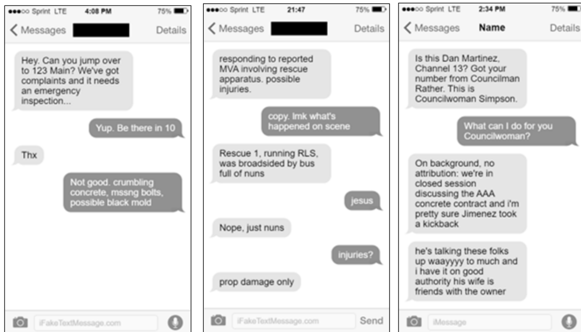
Can I see that?: Sunshine-ability of text messages

City of Kansas City, Missouri
Law Department
Missouri Municipal Attorneys Association
Summer 2023

1

Do any of these look familiar?



2

Scenario 1:

Each of these text messages was both sent and received on a city-owned phone. A Sunshine request comes in and these texts would be responsive to the request. Do you produce them?

3

Start with the Statute(s)

RSMo § 610.011.1:
It is the public policy of this state that ... records ... of public governmental bodies be open to the public unless otherwise provided by law.

RSMo § 610.023.2:
Each public governmental body shall make available for inspection and copying by the public of that body's public records.

4

Start with the Statute(s)

RSMo § 610.010(6):
"Public record", any record, whether written or electronically stored, retained by or of any public governmental body...

5

O'Connor v. Ortega, 480 U.S. 709 (1987)

(1) Reasonable expectation of privacy?
(2) Work-related purpose or work-related misconduct?

Government searches ok to "retrieve work-related materials or to investigate violations of workplace rules"

6

City of Ontario v. Quon, 560 U.S. 746 (2010)

Search of police officer's text messages was for a "legitimate work-related purpose" and "was not excessive in scope"

Id. at 764-65.

7

Scenario 1:

Each of these text messages was both sent and received on a city-owned phone. A Sunshine request comes in and these texts would be responsive to the request. Do you produce them?

YES!

8

Scenario 2:

Each of these text messages was both sent and received on a <u>private phone</u>. A Sunshine request comes in and these texts would be responsive to the request. Do you produce them?

9

Lessons from Case Law:

- **Missouri hasn't ruled on whether business messages on private phones are subject to Sunshine**
- **Other states have ruled that government business conducted on private cell phone is subject to open records**

10

Lessons from Case Law:

- **Lunney v. Arizona, 418 P.3d 943 (Ariz. 2017)**
- **Nissen v. Pierce Cnty., 357 P.3d 45 (Wash. 2015)**
- **Comstock Residents Ass'n v. Lyn Cnty. Bd. Of Comm'rs, 414 P.3d 318 (Nev. 2018)**
- **Denver Post Corp. v. Ritter, 255 P.3d 1083 (Colo. 2011)**
- **McKay v. State Div. of Admin., 143 So.3d 510 (La. 2014)**
- **Paint Twnshp. V. Clark, 109 A.3d 796 (Pa. 2015)**

11

Start with the Statute(s)

RSMo § 610.010(6):
"Public record", any record, whether written or electronically stored, retained by or of any public governmental body...

12

Lessons from Case Law:

Glasgow Sch. Dist. V. Howard Cnty. Coroner, 633 S.W.3d 822 (Mo. App. W.D. 2021)
"[T]his court is tasked with determining whether Coroner's Office violated the Sunshine Law when it did not disclose the records not in its custody. We find that it did not."

13

Lessons from Case Law:

Sansone v. Governor of Missouri, 648 S.W.3d 13 (Mo. banc 2022)

"the messages and data Sansone seeks were not in existence, in the possession of the Governor's Office, or retrievable at the time of his request."

14

Scenario 2:

Each of these text messages was both sent and received on a private phone. A Sunshine request comes in and these texts would be responsive to the request. Do you produce them?

NO!

15

16

Missouri Secretary of State:

"Communications are subject to 610 RSMo, more commonly known as the Sunshine Law. Government records on cell phones (business **and** personal phones) are subject to Sunshine requests..." (emphasis in original)

17

So what do I do??

- **No expectation of privacy in city-owned phones!**

18

KCMO AR 1-16

B. Privacy Generally
1) The City can search and employees shall not have an expectation of privacy with respect to the use of a City supplied technology asset, whether being used for conduct of the City's business or for an approved exemption.
2) The City can search and employees shall not have an expectation of privacy to any City data stored on any portable device or non-City asset, whether the device is encrypted or not, if the data is not stored on City assets.

19

So what do I do??

- **No expectation of privacy in city-owned phones!**
- **Guidelines for workplace searches.**
- **Ban ephemeral messaging apps.**
- **Ban personal phone texting.**

20

So what do I do??

"All county business generate on personal mobile devices are subject to the Public Records Act . . . . Text messages sent and received on a personal mobile device are not stored in any other form. Employees shall not use texting for any County business"

21

So what do I do??

- No expectation of privacy in city-owned phones!
- Guidelines for workplace searches.
- Ban ephemeral messaging apps.
- Ban personal phone texting.
- Require saving/forwarding/synching texts.

22

So what do I do??

"Employees utilizing cell phones for City business must not utilize written cell phone capabilities such as text messaging or email for City business unless such phone is synchronized with the City's computer system so that such electronic records can be maintained according to the State records retention requirements."

23

24

Questions?

Tara Kelly
tara.kelly@kcmo.org

City Attorney's Office
City of Kansas City, Mo.
414 E. 12th Street, 23rd Floor
Kansas City, MO 64106
(816)-513-3117
www.KCMO.gov

25

648 S.W.3d 13
Missouri Court of Appeals, Western District.

Ben SANSONE, Appellant,
v.
GOVERNOR OF MISSOURI, et al., Respondents.

WD 84426
|
Filed: June 7, 2022
|
Application for Transfer to Supreme Court Denied July 26, 2022

Synopsis

Background: Records requester filed Sunshine Law petition against the Governor's Office, alleging that former Governor and other Office employees violated the Sunshine Law. The Circuit Court, Cole County, Jon E. Beetem, J., 2019 WL 6178663, granted Governor's motion for summary judgment. Requester appealed.

