STATE OF MINNESOTA

IN SUPREME COURT

A14-1957

Court of Appeals

Stras, J.
Dissenting, Lillehaug, J., Gildea, C.J.
Took no part, Hudson, Chutich, JJ.

KSTP-TV,

Respondent,

vs.

Filed: August 24, 2016
Office of Appellate Courts

Metropolitan Council,

Appellant.

Mark R. Anfinson, Minneapolis, Minnesota, for respondent.

David D. Theisen, Deputy General Counsel, Sydnee N. Woods, Associate General Counsel, Metropolitan Council, Saint Paul, Minnesota, for appellant.

Mahesha P. Subbaraman, Subbaraman PLLC, Minneapolis, Minnesota, for amici curiae Public Record Media and The Minnesota Coalition on Government Information.

S Y L L A B U S

1. Video data from public buses is "personnel data" under Minn. Stat. § 13.43, subd. 1 (2014), only if it is "maintained" exclusively because an individual subject of the data is a government employee.

2. To determine whether particular data is "personnel data" under the Minnesota Government Data Practices Act, a government entity must classify the data at the time a request for access to the data is made.

Reversed and remanded.

O P I N I O N

STRAS, Justice.

This case is about the proper classification of video data under the Minnesota Government Data Practices Act ("Data Practices Act"). *See* Minn. Stat. §§ 13.01-.90 (2014). KSTP-TV ("KSTP") requested videos that contain recordings of two incidents involving the drivers of Metro Transit buses. Metro Transit, a division of Metropolitan Council, denied the request based on its conclusion that the videos contain non-disclosable, private personnel data on the bus drivers. *See* Minn. Stat. § 13.43 (defining "personnel data"). KSTP filed a complaint under the Data Practices Act with the Office of Administrative Hearings. Following a hearing, an administrative law judge concluded that KSTP was entitled to the video data under the Data Practices Act. The court of appeals affirmed. *KSTP-TV v. Metro Transit*, 868 N.W.2d 920, 921 (Minn. App. 2015). We reverse the decision of the court of appeals and remand to the Office of Administrative Hearings for further proceedings consistent with this opinion.

I.

The Data Practices Act governs public access to information maintained by government agencies in Minnesota. Minn. Stat. § 13.01, subd. 3. The Act covers data

"collected, created, received, maintained or disseminated" by government agencies "regardless of its physical form, storage media or conditions of use." Minn. Stat. § 13.02, subd. 7. In this case, the data sought by KSTP currently exists on DVDs "maintained" by Metro Transit. Each Metro Transit bus is equipped with a digital-recording system that records events occurring in and around the bus. The captured images and sounds sought by KSTP in this case were originally stored on hard drives located on two buses. The hard drives could hold as much as 330 hours of video before the system would begin to record over the oldest data first. The video data sought by KSTP would have been erased after the completion of the 330-hour recording cycle if Metro Transit employees had not downloaded and placed the data on DVDs. The disputed data in this case now exists exclusively in DVD form.

The data are video recordings of two incidents on Metro Transit buses. In the first incident, which occurred on July 26, 2013, a Metro Transit bus veered off the road and crashed while carrying passengers. KSTP requested the recording 45 days after the incident. In the second incident, which occurred on September 13, 2013, a bus driver allegedly had an altercation with a bicyclist. KSTP asked for a copy of the recording within 13 days of the incident.[1] Metro Transit employees downloaded the recordings from the

[1] On September 26, 2013, a representative of KSTP forwarded an email to KSTP's attorney. The forwarded email contained previous correspondence between KSTP and Metro Transit regarding KSTP's request for a recording of the September 13 incident. The email correspondence did not state when KSTP had first requested the data, only that Metro Transit had refused the request. Based on the email, KSTP must have requested the recording sometime between September 13 and September 26.

hard drives at some point after each incident, although the record is unclear about precisely when the transfers were completed. Metro Transit evaluated the conduct of both drivers, but did not discipline either of them. Metro Transit denied both of KSTP's requests, relying on the exception in the Data Practices Act that classifies some personnel data as private. *See* Minn. Stat. § 13.43.

