant declaratory relief, (3) authorize the disclosure of investigative data, and (4) order that he "is entitled to have access to the data he requested in his MGDPA requests" and compel respondents "to provide [him] with access to the requested data."

Respondents moved for summary judgment, arguing that the district court could not compel compliance with the MGDPA because appellant was seeking neither government data nor investigative data under the MGDPA. Respondents also argued that the requested information was protected under the United States and Minnesota Constitutions. Appellant also moved for summary judgment, arguing that he was entitled under the MGDPA to the data on the imaged hard drives that concerned him and his dispute with Vilana and its affiliates. The parties agreed that there were no genuine and material factual disputes.

The district court granted respondents' motion for summary judgment and denied appellant's motion. The district court concluded that "the data requested by [appellant do] not constitute 'government data' under the MGDPA," nor were they "criminal

investigative data under the MGDPA." Moreover, "a warrantless search of the data by the HCSO, as requested by [appellant], would violate the Fourth Amendment and the Minnesota Constitution." As additional bases for denying appellant's requested relief, the district court noted that appellant failed to join Vilenchik as a party and failed to demonstrate a bona fide legal interest because appellant was not entitled to the data. This appeal followed.

D E C I S I O N

The MGDPA

> regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Minn. Stat. § 13.01, subd. 3 (2012). "The purpose of the MGDPA is to reconcile the rights of data subjects to protect personal information from indiscriminate disclosure with the right of the public to know what the government is doing. The Act also attempts to balance these competing rights within a context of effective government operation." *KSTP-TV v. Ramsey Cnty.*, 806 N.W.2d 785, 788 (Minn. 2011) (quotation omitted).

The district court concluded that the MGDPA's definition of "government data" was ambiguous as applied here before concluding that "government data" means "only the specific data collected by the Crystal [police department] for its criminal investigation" and "used for a governmental purpose." Appellant challenges the district

court's determination that the data he requested were not "government data" under the MGDPA.

We review the district court's statutory interpretation of the MGDPA de novo. *KSTP-TV*, 806 N.W.2d at 788; *see also Schwanke v. Minn. Dep't of Admin.*, 851 N.W.2d 591, 594 n.1 (Minn. 2014) (applying de novo review to the "legal question[s] of statutory interpretation" when the MGDPA is unambiguous in context (quotation omitted)).

Our supreme court recently explained that "'[d]ata' are 'facts that can be analyzed or used in an effort to gain knowledge or make decisions' or, more broadly, are 'information.'" *Schwanke*, 2014 WL 3844200, at *2 (quoting *The American Heritage Dictionary of the English Language* 462 (5th ed. 2011)). "Government data" are "all data collected, created, received, maintained or disseminated by any government entity regardless of [their] physical form, storage media or conditions of use." Minn. Stat. § 13.02, subd. 7 (2012). Here, a government entity, the HCSO, collected and maintains data that could be analyzed in the future with a proper warrant. Therefore, the data on the imaged hard drives are "government data" under the MGDPA.[3]

Although the data are "government data," we hold that appellant is not entitled to receive copies of or search the hard drives for the information he seeks. Under the MGDPA, government data can be "classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic [data]." *Id.*,

[3] Respondents do not dispute that appellant seeks "data" or that the HCSO is a "government entity" under the MGDPA. They argue that the data are neither "government data" nor "investigative data."

subd. 8a; *see also* Minn. Stat. § 13.03, subd. 1 (2012) (explaining that government data are public unless federal or state law classify the data as private or confidential).

"The United States and Minnesota Constitutions protect 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.'" *State v. Diede*, 795 N.W.2d 836, 842 (Minn. 2011) (quoting U.S. Const. amend. IV) (citing Minn. Const. art. I, § 10). "A search conducted without a warrant issued upon probable cause is generally unreasonable." *State v. Flowers*, 734 N.W.2d 239, 248 (Minn. 2007). A search "occurs upon an official's invasion of a person's reasonable expectation of privacy. A reasonable expectation of privacy exists as to areas and objects in which the person invoking the Fourth Amendment has a subjective expectation of privacy that society is prepared to recognize as reasonable." *State v. Johnson*, 831 N.W.2d 917, 922 (Minn. App. 2013), *review denied* (Minn. Sept. 17, 2013). But "the reasonableness of a person's expectation of privacy is appraised on the basis of the facts as they existed at the time the invasion occurred." *Id.* at 923 (quotation omitted).

In *Johnson*, police officers obtained a search warrant authorizing seizure of the appellant's computer hard drive to search for evidence of child pornography. *Id.* at 920. An officer seized the appellant's computer hard drive when executing the search warrant, but the hard drive was not analyzed until seven months later. *Id.* The appellant argued that the eventual forensic analysis amounted to a warrantless search. *Id.* at 920-21. We explained that "a person has the same reasonable expectation of privacy in the concealed digital contents of a cellular telephone [or computer hard drive] as a person has in the

concealed physical contents of a container." *Id.* at 922 (quotation omitted). But "once the government lawfully seizes a container during the execution of a warrant authorizing the search of the container for particularly identified evidence, the owner's expectation of privacy in that evidence is frustrated." *Id.* at 924 (quotation marks omitted). Because there was no substantial likelihood that the appellant in that case had changed the contents of the hard drive after it was seized and because the hard drive was searched only for the evidence sought in the search warrant, the appellant did not have an expectation of privacy in the material on the hard drive that was identified in the warrant. *Id.*