Holdings: The Court of Appeals, Hardwick, P.J., held that:

Office did not violate the Sunshine Law when it failed to disclose information that was no longer in its possession;

requester failed to meet his burden of establishing that records he sought were existing public records subject to disclosure under Sunshine Law;

as matter of first impression, Office had statutory authority to close records of Governor's personal cell phone number;

Office's response to records request did not violate its statutory obligation to give a detailed, reasonable explanation of cause for delay in access;

requester was not entitled to Sunshine Law injunction forbidding the Governor's Office from using ephemeral messaging applications; and

stay of general discovery was warranted, pending resolution of threshold issue of whether requested records were public records subject to disclosure under Sunshine Law.

Affirmed.

Procedural Posture(s): On Appeal; Motion for Summary Judgment.

***15 APPEAL FROM THE CIRCUIT COURT OF COLE COUNTY, THE HONORABLE JON E. BEETEM, JUDGE**

Attorneys and Law Firms

Mark J. Pedroli, Clayton; Daniel J. Kolde, St. Louis for appellant.

Robert M. Thomspon, Kansas City; Barbara A. Smith, St. Louis; Scott R. Pool, Adam Hermann, Jefferson City; and Colen Gaus, St. Louis for respondent.

Before Division One: Lisa White Hardwick, Presiding Judge, Alok Ahuja, and Mark D. Pfeiffer, Judges

Opinion

Lisa White Hardwick, Judge

Ben Sansone, on behalf of The Sunshine Project ("Sansone"), appeals the circuit court's entry of summary judgment against him and in favor of the Governor of Missouri [1] and the custodian of records for the governor's office, Michelle Hallford (collectively, "the Governor's Office"), on Sansone's petition alleging that the former governor, Eric Greitens, Hallford, and other Governor's Office employees violated ***16** the Sunshine Law. [2] Sansone contends the court misinterpreted and misapplied the law in several respects and abused its discretion in staying discovery related to six of his claims. For reasons explained herein, we affirm.

FACTUAL AND PROCEDURAL HISTORY

On December 20, 2017, Sarah Madden, special counsel for the Governor's Office under Greitens, received an email on behalf of Sansone requesting that Hallford provide records under the Sunshine Law. The email included these five requests:

> 1. Documents or phone records, including logs, that show the date that the governor or anyone employed by the governor's office downloaded the phone application Confide on any [of] their mobile phones.

2. Documents or phone logs that show the date that the governor and anyone employed by the governor's office downloaded any mobile phone and/or computer application which purpose of the application is to automatically destroy text messages and/or other forms of communication after the communication is sent or received.

3. Documents or phone records that show the mobile phone numbers used by the governor.

4. A copy of all SMS messages, text messages, and/or communications sent and/or received by the Governor using the mobile phone application Confide.

5. A copy of all SMS messages, text messages, and/or communications sent and/or received by anyone employed by the governor's office using the mobile phone application Confide. [3]

Madden responded to the email within three business days. In her response, she stated that the Governor's Office was reviewing the request and anticipated being able to provide a response or a time and cost estimate, if applicable, for the requested records in no more than twenty business days. After receiving this response, Sansone filed a petition against the Governor's Office seeking an immediate injunction prohibiting the governor and all Governor's Office employees from using Confide or any other automatic communication destruction software and alleging violations of the Sunshine Law and the State and Local Records Law.

Madden sent a follow-up letter to Sansone on January 25, 2018. In this letter, Madden stated that the Governor's Office did not have any records to provide in response to his request for the date that Greitens or anyone employed in the Governor's Office downloaded the Confide application and for the Confide messages sent or received by Greitens or anyone employed in the Governor's Office. As for the remaining requests, Madden stated that any records in response to Sansone's request for the date that Greitens and anyone employed by the Governor's Office downloaded any cell phone and/or computer application whose purpose is to automatically destroy text messages and/or other forms of communication after the communication is sent or received would be considered closed pursuant to Sections 610.021(21) and 610.021(18). She explained that the disclosure of such information ***17** would impair the ability of the Governor's Office's Security Division to protect Greitens and his staff and asserted that the interest in non-disclosure outweighed the public interest in disclosure. Lastly, with respect to Sansone's request for Greitens's cell phone numbers, Madden stated that such records were considered closed under Sections 610.021(14) and 407.1500.

In May 2018, Sansone filed a second amended petition. In his second amended petition, Sansone again sought injunctive relief prohibiting the Governor and all Governor's Office employees from using Confide or any other automatic message destruction software (Count I). Sansone alleged seven counts of Sunshine Law violations: the Governor's Office failed to provide access to the records within three days, in violation of Section 610.023.3 (Count II); the Governor's Office failed to provide a detailed and reasonable explanation of the cause of the delay in producing the record within three days, in violation of Section 610.023.3 (Count III); the Governor's Office failed to produce records showing the date that Greitens and anyone employed in the Governor's Office downloaded Confide on their cell phones, in violation of Section 610.023.3 and .4 (Count IV); the Governor's Office deliberately misapplied Section 610.021(21)'s "terrorism exception" and Section 610.021(18)'s "hacker exception" in refusing to produce records of the date that Greitens and anyone employed in the Governor's Office downloaded any automatic message destruction software (Count V); the Governor's Office deliberately misapplied Section 407.1500 in refusing to produce records showing Greitens's cell phone numbers (Count VI); the Governor's Office violated Section 610.023.2 when it failed to collect, maintain, and produce messages sent or received by the office using Confide (Count VII); and there was a civil conspiracy between all defendants to violate the Sunshine Law by using automatic message destruction software (Count VIII). [4]

The court entered an order stating that discovery should proceed sequentially to determine whether any messages sent or received over the Confide application could be recovered, either through Confide, Inc., Confide-affiliated third-party servers, or on cell phones that send or receive messages using Confide. The court ordered Sansone to serve a subpoena on Confide, Inc. The court further ordered the Governor's Office to produce and pay for a forensic expert to conduct a forensic examination, using exemplar cell phones, to determine whether any messages sent or received using Confide could be recovered on those phones after those messages are sent or received. The order provided that, after Sansone received the report from this expert, he could depose the expert and, at his discretion and cost, put forth his own

expert to conduct his or her own review. The court stayed all other pending discovery until it could determine whether or not messages sent or received using Confide could be recovered, which the court stated "may have a bearing on what records are at issue." The court reiterated that, at that point in the process, it needed "to ascertain exactly what type of evidence is likely to exist as well as the exact nature of the operation of the Confide application."