After Metro Transit refused the requests, KSTP filed a data-practices complaint with the Office of Administrative Hearings. Following a hearing, an administrative law judge ("ALJ") concluded that the recordings were public data. In the ALJ's view, Metro Transit's decision to view the recordings to determine whether to discipline each driver did not convert them into private personnel data. Nor was the data private, in the ALJ's judgment, simply because it depicted a government employee. The ALJ therefore ordered Metro Transit to turn over copies of the requested videos to KSTP. In a published opinion, the court of appeals affirmed the ALJ's decision, concluding that the video recordings were public data because they "were maintained for a variety of purposes, and not solely because the bus drivers were government employees." *KSTP-TV*, 868 N.W.2d at 925. We granted Metropolitan Council's petition for review.

II.

The question presented in this case requires us to determine the proper classification of video data depicting incidents involving Metro Transit employees. If the video recordings contain public data, as KSTP argues, then KSTP has a right to access them. Minn. Stat. § 13.01, subd. 3. If, on the other hand, the information on the recordings are

private personnel data, as Metropolitan Council argues, then they "may [only] be released pursuant to a court order," Minn. Stat. § 13.43, subd. 4, or accessed by a subject of the data, *see* Minn. Stat. § 13.04, subd. 3; *Burks v. Metro. Council*, ___ N.W.2d ___, No. A14-1651, slip op. at __ (Minn. Aug. 24, 2016) (applying section 13.04, subdivision 3). The resolution of this question presents an issue of statutory interpretation that we review de novo. *Am. Nat'l Gen. Ins. Co. v. Solum*, 641 N.W.2d 891, 895 (Minn. 2002).

As a "public corporation and political subdivision of the state," Minn. Stat. § 473.123, subd. 1 (2014), Metropolitan Council qualifies as a "government entity," *see* Minn. Stat. § 13.02, subd. 7a (defining "government entity"). As a division of Metropolitan Council, Metro Transit is subject to the requirements of the Data Practices Act. *See* Minn. Stat. §§ 13.01, subd. 1, 13.02, subd. 7a, 473.123, subd. 1. The Data Practices Act contains a statutory "presumption that government data are public and are accessible by the public for both inspection and copying" unless an exception applies. Minn. Stat. § 13.01, subd. 3.

The exception relevant to this dispute is for "personnel data," which is defined as "government data on individuals *maintained because* the individual is or was an employee of . . . a government entity." Minn. Stat. § 13.43, subd. 1 (emphasis added). In denying KSTP's request, Metro Transit relied on the personnel-data exception, which contains three statutory elements, only the last of which is in dispute here.

The first element is that the data in question must be "data on individuals," which is defined as

> all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual.

Minn. Stat. § 13.02, subd. 5. The parties do not dispute that the data in question constitute "data on individuals." The "subject[s] of th[e] data" are the bus drivers, passengers, and pedestrians depicted on the video recordings, and the identity of these individuals is not "incidental to the data." *Burks*, ___ N.W.2d at ___, No. A14-1651, slip op. at __ (applying Minn. Stat. § 13.04, subd. 3). The purpose of the recordings, at least at an abstract level, is to keep a record of the events occurring in and around public buses and the identity of the individuals involved in those events.

The second element is that "data" must be "maintained." Minn. Stat. § 13.43, subd. 1. The common and ordinary meaning of the term "maintained" is to "keep in an existing state; [to] preserve or retain." *The American Heritage Dictionary of the English Language* 1058 (5th ed. 2011); *Webster's Third New International Dictionary* 1362 (2002) (defining "maintain" as "to keep in a state of repair, efficiency, or validity: preserve from failure or decline"). Although the videos were initially "maintained" on hard drives, they are now "preserv[ed] or retain[ed]" on DVDs because Metro Transit employees downloaded them. It is undisputed that Metro Transit continues to maintain the data requested by KSTP.

The third element, which is the focus of this case, is whether Metro Transit maintains the data "because the individual is or was an employee of a . . . government entity." Minn. Stat. § 13.43, subd. 1. The parties take differing positions on the meaning

and application of this element. Metropolitan Council argues that the recordings are personnel data "because the videos contain the recorded images and voices of the two bus operators who were employees" of Metro Transit and the purpose of placing the videos onto DVDs was to evaluate the "employees' conduct or performance during the incidents." This is true, Metropolitan Council claims, even if Metro Transit originally kept the data for multiple other reasons and only later decided to preserve the data solely for personnel purposes. KSTP, on the other hand, urges us to conclude that the recordings are public data because Metro Transit created them for a variety of reasons, including for public-safety and management purposes. Because some of these reasons initially required the data to be classified as public, KSTP argues, the data must remain public regardless of whether Metro Transit later decided to maintain the data on DVDs solely for personnel purposes.