Here, the two search warrants were issued based on probable cause to believe that Vilana's premises were being used as an unlicensed massage parlor and that Vilenchik had engaged in theft by swindle. The warrants authorized only a search of the computer drives for information related to those two specific crimes. As in *Johnson*, the Crystal police officers lawfully seized the hard drives, which were the equivalent of "containers" of the data sought by police. *See id.* "Therefore, the execution of the warrant[s] 'frustrated' and terminated [Vilenchik's and Vilana's] expectation of privacy in the hard drive[s] and the digital contents *identified in the warrant*." *See id.* (emphasis added). But the execution of the warrants did *not* frustrate any expectation of privacy in other data contained on the hard drives and not identified in the warrant. *See United States v. Carey*, 172 F.3d 1268, 1270, 1276 (10th Cir. 1999) (explaining that police officers should generally perform a keyword search of computer files for specific terms sought by the search warrant, and suppressing evidence of child pornography on a computer hard drive

when the warrant authorized a search for evidence of drug trafficking). Any search of the hard drives for the data appellant now seeks would be a warrantless search and would invade Vilenchik's reasonable expectation of privacy.[4] *See Johnson*, 831 N.W.2d at 922. Therefore, a search of the hard drives for the data appellant requested would violate the Fourth Amendment rights of the owner(s) of the hard drives.

The United States Supreme Court recently held that police officers "must generally secure a warrant" before searching the cell phones of recently arrested individuals. *Riley v. California*, 134 S. Ct. 2473, 2485 (2014). Like the cell phones in *Riley*, the hard drives here contain a large quantity of private information, which police officers cannot lawfully search without a warrant. *See id.* at 2489, 2494-95 (explaining that cell phones differ from other types of searchable containers because they contain every piece of information about the individual for the past several months or more). And, like the searches of the cell phones in *Riley*, there is no evidence that any exception to the warrant requirement would justify a warrantless search of the hard drives for appellant's information. *See id.* at 2494 (explaining that "other case-specific exceptions may still justify a warrantless search of a particular phone," but that no such exceptions applied). Contrary to appellant's suggestion, a search of the hard drives is not equivalent to an inventory search, *see Colorado v. Bertine*, 479 U.S. 367, 372, 107 S. Ct. 738, 741 (1987) (defining an inventory search), or a "one-time screening" of a President's papers as authorized by law, *see Nixon v. Adm'r of Gen. Servs.*, 408 F. Supp. 321, 361 n.56

[4] The district court observed that appellant should have joined Vilenchik as a party to this lawsuit because the data on the hard drives that was not subject to the search warrants belongs to him and his expectations of privacy in that data have not been disturbed.

(D.D.C. 1976) (allowing a warrantless search of President Nixon's papers according to federal law), *aff'd*, 433 U.S. 425, 97 S. Ct. 2777 (1977). The owner(s) of the data on the hard drives continue(s) to have a reasonable privacy expectation in the data, except to the extent of the warrants authorizing seizure of the drives for specific and limited purposes. Making the data on the hard drives available for public inspection under the MGDPA under these circumstances would be inconsistent with the constitutional principles underlying *Riley*. Simply stated, the government collected data on the seized hard drives but may not constitutionally access or inspect the data except as authorized by the warrants.

Appellant has commendably briefed the issues, but his argument assumes that, because the data are "government data" under the MGDPA, he is entitled to the data. But appellant ignores the next step in the analysis. Because the owner(s) of the hard drives continue(s) to have a reasonable expectation of privacy concerning all data on those hard drives not authorized to be accessed by the search warrants, the data are either "confidential data on individuals" or "protected nonpublic data." *See* Minn. Stat. § 13.02, subds. 3, 13 (2012). Federal constitutional law prohibits the seizure or inspection of the contents of the data beyond the scope of the search warrants. Even if data concerning appellant is contained on the hard drives collected by police officers pursuant to the search warrants, those warrants did not authorize the government to search for or collect that data. The reasonable expectation of privacy of the owner(s) of the hard drives in the contents thereof has not been extinguished or overcome. We therefore hold that the data

not authorized by the search warrants to be accessed by the government are inaccessible to appellant or any other person under the MGDPA.

Appellant also argues that the Fourth Amendment does not apply to a search conducted by a private individual like himself. In *United States v. Jacobsen*, airport employees examined a damaged package and discovered a white powdery substance, which police officers later determined to be cocaine. 466 U.S. 109, 111, 104 S. Ct. 1652, 1655 (1984). The United States Supreme Court explained that "[t]he initial invasions of respondents' package were occasioned by private action" and that such private action does not violate the Fourth Amendment. *Id.* at 115, 104 S. Ct. at 1657. Citing *Jacobsen*, appellant argues that his private search of the hard drives cannot violate the Fourth Amendment. But appellant asks the HCSO to conduct an additional search of the hard drives for data beyond the scope of the search warrants. Such a search involves government action, not private action, and triggers Fourth Amendment protection. *See id.* at 113, 104 S. Ct. at 1656.

The district court did not err in granting summary judgment to respondents.

Affirmed.