In response to Sansone's subpoena, Confide, Inc.'s co-founder and president, Jon Brod, sent a letter stating:

> ***18** As an end-to-end encrypted and ephemeral messenger, all Confide messages and substantially all data disappear after a message is read. The data we retain and are able to provide is principally around account creation – user name, email address and/or phone number used to sign up for the account, and when the account was created. We do not have any data on deleted accounts, including whether or not the account ever existed.

The Governor's Office hired forensic expert John Mallery to determine what artifacts, if any, could be recovered from an iPhone that is using the Confide application. According to Mallery, the difference between an ordinary messaging application and an ephemeral messaging application such as Confide is that, in an ephemeral messaging application, once the messages are sent, they are automatically deleted from the phone that sent them, and once the messages are read, they are automatically deleted from the phone that received them. In contrast, standard messaging applications require user interaction to delete sent and received messages.

Mallery analyzed an Apple iPhone 6s, which he set up as a new phone, and downloaded and installed the Confide application. Mallery then sent and received messages using Confide. After the messages had been sent from and received by the test phone, Mallery processed and analyzed the test phone using industry standard forensic analysis tools from MSAB, Cellebrite, and XRY. Mallery chose Cellebrite because it has been in the mobile device industry for a very long time and the FBI uses it. XRY is used by police, law enforcement, military, government intelligence agencies, and forensic laboratories in over 100 countries. According to Mallery, he performed all possible extractions of data on the test phone. After performing the extractions, he analyzed the extracted data using non-case sensitive keyword searches, including terms, phrases, and phone numbers, and he performed a manual review of the data.

Mallery was able to verify that Confide does not allow the recipient to retain opened messages; sent messages are deleted from the sender's phone upon the opening of a new message; and the last unopened sent message is no longer on the sender's phone after 48 hours. Mallery assumed the recipient of an unopened message would not have access to the message after 48 hours. In Mallery's opinion, text messages sent and received using Confide cannot be recovered using forensic methodology, and he was "fairly certain" that fragments from messages sent and received using Confide on an iPhone cannot be recovered. Mallery believed there was "zero chance" of using forensic methods to reconstruct messages sent or received via Confide.

Mallery opined that he would have reached the same result if he had conducted the same experiment on a different version of the iPhone, on another type of phone such as an Android, with a different version of the Confide application, or if he had used any particular phone that a member of the Governor's Office might have had. He admitted, however, there was a "slim possibility" that the results would have been different on a different version of the phone. Mallery concluded that his findings were consistent with Confide, Inc.'s description of the application and were also expected when using an ephemeral messaging application.

Mallery issued his report stating these conclusions and was deposed by both parties. During his deposition, Sansone questioned Mallery extensively about his qualifications and the scope of his analysis. Mallery admitted that he had no other ***19** experience with Confide before this case. Although Mallery's searches identified several configuration files on the phone for the Confide application, he did not open those files. He explained that configuration information "allows the application to run." Mallery was "not certain" as to whether configuration files contained any personal information about someone's use of Confide, but he did not believe that they did.

Mallery testified that he could "potentially" or "possibly" determine the dates the Confide application was downloaded on and deleted from a phone; however, he did not perform

such an analysis. Additionally, he testified he did not perform any analyses to determine how many messages were sent or received using Confide, who received or sent messages using Confide, whether using the microphone to speak a message into Confide would leave any artifacts or metadata that could be recovered, or whether messages could be recovered if Confide was used on a desktop computer instead of a phone. Mallery explained that the scope of his analysis was very limited in that he was simply trying to determine whether or not he could find artifacts from specific messages that were sent and received, and he "did no other analysis on the application Confide beyond that."

Sansone declined the opportunity to have an expert of his choosing perform a forensic analysis. The Governor's Office filed a motion for summary judgment in December 2018. Sansone requested time to conduct additional discovery before responding to the summary judgment motion.

On July 8, 2019, the court denied the motion for additional discovery after finding that "the discovery sought would not have made a difference as it primarily went to the mental state of the alleged violators or to issues after [Sansone]'s Sunshine Law request was submitted." The court granted summary judgment in favor of the Governor's Office on all counts except Count VI, which concerned the Governor's Office's refusal to produce Greitens's cell phone numbers. In its judgment, the court found that the undisputed facts established that messages sent and received using Confide are not retained on the device or on a server. The court found that, "[t]o the extent that it is a record, it is not much different tha[n] a digital phone call which exists only for the moment." The court noted that, while Sansone was permitted to engage an expert, he did not do so and, therefore, he could not controvert Mallery's findings. The court further noted that Sansone's counsel argued a number of facts on which Mallery might be subject to impeachment, but because Sansone's counsel was not an expert, such arguments did not satisfy Sansone's burden to show that genuine issues of material fact remained.

With regard to each count, the court found on Count I that enforcement of Chapter 109's records retention requirements was not available via private action and, therefore, Sansone was not entitled to an injunction; on Count II that no violation occurred because the Governor's Office replied within three days; on Count III that the Governor's Office's explanation for its delay in providing records was reasonable; and on Counts IV, V, VII, and VIII that the undisputed facts indicated that the records Sansone was seeking, *i.e.*, the dates that Greitens and Governor's Office employees downloaded Confide or other ephemeral messaging applications and the Confide messages that Greitens and Governor's Office employees sent and received, did not exist. The court subsequently ordered that discovery proceed only on Count VI, which asserted that the Governor's Office deliberately misapplied Section 407.1500 in refusing to produce ***20** records showing Greitens's cell phone numbers.