To determine whether the video recordings are public or private data, the parties' arguments require us to answer two questions about "personnel data." First, we must decide *what* qualifies as personnel data: is data subject to the personnel-data exception even if there are multiple reasons for the government entity to maintain it? This question requires us to determine the meaning of the phrase "maintained because" in the personnel-data definition. Second, we must address *when* to classify the data: is the data classified at the time of its creation or at the time of the request? Answering this question requires us to look at the text of the personnel-data exception as well as other provisions of the Data Practices Act for guidance about the timing of making a classification.

A.

The first of the two questions—what qualifies as personnel data—focuses on the reasons for the government entity's maintenance of the data. Both parties have a reasonable answer to the "what" question. KSTP argues that, if there are multiple reasons for a government entity to "maintain the data," some of which are unrelated to personnel matters, the data is not "maintained because" the individual is an employee of the government entity. We call this the "single-purpose reading." Metropolitan Council interprets the phrase "maintained because" in precisely the opposite way. It asserts that it is "not relevant" that it uses the videos "for a variety of purposes," so long as the "video data were retained to evaluate employee conduct." We call this the "multiple-purpose reading." Both readings are reasonable.

We have already defined the word "maintained" as to keep in "an existing state; to preserve or retain." *The American Heritage Dictionary of the English Language* 1058 (5th ed. 2011). However, the meaning of the word "because," used as a conjunction in the statute, is unclear. "Because" means "since : for the reason that : on account of the cause that." *Webster's Third New International Dictionary* 194 (2002); *see also The American Heritage Dictionary of the English Language* 158 (5th ed. 2011) (defining "because" as "[f]or the reason that; since"). Although the use of the word "because" as a conjunction clearly connects the requirement that the data be "maintained" with the requirement that the subject of the data be an "employee of the government agency," the text of the statute does not explain the extent of the connection required between the two elements. *See* Minn.

Stat. § 13.43, subd. 1. It is unclear, in other words, whether the government entity must maintain the data solely for a personnel purpose or whether the personnel purpose can be just one justification among many. The statute is therefore ambiguous on the "what" question. *See State v. Hayes*, 826 N.W.2d 799, 804 (Minn. 2013).

Two aspects of the Data Practices Act convince us that the better interpretation of the statute is the single-purpose reading. *See id.* at 804-05 (adopting the "better interpretation" of an ambiguous statute); *In re Estate of Butler*, 803 N.W.2d 393, 397 (Minn. 2011) (same). First, the Data Practices Act's "scope" provision, aside from making clear that it covers "[a]ll government entities," contains an explicit statutory "presumption that government data are public and are accessible by the public for both inspection and copying." Minn. Stat. § 13.01, subds. 1, 3. We have described this provision as being "at the heart of the [A]ct." *Demers v. City of Minneapolis*, 468 N.W.2d 71, 73 (Minn. 1991). Adopting the multiple-purpose reading would allow government entities to shield data from public view simply by establishing that one of the reasons for preserving the data is that "the individual is or was an employee of . . . a government entity," Minn. Stat. § 13.43, subd. 1, even if the personnel-related reason is inconsequential and only one reason among many. *See Harlow v. Minn. Dep't of Human Servs.*, ___ N.W.2d ___, 2016 WL 4211955, at *5 (Minn. Aug. 10, 2016) (applying the presumption to reach a similar conclusion). Such a reading would allow the personnel-data exception to swallow the presumption.[2] *See id.*

[2] To be sure, "the provision regarding personnel data, Minn. Stat. § 13.43 . . . , provides that all personnel data on public employees is private unless specifically listed