Sansone filed a motion for partial summary judgment on Count VI. In his motion, he sought a judgment ordering that Greitens's cell phone numbers were public records that could not be closed and had to be produced. The Governor's Office filed a cross-motion for summary judgment arguing that Greitens's personal cell phone number [5] was a closed record and that, even if it was not a closed record, the court should still grant summary judgment in its favor because the decision to close the record of his cell phone number was made in good faith and was not a knowing and purposeful violation of the Sunshine Law.

On February 22, 2021, the circuit court entered an amended judgment finding that Greitens's personal cell phone number was an individually identifiable personnel record and, therefore, was exempt from disclosure under Section 610.021(13). The court granted summary judgment in favor of the Governor's Office on Count VI and incorporated by reference its July 8, 2019 order granting summary judgment in favor of the Governor's Office on all other counts. Sansone appeals.

STANDARD OF REVIEW

Appellate review of summary judgment is essentially *de novo. ITT Commercial Fin. Corp. v. Mid-Am. Marine Supply Corp.*, 854 S.W.2d 371, 376 (Mo. banc 1993). Summary judgment is appropriate when there are no genuine issues of material fact and the movant is entitled to judgment as a matter of law. Rule 74.04(c)(6). "Only genuine disputes as to material facts preclude summary judgment." *Goerlitz v. City of Maryville*, 333 S.W.3d 450, 453 (Mo. banc 2011).

Where, as in this case, the movant is the defendant, the movant establishes the right to judgment as a matter of law by showing one of the following:

> (1) facts negating any one of the claimant's elements necessary for judgment; (2) that the claimant, after an adequate period of discovery, has not been able to—and will not be able to—produce evidence sufficient to allow the trier of fact to find the existence of one of the claimant's elements; or (3) facts necessary to support [its] properly pleaded affirmative defense.

Roberts v. BJC Health Sys., 391 S.W.3d 433, 437 (Mo. banc 2013).

In determining whether the movant has met this burden, we review the summary judgment record in the light most favorable to the party against whom judgment was entered and accord that party the benefit of all reasonable inferences. *Goerlitz*, 333 S.W.3d at 453. We "do not weigh conflicting evidence or make credibility determinations." *Brentwood Glass Co. v. Pal's Glass Serv., Inc.*, 499 S.W.3d 296, 302 (Mo. banc 2016). "Instead, summary judgment tests 'simply for the existence, not the extent' of genuine issues of material fact." *Id.* (quoting *ITT*, 854 S.W.2d at 378). "A factual question exists if evidentiary issues are actually contested, are subject to conflicting interpretations, or if reasonable persons might differ as to their significance." *Id.* (quoting *Martin v. City of Washington*, 848 S.W.2d 487, 492 (Mo. banc 1993)). "Only evidence that is ***21** admissible at trial can be used to sustain or avoid summary judgment." *Jones v. Union Pac. R.R. Co.*, 508 S.W.3d 159, 162 (Mo. App. 2016) (citation omitted). "Hearsay statements cannot be considered in ruling on the propriety of summary judgment." *Id.* (citation omitted).

Citing *Dial v. Lathrop R-11 School District*, 871 S.W.2d 444, 446 (Mo. banc 1994), both parties state that we must examine the "entire record" to determine whether any genuine issues of material fact remain. This is not an accurate statement of current law. In a more recent case than *Dial*, the Supreme Court described the record we review on summary judgment:

> [1] Facts come into a summary judgment record *only* via Rule 74.04(c)'s numbered-paragraphs-and-responses framework. [2] Courts determine and review summary judgment *based on that Rule 74.04(c) record, not* the whole trial court record. [3] Affidavits, exhibits, discovery, etc. generally play only a secondary role, and then only as cited to support Rule 74.04(c) numbered paragraphs or responses, *since parties cannot cite or rely on facts outside the Rule 74.04(c) record.* [4] Summary judgment rarely if ever lies, or can withstand appeal, unless it flows as a matter of law from appropriate Rule 74.04(c) numbered paragraphs and responses *alone.*

Green v. Fotoohighiam, 606 S.W.3d 113, 117-18 (Mo. banc 2020) (quoting *Jones*, 508 S.W.3d at 161). As the Court noted in *Green*, when read together, these principles "require a court to 'determine whether *uncontroverted* facts established via Rule 74.04(c) paragraphs and responses demonstrate movant's right to judgment *regardless of other facts or factual disputes.*' " *Id.* at 118 (citation omitted). Neither the circuit court nor the appellate court should "sift through the entire record to identify disputed issues, which, in turn, would cause a court to impermissibly act as an advocate for a party." *Id.*

ANALYSIS

In Point I, Sansone contends the circuit court erred in granting summary judgment against him because the court misinterpreted Section 610.010(6)'s definition of the term "public record" to require retention as "an exclusive definitional element and necessary condition of a public record." Sansone argues this interpretation is contrary to legislative intent and the plain meaning of the term as it is used in the Sunshine Law.

Section 610.010(6) defines a "public record" subject to disclosure under the Sunshine Law as:

> [A]ny record, whether written or electronically stored, retained by or of any public governmental body including any report, survey, memorandum, or other document

WESTLAW © 2023 Thomson Reuters. No claim to original U.S. Government Works.

> or study prepared for the public governmental body by a consultant or other professional service paid for in whole or in part by public funds, including records created or maintained by private contractors under an agreement with a public governmental body or on behalf of a public governmental body; provided, however, that personally identifiable student records maintained by public educational institutions shall be open for inspection by the parents, guardian or other custodian of students under the age of eighteen years and by the parents, guardian or other custodian and the student if the student is over the age of eighteen years. The term "public record" shall not include any internal memorandum or letter received or prepared by or on behalf of a member of a public governmental body consisting of advice, opinions and recommendations in connection with the deliberative decision-making ***22** process of said body, unless such records are retained by the public governmental body or presented at a public meeting. Any document or study prepared for a public governmental body by a consultant or other professional service as described in this subdivision shall be retained by the public governmental body in the same manner as any other public record[.]