The single-purpose reading also avoids a conflict among various provisions of the Data Practices Act. *See Am. Family Ins. Grp. v. Schroedl*, 616 N.W.2d 273, 277 (Minn. 2000) ("We are to read and construe a statute as a whole and must interpret each section in light of the surrounding sections to avoid conflicting interpretations."). A government entity can create or maintain data for a variety of reasons, and the single-purpose reading prevents situations in which particular data is simultaneously public and private under different provisions of the Data Practices Act.[3] For example, several provisions of the Data Practices Act declare that specific data are public, such as directory information maintained by public educational agencies and institutions and certain data "created or collected" by a

otherwise." *Annandale Advocate v. City of Annandale*, 435 N.W.2d 24, 27 (Minn. 1989). Metropolitan Council argues that this provision creates a counter-presumption that governs over the general presumption that all government data are public. We disagree. First, we have never described the provision on personnel data as creating a presumption, which means that the general presumption that data are public informs our interpretation of every provision of the Data Practices Act, including this one. Second, even if Minn. Stat. § 13.43 contains a presumption, the presumption is limited to the fact that "personnel data" are private, which is not the question we are asked to decide here. That is to say, we decline to extend the alleged presumption to the antecedent question of what data qualify as personnel data, which *is* the question the parties have asked us to decide.

[3] Although the dissent mentions in passing some of the statutory penalties associated with the Data Practices Act, several provisions make clear that the Legislature was also concerned about the privacy issues associated with data disclosure. Government entities and their employees face significant penalties if they misclassify data. In the event that a "government entity" improperly discloses private data, the entity is liable to any "person damaged" for the "damages sustained, plus costs and reasonable attorney fees." Minn. Stat. § 13.08, subd. 1. Willful violations of the Act subject entities "to exemplary damages of not less than $1,000, nor more than $15,000 for each violation." *Id.* The stakes are potentially even higher for individuals who violate the Data Practices Act. Any person who willfully violates the Data Practices Act is "guilty of a misdemeanor" and may be suspended or dismissed from public employment for "just cause." Minn. Stat. § 13.09.

medical examiner. Minn. Stat. §§ 13.32, subd. 5; 13.83, subd. 6. Yet these same data, depending on the reason a government entity decides to maintain them, can also satisfy the definition of private personnel data.

The facts of this case present another example of potential conflict. Metropolitan Council does not dispute that, if it were maintaining the data for solely a non-personnel reason, such as a safety-related purpose, then the data would be public. Similarly, if Metropolitan Council maintained the data solely because the subject of the data is an employee of the government entity, then the data would be private under the plain language of Minn. Stat. § 13.43. The single-purpose reading avoids a potential conflict in mixed-purpose cases by allowing data to be categorized as private or public, but not both, when it is "maintained" for more than one reason. We accordingly adopt the single-purpose reading because it is more consistent with the Data Practices Act as a whole. *See Schroedl*, 616 N.W.2d at 277.

B.

We now turn to the "when" question, which requires us to determine the point in time at which to classify the data. On this question, too, the parties have competing positions. The first possibility, advanced by Metropolitan Council, is that classification of data occurs when the government entity receives a request to access the data. According to Metropolitan Council's position, the relevant point for classifying the data would be when KSTP sent a request to Metro Transit to access the video recordings. The second possibility, asserted by KSTP, is that classification of the data is required when the

government entity initially creates, receives, or collects the data. If the initial collection of the data is the relevant point in time for classifying the data, then KSTP could be entitled to access the data if, when the data was initially stored on the hard drives, it was maintained by Metro Transit for a variety of reasons. According to KSTP, it would be entitled to view the data even if, as Metropolitan Council argues, Metro Transit later maintained the data on the DVDs solely for a personnel purpose.

The Data Practices Act "regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities." Minn. Stat. § 130.01, subd. 3. Unlike the words "collection" and "creation," which in the context of a particular piece of data occurs at a discrete point in time, the word "maintenance" refers to an ongoing decision by the government entity to "preserve" or "retain" the data. *The American Heritage Dictionary of the English Language* 1058 (5th ed. 2011). To take the facts of this case as an example, Metro Transit "maintained" the video recordings in different forms at different times. When the data were created, they were "maintained" on hard drives located on each bus, ostensibly for a variety of reasons, including public-safety and management purposes. However, after the recording system created the data, the system stored the data for only 330 additional operating hours before automatically erasing the data from the hard drives. At that point, Metro Transit only maintained the data in a different form—on DVDs—for an allegedly different purpose: to evaluate the conduct of the bus drivers. KSTP's argument, which focuses largely on the initial classification of the data, overlooks the fact that the verb "maintained," as used in the personnel-data exception,

necessarily has a temporal component.