We need not decide whether messages exchanged by Greitens and his staff using Confide, and other data concerning the Governor's Office's use of Confide, constituted "public records" under this definition. Even if the requested information constituted "public records," Sansone's request faces a separate, insuperable obstacle: the summary judgment record establishes, as a matter of undisputed fact, that the messages and data Sansone seeks were not in existence, in the possession of the Governor's Office, or retrievable at the time of his request.

The Sunshine Law only requires that governmental agencies provide access to records then in existence, and in the agencies' possession or under their control. As the Missouri Supreme Court recognized in *Hemeyer v. KRCG-TV*, 6 S.W.3d 880 (Mo. banc 1999), "While chapter 109 specifies how long materials are retained, access is governed by chapter 610" – the Sunshine Law. *Id.* at 882. Where requesters have asked government agencies to create customized compilations or summaries of their records, we have held that the Sunshine Law was inapplicable, since it only requires agencies to disclose *existing* records – not to create new ones. "The plain language of the Sunshine Law does not require a public governmental body to create a new record upon request, but only to provide access to existing records held or maintained by the public governmental body." *Jones v. Jackson Cnty. Circuit Ct.*, 162 S.W.3d 53, 60 (Mo. App. 2005); *accord*, *Am. Family Mut. Ins. Co. v. Mo. Dep't of Ins.*, 169 S.W.3d 905, 915 (Mo. App. 2005) (agency could properly refuse records request where "the data requested ... was not contained in an existing record held by" the agency).

Similarly, in *Glasgow School District v. Howard County Coroner*, 633 S.W.3d 822 (Mo. App. 2021), we recently held that the Howard County Coroner's Office had not violated the Sunshine Law when it failed to disclose exhibits that were admitted at a public coroner's inquest, but which were "generated by or obtained by the sheriff's department" and retained by the sheriff's department after the inquest. *Id.* at 833. We explained: "[T]his court is tasked with determining whether Coroner's Office violated the Sunshine Law when it did not disclose the records not in its custody. We find that it did not." *Id.*

Two provisions of the Sunshine Law address the duty of governmental agencies to maintain possession of public records. Those provisions are inapplicable here, however. Section 610.027.1 provides that, upon service of a summons or a pleading asserting a Sunshine Law claim, "the custodian of the public record that is the subject matter of such civil action shall not transfer custody, alter, destroy, or otherwise dispose of the public record ... until the court directs otherwise"—even if the agency claims that the record is not a "public record" or that it is exempt from disclosure. In this case, the information at issue was destroyed well before the filing of this lawsuit; accordingly, Section 610.027.1 is inapplicable. Section 610.023.2 provides that "[n]o person shall remove original public records from the office of a public governmental body or its custodian without written permission of the designated custodian." Sansone does not

argue that the information at issue here was "remove[d] ***23** ... from the office of a public governmental body"—indeed, he makes no argument that the data he seeks was ever physically located in the Governor's Office.

We also recognize that Section 610.025 specifically designates as public records certain "message[s] relating to public business" that are "transmit[ted] ... by electronic means" and requires those messages to be transmitted to the agency's custodian of records, or to the sender's "public office computer." [6] Sansone has never invoked this provision, however, either in the circuit court or on appeal and, accordingly, we do not consider its potential applicability to the information Sansone requested.

Defining the records subject to disclosure under the Sunshine Law as records that have been maintained by a public governmental body makes sense in light of the purpose of Chapter 610, which is to provide *access* to such records. *See Hemeyer*, 6 S.W.3d at 882. Adoption of Sansone's argument would lead to the absurd result that public governmental bodies would have to provide access to records that they do not hold or maintain, either in their keeping or someone else's. "When engaging in statutory interpretation, we are to presume a logical result, as opposed to an absurd or unreasonable one, and we are always led to avoid statutory interpretations that are unjust, absurd, or unreasonable." *State ex rel. Jones v. Prokes*, 637 S.W.3d 110, 116 (Mo. App. 2021) (internal quotation marks and citations omitted).

Prior to a Sunshine Law request, whether a record must have been retained and, if so, for how long are issues governed by Chapter 109, not Chapter 610. *See Hemeyer*, 6 S.W.3d at 882. Chapter 610 governs access to records, *id.*, and public governmental bodies can only provide access to records that they hold or maintain, either in their keeping or someone else's. The circuit court did not err in finding that the Governor's Office did not violate the Sunshine Law when it failed to disclose information that was no longer in its possession. Point I is denied. [7]

In Point II, Sansone contends the circuit court erred in granting summary ***24** judgment in favor of the Governor's Office because the court erroneously shifted the burden of persuasion to him to prove the Governor's Office violated the Sunshine Law. Section 610.027.2 provides:

> Once a party seeking judicial enforcement of sections 610.010 to 610.026 demonstrates to the court that the body in question is subject to the requirements of sections 610.010 to 610.026 and has held a closed meeting, record or vote, the burden of persuasion shall be on the body and its members to demonstrate compliance with the requirements of sections 610.010 to 610.026.

Under this section, the party seeking enforcement of the Sunshine Law has the initial burden of demonstrating that "a governmental body is subject to the Sunshine Law and that it has claimed that a record is closed." *Gross v. Parson*, 624 S.W.3d 877, 891 (Mo. banc 2021) (quoting *Laut v. City of Arnold*, 491 S.W.3d 191, 194 (Mo. banc 2016)). Once the party makes this showing, "the burden is on the governmental body to demonstrate that the Sunshine Law does not require disclosure." *Id.* (quoting *Laut*, 491 S.W.3d at 194). Sansone argues that he met his initial burden because he established that the Governor's Office was a public governmental body that closed records by destroying them, and the court should have then shifted the burden of persuasion to the Governor's Office to establish that its closures and "destruction of records" were permissible pursuant to an exemption.