We resolve the temporal question in two ways. First, we once again rely on the common and ordinary meaning of the word "maintained." As we state above, the word "maintained" refers to the "*existing* state" in which something is kept, *The American Heritage Dictionary of the English Language* 1058 (5th ed. 2011) (emphasis added), and once 330 hours of operating time on the video-recording system had passed, the data no longer existed on the hard drives.[4] By using the word "maintained," rather than "created" or "collected," the personnel-data exception focuses on the "existing state" of the data—that is, the form of the data at the time a request to access it is made.[5]

---

[4] The dissent does not tell the whole story, omitting perhaps the most critical fact: in the absence of Metro Transit's evaluation of the bus drivers, the data would not exist at all after the 330 hours had passed. It is at that point—and only at that point—that the data becomes private under the single-purpose reading. To the extent that the dissent implies otherwise by hypothesizing about government agencies intentionally hiding data under the personnel-data exception, the dissent thoroughly dismantles a straw man. Moreover, even if the dissent were correct that our decision today encourages government agencies to "hide" otherwise-public data under the personnel-data exception, we are not free to interpret the Data Practices Act to make it reflect what *we* think it *should* say. Rather, it is our job to interpret the Act as written and it is the Legislature's job to draft legislation, as it deems appropriate, addressing the dissent's concerns about transparency and accountability.

[5] The Data Practices Act defines "government data" as "all data *collected, created, received,* [*or*] *maintained* . . . by any government entity." Minn. Stat. § 13.02, subd. 7. It is notable, however, that the definition of personnel data uses only the verb "maintained," which must cover something different than data that is "collected, created, or received" under the canon that "no word, phrase, or sentence should be deemed superfluous, void, or insignificant." *Schroedl*, 616 N.W.2d at 277 (citation omitted) (internal quotation marks omitted). The dissent, through sleight of hand, simply replaces the word "maintained" with "created" in the personnel-data exception to support its assertion that "the images were maintained by Metro Transit from the instant the signals went from the cameras to a digital

Second, our interpretation is reinforced by Minn. Stat. § 13.03, subd. 9, which provides that, "[u]nless otherwise expressly provided by a particular statute, the classification of data is determined by the law applicable to the data at the time a request for access to the data is made, regardless of the data's classification at the time it was collected, created, or received." Under the plain language of this provision, "the classification of data" is determined based on the "law applicable to the data at the time" a request is made.[6] *Id.* Thus, it is the timing of the request, not the "data's classification at the time" the data was "created," that determines the data's classification under the Data Practices Act. *Id.*

---

storage medium." Our approach, by contrast, interprets the statute as a whole, treating the Legislature's differing word choices as significant. *See id.* at 277, 280-82 (requiring courts to read statutes as a whole and to give meaning to each individual word in a statute).

[6] We interpret the phrase "law applicable to the data at the time" a request is made as requiring the government entity to examine whatever provision within the Data Practices Act is applicable to the data at the time the request is made, which in this case was the personnel-data exception. Minn. Stat. § 13.03, subd. 9. The statute is not exclusively, nor even primarily, a choice-of-law provision that guides a government entity in its selection of which version of the Minnesota Statutes to apply, nor is it a one-way ratchet, as the dissent suggests, "prevent[ing] an entity from obstructing access to public data on the ground that the data *used to be private*." In fact, the dissent cannot point to any specific phrase or words within Minn. Stat. § 13.03, subd. 9 that supports its novel, unidirectional interpretation of the statute. If anything, the use of the words "collected, created, or received" in subdivision 9, but not the word "maintained," fully supports *our* interpretation by harmonizing it with the plain language of the personnel-data exception. These words indicate that the classification of data can change as the data evolves from creation to maintenance.

III.

Having resolved the two interpretive questions raised by the parties' arguments, we now turn to an examination of the record to determine if KSTP is entitled to access the data it has requested from Metro Transit under the Data Practices Act. If KSTP requested the recordings while they were still stored on the hard drives, then under the single-purpose reading we adopt above, it could be entitled to access the data. If, however, KSTP requested the recordings after they were erased from the hard drives and placed on DVDs, then Metropolitan Council could successfully argue that the recordings were personnel data maintained only because "the individual is or was an employee of" Metro Transit. Minn. Stat. § 13.43, subd. 1.[7]

The record indicates that KSTP requested the video recordings from the July 26, 2013, bus crash 45 days after the incident occurred. Nevertheless, the record fails to include certain facts that are necessary for us to resolve whether the video data was public or private personnel data at the time KSTP made the request. The record indicates that the buses' video-recording system could hold only 330 hours of video data, but we do not know how many hours per day the system ordinarily operated. Accordingly, we do not know whether the data existed only in DVD form, or on both a DVD and the hard drive, when KSTP requested the data. Additionally, the record does not indicate whether the data

[7] Certain types of personnel data are public, such as actual gross salary, job title and bargaining unit, the existence and status of any complaints or charges against the employee, and the final disposition of any disciplinary action. Minn. Stat. § 13.43, subd. 2. KSTP does not argue that the requested video recordings are public personnel data.

was being "maintained" exclusively for a personnel purpose at the time Metro Transit received the request, which is a factual question for the ALJ to resolve on remand.

In contrast, the record is strongly suggestive that the recording of the September 13, 2013, incident with the bicyclist existed in both DVD form and on the hard drive when KSTP requested it on or before September 26, 2013. After all, even if the video-recording system on the bus had operated for 24 hours a day—an unlikely possibility—the video data of the incident would still have been available 13 days later on the hard drive. Even so, as with the recording of the July 26 incident, we remand to the ALJ to determine in the first instance whether the recording of the September 26 incident was "maintained" by Metro Transit exclusively for a personnel purpose at the time KSTP made its request to access the data.

IV.

For the foregoing reasons, we reverse the decision of the court of appeals and remand to the Office of Administrative Hearings for further proceedings consistent with this opinion.

Reversed and remanded.

HUDSON, CHUTICH, JJ., took no part in the consideration or decision of this case.

D I S S E N T

LILLEHAUG, Justice (dissenting).

Because the court decides that public data—images of events that occurred in public, on public transportation—can morph into private data, and thereby become inaccessible to the public, I respectfully dissent. Such a misreading of the Minnesota Government Data Practices Act, Minn. Stat. §§ 13.01–.90 (2014), has the effect of throwing under the bus two of our important democratic values: transparency and accountability.

I.

The facts are undisputed. When you ride a Metro Transit bus, you are in a public place. You, your fellow passengers, your driver, and the activities on the bus itself are being recorded by up to five cameras.

Metro Transit records you for multiple reasons. Recorded images of bus activity are useful to deter misconduct, investigate crime, respond to rider complaints, discipline employees, and defend personal injury and property damage claims. While some riders might be surprised to learn that they are being recorded, Metro Transit's rationale is that a public bus is a public place. And so it is.

The images Metro Transit records are stored on a hard drive located in the bus. There the images remain, until the hard drive is full, when the oldest images begin to be replaced with newer ones. Like any digital file, the images may be copied onto other media. In this case, the data KSTP-TV (KSTP) seeks are the images moved verbatim from hard drives to digital video disks.

The images on the hard drive are public data from the moment of their electronic creation, and the court so holds. In other words, KSTP seeks only images that were public data when created and maintained on the hard drives.

But Metro Transit contends that the public data are no longer public. Metro Transit's argument rests on the theory that the data classification changed from public to private when the images were moved from the hard drive to digital disks for use in personnel matters. Put another way, KSTP's requests were too late; it missed the bus. Unfortunately, the court agrees.

II.

Does the Minnesota law that is the foundation of Minnesotans' access to their government's information, such as these images, require such a result? No, it does not.

The entire presumption of the Data Practices Act is that "government data are public and are accessible by the public." Minn. Stat. § 13.01, subd. 3. This presumption is "at the heart" of the Data Practices Act. *Demers v. City of Minneapolis*, 468 N.W.2d 71, 73 (Minn. 1991). We applied this presumption recently when we held that data may remain public under one provision of the Data Practices Act even though the same data are classified as confidential under another provision. *Harlow v. Minn. Dep't of Human Servs.*, __ N.W.2d __, 2016 WL 4211955, at *4-5 (Minn. Aug. 10, 2016).