As we explained in Point I, to constitute a public record subject to disclosure under the Sunshine Law, the record must have been maintained by the agency at the time of a records request. The uncontroverted evidence before the circuit court was that the messages Sansone was seeking did not exist, and were not capable of being recovered, at the time of Sansone's request. The only admissible evidence in the summary judgment record was Mallery's expert testimony that a message sent using Confide is automatically deleted from the sender's phone after the sender opens a new message or after 48 hours, a message received using Confide is automatically deleted from the recipient's phone after the recipient reads it, and deleted messages are not recoverable using forensic methodology. Sansone had the opportunity to present testimony from his own expert to controvert Mallery's testimony, but he chose not to do so. Under the uncontroverted evidence, Sansone could not meet his initial burden of establishing that the Confide messages were public records

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

subject to disclosure under the Sunshine Law; therefore, the burden of persuasion to show that the messages were exempt from disclosure never shifted to the Governor's Office. The court properly applied the burden of persuasion with regard to Sansone's request for the Confide messages. [8] Point II is denied.

***25** In Points III, V, and VI, Sansone alleges the circuit court erred in granting summary judgment in favor of the Governor's Office on three counts in his second amended petition because the court misinterpreted Section 610.010(6)'s definition of a public record to require that the record must have been retained. Specifically, Sansone contends this "misinterpretation" of the definition of public record caused the court to erroneously grant summary judgment on his claim in Count VII that, in failing to produce a copy of all messages Greitens and the Governor's Office employees sent and received using Confide, the Governor's Office violated its duty under Section 610.023.2 to collect, maintain, and produce public records; his claim in Count V that the Governor's Office deliberately misapplied Section 610.021(21)'s "terrorism exception" and Section 610.021(18)'s "hacker exception" in refusing to produce records showing the date that Greitens and anyone employed in the Governor's Office downloaded any automatic message destruction software; and his claim in Count VIII that there was a civil conspiracy between all defendants to violate the Sunshine Law by using automatic message destruction software.

As we discussed *supra*, the uncontroverted evidence was that the Confide messages did not exist at the time of Sansone's request. Likewise, while Mallery testified that he might "possibly" or "potentially" be able to find records showing the date that someone downloaded Confide and that Confide performs as any other ephemeral messaging application, this was not sufficient to establish that such records existed for Confide or any other ephemeral messaging application that Sansone alleged the Governor's Office was using. Again, Sansone had the opportunity to obtain and present testimony from his own expert to controvert Mallery's testimony and raise a genuine issue of material fact on these issues, but he chose not to do so. Because the uncontroverted evidence was that these records did not exist and, therefore, were not public records subject to disclosure under the Sunshine Law, the court properly granted summary judgment in favor of the Governor's Office on Sansone's Counts VII, V, and VIII. Points III, V, and VI are denied.

In Point IV, Sansone contends the circuit court erred in granting summary judgment in favor of the Governor's Office on Count VI, which was his claim that the Governor's Office violated the Sunshine Law by failing to produce documents that showed Greitens's personal cell phone number. The Governor's Office answered Sansone's request for these records by asserting that the phone number was considered closed under Section 610.021(14), which allows public governmental bodies to close records that are "protected from disclosure by law." The Governor's Office then cited Section 407.1500, a provision in the Missouri Merchandising Practices Act, as the legal authority protecting Greitens's personal cell phone number from disclosure. In its summary judgment pleadings, the Governor's Office argued that Greitens's personal cell phone number was protected from disclosure under Section 407.1500.1(9)(b), because it was a "unique identification number ... collected by a government body."

In its amended judgment, the court found that Section 407.1500.1(9)(b) does not protect a personal cell phone number "from disclosure by law"; rather, it merely provides that a person who fails to give notice of the unauthorized disclosure of such information due to a security breach may be subject to an action for civil monetary penalties brought by the attorney general. After finding that the specific exception to disclosure cited by the Governor's ***26** Office did not apply, the court considered whether other any other exceptions applied. The court determined that Section 610.021(13), which provides that a public governmental body may close "[i]ndividually identifiable personnel records ... pertaining to employees," allowed the Governor's Office to close records of Greitens's personal cell phone number.

On appeal, Sansone first contends the circuit court erred in granting summary judgment on a basis not asserted by the Governor's Office in the summary judgment record. To support his argument, he relies on *Jones v. Housing Authority of Kansas City, Missouri*, 118 S.W.3d 669, 674 (Mo. App. 2003), and *Mothershead v. Greenbriar Country Club, Inc.*, 994 S.W.2d 80, 85 (Mo. App. 1999). *Jones* and *Mothershead* applied the principles that (1) the circuit court is confined to entering summary judgment only on the issues raised in the summary judgment motion, and (2) both the circuit court and this court are confined to considering only the factual record presented pursuant to Rule 74.04. *Jones*, 118 S.W.3d at 674 (finding the circuit court erred in ruling on the movant's right to attorney fees because it was not raised in the movant's summary judgment motion); *Mothershead*, 994 S.W.2d at 85

(stating that the circuit court's review and our review are limited to the evidence specified in the summary judgment motion and response).

The circuit court violated neither of these principles here. Whether the Governor's Office had the authority to close records of Greitens's personal cell phone number was the central issue in both parties' motions for summary judgment on Count VI, and in making its ruling, the court did not consider facts outside of the Rule 74.04 record. Rather, the court merely ruled that the Governor's Office's decision to close the records of Greitens's personal cell phone number was proper on a different legal basis than the Governor's Office asserted. Because we exercise *de novo* review, we may affirm it on that same basis or on any other legal basis we deem appropriate. *Ferbet v. Hidden Valley Golf & Ski, Inc.*, 618 S.W.3d 596, 603 (Mo. App. 2020). Indeed, we may affirm summary judgment "on an entirely different basis than that posited at trial." *ITT*, 854 S.W.2d at 387-88. *See also Ferbet*, 618 S.W.3d at 603 (affirming summary judgment on a legal basis neither asserted in the summary judgment motion nor relied on by the circuit court). Sansone's contention that granting summary judgment on a different legal basis than that asserted in the summary judgment record constitutes reversible error is without merit.