The exception to this presumption of public access on which Metro Transit relies, and on which the majority rests its decision, is for "personnel data," defined as "government data on individuals maintained because the individual is or was an employee of . . . a government entity." Minn. Stat. § 13.43, subd. 1. I agree with the court and the

parties that images of bus passengers and drivers are, among other things, "data on individuals." I also agree with the court that the images were created and (at least initially) maintained for multiple purposes, as I have already discussed. And I agree with the court that the "personnel data" exception applies only if the images are kept for the "single purpose" of personnel matters. But the court has a blind spot when it concludes that images that are already public become private simply because the request for access comes after, rather than before, a personnel matter commences.

Most importantly, the statute says no such thing. Given the presumption of access that is at the heart of the Data Practices Act, one would think that, if the Legislature had wanted to give government entities the right to turn public data into private data, it would have said so, clearly and unequivocally. It did not.[1] *See Rohmiller v. Hart*, 811 N.W.2d 585, 591 (Minn. 2012); *Genin v. 1996 Mercury Marquis*, 622 N.W.2d 114, 117 (Minn. 2001) ("The rules of construction forbid adding words or meaning to a statute that were intentionally or inadvertently left out."). *Cf. Doe v. Minn. State Bd. of Med. Exam'rs*, 435 N.W.2d 45, 50 (Minn. 1989) ("[A]gency rules cannot classify data as 'private' or make data inaccessible to the public 'unless there is a state statute or federal law as the basis for the classification.' " (quoting Minn. R. 1205.0200, subp. 9 (1987))).

[1] By contrast, another part of the Data Practices Act provides that, when a government entity collects data for an active civil investigation or anticipated legal action, the data becomes "protected nonpublic data." Minn. Stat. § 13.39, subd. 2. But even such data may become public upon court order, *id.*, subd. 2a, or when the investigation becomes inactive, *id.*, subd. 3. This shows that if the Legislature intends to have a government entity re-classify data, it knows how to direct that entity to do so.

To the contrary, the Data Practices Act sends a strong signal that moving public data from one medium to another, whatever the reason, does not make public data private. The statute provides expressly that, for the purpose of access, "government data" means "all data . . . regardless of its physical form, storage media or conditions of use." Minn. Stat. § 13.02, subd. 7. And it expressly contemplates that public data in digital form will be moved from medium to medium. *See* Minn. Stat. § 13.03, subd. 3(e) ("The responsible authority of a government entity that maintains public government data in a computer storage medium shall provide to any person making a request under this section a copy of any public data contained in that medium, in electronic form, if the government entity can reasonably make the copy or have a copy made.").

The only portion of the Data Practices Act that deals generally with "[c]hange in classification of data" is Minn. Stat. § 13.03, subd. 4. Four of its five subparts cover dissemination of data among agencies, which is not at issue here. The remaining subpart, (a), is inapplicable here. Subpart (a) says that an entity must change the data classification if it is required to do so to comply with "judicial or administrative rules pertaining to the conduct of legal actions" or with a specific statute applicable to the data. *Id.* Metro Transit does not rely on subpart (a), and there is no separate judicial, administrative, or statutory requirement. Accordingly, the Data Practices Act contains no general authority, express or implied, for a government entity to turn its public data into private data.[2]

[2] This is not to say that there is no remedy when a government entity's "appropriate security safeguards" for private data, Minn. Stat. § 13.05, subd. 5(a)(2), break down and the private data mistakenly is made accessible. The entity must notify individuals when

Minnesota Statutes § 13.03, subd. 9, on which the court relies, does not give any such authority. Rather than empowering entities to make public data private, subdivision 9 empowers data requesters to access data previously classified as private.

Subdivision 9 provides: "Unless otherwise expressly provided by a particular statute, the classification of data is determined by the law applicable to the data at the time a request for access to the data is made, regardless of the data's classification at the time it was collected, created, or received." Minn. Stat. § 13.03, subd. 9. The purpose of this plain and unambiguous language is obvious: the government entity holding the data must apply the Data Practices Act in effect at the time of the request, rather than deny access on the theory that the data was private under prior law. This prevents an entity from obstructing access to public data on the ground that the data *used to be private*. As explained by commentators (including a former director in the Minnesota Department of Administration), subdivision 9 allows "an act of the Legislature" to make public data that was classified as "not public." Donald A. Gemberling & Gary A. Weissman, *Data Practices at the Cusp of the Millennium*, 22 Wm. Mitchell L. Rev. 767, 825 (1996). Subdivision 9 implements—not undermines—the presumption of the Data Practices Act that government data is public.[3]

---

their data has been breached, Minn. Stat. § 13.055, and the remedies include a private cause of action, injunctive relief, administrative penalties, and criminal penalties. Minn. Stat. §§ 13.08, subds. 1-2, 13.085, 13.09.