Sansone next argues the court misapplied Section 610.021(13) in finding that the section allowed the Governor's Office to close records of Greitens's personal cell phone number. Section 610.021(13) gives a public governmental body the discretionary authority to close records relating to "[i]ndividually identifiable personnel records, performance ratings or records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names, positions, salaries and lengths of service of officers and employees of public agencies once they are employed as such." This court recently explained that, in this section, the legislature has authorized public governmental bodies to choose to close individually identifiable personnel records except for employees' names, positions, salaries, and length of service "presumably in order to afford employees of public governmental bodies a modicum of privacy." *Show-Me Inst. v. Office of Admin.*, No. WD84561, ––– S.W.3d ––––, ––––, 2022 WL 904703 at *6 (Mo. App. Mar. 29, 2022) (citing ***27** *State ex rel. Delmar Gardens N. Operating, LLC v. Gaertner*, 239 S.W.3d 608, 611 (Mo. banc 2007), which we described as "acknowledging that 'Missouri recognizes a right of privacy in personnel records that should not be lightly disregarded or dismissed' " in determining the discoverability of such records).

"[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Riley v. California*, 573 U.S. 373, 395, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). Releasing an employee's personal cell phone number—particularly an employee as prominent as the State's Governor—renders the employee susceptible to being harassed, or having his or her cell phone account hacked, which could result in hackers gaining access to a trove of highly personal information and using this information for fraudulent and/or criminal purposes.[9] Therefore, we find that an employee's personal cell phone number is an individually identifiable personnel record that falls within the "modicum of privacy" afforded by Section 610.021(13).

Sansone's contention that *Guyer v. City of Kirkwood*, 38 S.W.3d 412 (Mo. banc 2001), held that Section 610.021(13)'s exception is limited to records relating to the "hiring, firing, or disciplining ... of a particular employee" is erroneous. In considering whether any of Section 610.021's exceptions to disclosure might apply, the Court in *Guyer* determined that, because internal police investigation reports related to the performance or merit of individual employees, they appeared to fall under both Section 610.021(3)'s exception for records relating to the "hiring, firing, disciplining, or promoting of particular employees," *and* Section 610.021(13)'s exception for "[i]ndividually identifiable personnel records, performance ratings or records pertaining to employees or applicants for employment." *Id.* at 414. The Court did not state that Section 610.021(13)'s exception for "individually identifiable personnel records" is limited to records described in Section 610.021(3)'s exception. Additionally, Sansone's reliance on *Oregon County R-IV School District v. LeMon*, 739 S.W.2d 553, 560 (Mo. App. 1987), a case that held that students' names, addresses, and telephone numbers were not protected from disclosure, is not persuasive, as that case does not appear to involve cell phone numbers.[10] Moreover, in a slightly more recent case than *LeMon*, this court stated that a public governmental agency *did* have the authority to close the telephone numbers of state employees to prevent the use of such information for nefarious purposes. In *Pulitzer Publishing Company v. Missouri State Employees' Retirement System*, 927 S.W.2d 477, 483 (Mo. App. 1996), we held that the name, position, pension amount, and length of service of members who

WESTLAW © 2023 Thomson Reuters. No claim to original U.S. Government Works.

had been or were receiving benefits were required to be disclosed per Section 610.021(13)'s exception to the exemption ***28** from disclosure, but the Missouri State Employees' Retirement System could still close "all other individually identifiable personnel information, including but not limited to, the addresses and telephone numbers of members, thereby minimizing the risk of exploitation of vulnerable, elderly retirees by unscrupulous elements who might request blanket information for inappropriate purposes."

Because Section 610.021(13) authorized the Governor's Office to close records of Greitens's personal cell phone number, the circuit court did not err in granting summary judgment in favor of the Governor's Office on Sansone's Count VI. [11] Point IV is denied.

In Point VII, Sansone contends the circuit court erred in granting summary judgment in favor of the Governor's Office on Count III, which was his claim that the Governor's Office's response to his records request violated Section 610.023.3. Section 610.023.3 provides, in pertinent part:

> Each request for access to a public record shall be acted upon as soon as possible, but in no event later than the end of the third business day following the date the request is received by the custodian of records of a public governmental body.... *If access to the public record is not granted immediately, the custodian shall give a detailed explanation of the cause for further delay* and the place and earliest time and date that the record will be available for inspection. This period for document production may exceed three days for reasonable cause.

(Emphasis added.) The Governor's Office responded to Sansone's December 20, 2017 request within three business days. In its response, the Governor's Office stated, "We are in the process of reviewing parts 1-5 of your request, and we anticipate that we will be able to provide a response or a time and cost estimate (if applicable) for records you have requested in no more than twenty business days. We will contact you at that time." Sansone argues this response was deficient because the Governor's Office failed to include a detailed and reasonable explanation for the delay.

The Governor's Office's stated reason for the delay was that it was "in the process of reviewing" all of Sansone's five requests for records. Ultimately, the only public record in existence that Sansone requested and did not receive access to within three business days was Greitens's personal cell phone number. The record indicates that Madden had never before received a Sunshine Law request for an employee's personal cell phone number, and she sent the request to the general counsel's office. Given that (1) this was the first time that Madden had received such a request, (2) the disclosure of a public governmental agency employee's personal cell phone number in response to a Sunshine Law request is an issue of first impression in Missouri, and (3) Sansone's requests were made right before the Christmas and New Year's holidays, when employees with information relevant to Sansone's requests ***29** may have been on vacation, that the Governor's Office needed more than three business days and up to twenty business days to review his requests was reasonable. The circuit court did not err in granting summary judgment in favor of the Governor's Office on Sansone's Count III. Point VII is denied.

In Point VIII, Sansone contends the circuit court erred in granting summary judgment in favor of the Governor's Office on his request in Count I for a preliminary and permanent injunction forbidding the Governor's Office from using Confide and similar ephemeral messaging applications. He argues that he was entitled to such relief under Chapters 610 and 109.

Sansone is correct that Section 610.027.1 authorizes private citizens to seek judicial enforcement of the Sunshine Law's provisions, and Section 610.030 authorizes the circuit court to issue injunctions to do so. As we have already noted, however, the Sunshine Law requires disclosure of only public records of which the governmental agency retains possession. The uncontroverted evidence was that messages sent via Confide and similar ephemeral messaging applications are not maintained, and, therefore, are not public records required to be disclosed under the Sunshine Law. Therefore, Sansone was not entitled to an injunction under Sections 610.027.1 and 610.030.