[3] Contrary to the majority's contention, I do not read subdivision 9 as a "one-way ratchet." Given the presumption that data is public, it is unlikely that the Legislature would amend the Data Practices Act the other way, that is, to make public data private.

In this case, the Legislature did not change the law applicable to the images in any material respect from the time Metro Transit created and began to maintain the images until the time KSTP made its requests for them. KSTP seeks access to the images based on the Data Practices Act in effect at the time of its request—the very statute the court now misreads.

Nor is the authority to transform public data into private data found in the portion of the Data Practices Act that, with specific exceptions, makes personnel data private. Section 13.43 covers "government data on individuals maintained because the individual is or was an employee of . . . a government entity." Minn. Stat. § 13.43, subd. 1; *see Star Tribune Co. v. Univ. of Minn. Bd. of Regents*, 683 N.W.2d 274, 279-80 (Minn. 2004).

Section 13.43, like all of the exceptions to the public accessibility presumption of the Data Practice Act, assumes that the government data requested is not yet public. *See Annandale Advocate v. City of Annandale*, 435 N.W. 2d 24, 29 (Minn. 1989) ("[T]he legislature has expressly indicated that *confidential* personnel data of government employees shall not become public") (emphasis added). Certainly it does not say, or even hint, that already-public data may be turned into private data by its mere maintenance for a personnel purpose.

I see absolutely no significance in the fact that the definition of personnel data, Minn. Stat. § 13.43, subd. 1, uses the word "maintained" rather than "collected," "created," or "received." Obviously, the Legislature chose the word "maintained" because all data is "maintained," or kept, after it is first collected, created, or received. That the word

"maintained" was employed begs the question whether already-public data necessarily becomes private because it is maintained for a personnel matter.

Any reading of section 13.43 to the effect that a government entity may transform public data into private data by moving it into a personnel file is unreasonable. Imagine a situation where, using a government laptop computer, a government employee generates an indisputably public report. The employee prints off one exact copy[4] and puts it in a government employee's personnel file. Before the report can be further copied and disseminated, the laptop is destroyed. There is no backup. By Metro Transit's and the majority's reasoning, the sole remaining copy—the one in the personnel file—must now be private because it has become "personnel data." Thus, by the majority's analysis, the personnel-data exception trumps the bedrock principle of the Data Practices Act that government data is presumed to be public.

Although the court is careful to say that it has tried to read the Data Practices Act so as not to allow the personnel-data exception to swallow the presumption, its decision today will undermine transparency and accountability. I suspect that today's decision will be taken by some government entities as a free pass to conceal that which should be public. If government data—whether a video, a paper document, or a digital file—might show misconduct, and disclosure might cause embarrassment or worse, then today's decision

[4] The alteration or annotation of public data for use in a personnel matter presents an entirely different situation. In such a case, the alterations or annotations might well be private (and could be redacted from the public data) under the personnel-data exception.

enhances the temptation for the entity to stash the data in an employee's personnel file. What is public becomes private—perhaps forever.[5] Odds are that the now-private data will never see the light of disinfecting sunshine.[6]

To summarize, KSTP requested images of public activity on public buses. All of the images were public from the moment of their creation. The images, generated for multiple purposes, were public data when maintained on hard drives. The images KSTP sought were, are, and remain public regardless of the medium on which they are maintained. Therefore, KSTP had a statutory right to inspect, copy, and broadcast these images for the benefit of its viewers. For these reasons, I would affirm the decision of the court of appeals, which affirmed the decision of the administrative law judge.

GILDEA, Chief Justice (dissenting).

I join in the dissent of Justice Lillehaug.

---

[5] Unlike, for instance, civil investigation data, which can become public when the investigation is no longer active, personnel data becomes public only upon "final disposition of any disciplinary action." Minn. Stat. § 13.43, subd. 2(a)(5). Only then is access granted to "the specific reasons for the action and data documenting the basis of the action . . . ." *Id.*

[6] As Louis Brandeis wrote: "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." Louis D. Brandeis, *What Publicity Can Do*, Harpers Wkly, Dec. 20, 1913, at 10.