Sansone next argues that he was entitled to injunctive relief under Chapter 109. Unlike Chapter 610, Chapter 109

WESTLAW © 2023 Thomson Reuters. No claim to original U.S. Government Works.

contains no language authorizing private citizens to seek judicial enforcement of its provisions. Nevertheless, Sansone contends that he can seek injunctive relief to enforce Chapter 109 based on *Egan v. St. Anthony's Medical Center*, 244 S.W.3d 169, 173 (Mo. banc 2008). In *Egan*, the Supreme Court held that, while there is generally "no private right of action to enforce a statute or regulation," a surgeon could seek the "less intrusive remedy" of injunctive relief to compel a hospital to follow its own bylaws in the disciplinary proceeding against him because a regulation required the hospital to follow its bylaws in such proceedings. *Id.*

Sansone asserts that he is entitled "to seek injunctive relief to prevent the ongoing and unlawful destruction of public records." He does not state, however, which provision of Chapter 109 he is attempting to enforce by way of a private right of action for injunctive relief forbidding the Governor's Office from using Confide and similar ephemeral messaging applications. The only specific sections of Chapter 109 that Sansone mentions in this point are Section 109.120, which sets forth the standards and cost of records reproduced by photographic, video, or electronic process, and Section 109.180, which states that public records are open to inspection and provides for the impeachment of and criminal penalties for officials who refuse to permit inspection. Sansone cites these sections only to note that neither statute provides a private cause of action for damages, but then adds that "he could still seek injunctive relief under that section [sic]." He does not explain how the Governor's Office's use of Confide and similar ephemeral messaging applications violates either of these sections. [12]

"While de novo review of an appellate court is broad, such review is not a ***30** license for the reviewing court to become an advocate for the appellant by conducting its own research and crafting its own argument on behalf of the appellant." *DLJ Mortg. Cap., Inc. v. Creative Client Recovery, Inc.*, 637 S.W.3d 612, 619 (Mo. App. 2021). Because Sansone fails to support his contention that he is entitled to seek injunctive relief under Chapter 109 with relevant authority or argument beyond conclusory statements, we decline to consider the issue on appeal. *Martin v. Div. of Emp. Sec.*, 384 S.W.3d 378, 384 (Mo. App. 2012). Point VIII is denied.

In Point IX, Sansone contends the circuit court erred in staying discovery related to his Counts I, III, IV, VI, VII, and VIII. The circuit court has "broad discretion in administering rules of discovery," and we will not disturb its decision unless we find an abuse of discretion. *State ex rel. Delmar Gardens N. Operating, LLC*, 239 S.W.3d at 610. An abuse of discretion occurs only when a ruling "is clearly against the logic of the circumstances then before the court and is so arbitrary and unreasonable as to shock the sense of justice and indicate a lack of careful consideration." *Matysyuk v. Pantyukhin*, 595 S.W.3d 543, 547 (Mo. App. 2020) (quoting *Holm v. Wells Fargo Home Mortg., Inc.*, 514 S.W.3d 590, 596 (Mo. banc 2017)).

Rule 56.01(b)(1) prescribes the scope of discovery in general:

> Parties may obtain discovery regarding any matter, not privileged, that is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter, *provided the discovery is proportional to the needs of the case considering the totality of the circumstances, including but not limited to, the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expenses of the proposed discovery outweighs its likely benefit.*

(Emphasis added.)

In this case, the court decided that the threshold issue of whether the requested records were public records subject to disclosure under the Sunshine Law should be determined first, as it would have an effect on what discovery was probative to the claims Sansone raised in his second amended petition. The court accordingly ordered that discovery start with a forensic evaluation of the retention characteristics of the Confide application. The court ordered the Governor's Office

to obtain, at its cost, an expert forensic examination. The Governor's Office's expert, Mallery, opined that the records Sansone was seeking were not retainable. The court then afforded Sansone not only the opportunity to depose Mallery, which Sansone did, but also the opportunity to obtain his own expert forensic examination to controvert Mallery's opinions, which Sansone chose not to do.

Sansone's voluntary decision to forgo his opportunity for discovery on the threshold issue of whether the records he was requesting were maintained or recoverable by the Governor's Office rendered Mallery's opinion uncontroverted, leaving no genuine issue of material fact that, with the exception of Greitens's personal cell phone number, the records Sansone was ***31** seeking were not public records subject to disclosure under the Sunshine Law. Under the circumstances, the court's decision that no further discovery was necessary to resolve Sansone's claims in Count IV for failing to produce records showing the date that Greitens and anyone employed in the Governor's Office downloaded Confide on their cell phones, Count VII for failing to maintain and produce messages sent or received using Confide, and Count VIII for a civil conspiracy between all defendants to violate the Sunshine Law by using automatic message destruction software, does not shock our sense of justice or indicate a lack of careful consideration. Likewise, the court's decision to stay discovery on his claims in Count I for injunctive relief prohibiting the Governor and all Governor's Office employees from using Confide or any other automatic message destruction software, Count III for failing to provide a detailed and reasonable explanation of the cause of the delay in producing the records within three days, and Count VI for refusing to produce records showing Greitens's personal cell phone number, does not shock our sense of justice or indicate a lack of careful consideration. These claims were all resolved on legal grounds, and no evidence obtained through discovery would have had any effect on their resolution.

The circuit court did not abuse its discretion in staying further discovery on Counts IV, VII, and VIII and in staying discovery on Counts I, III, and VI. Point IX is denied.

CONCLUSION

The judgment is affirmed.

All Concur.

All Citations

648 S.W.3d 13

Footnotes

1 Eric Greitens was sworn in as the governor of Missouri on January 9, 2017, and was governor when the petition was filed in this case. He resigned on June 1, 2018. Then-Lieutenant Governor Michael Parson became governor for the remainder of the term under article IV, section 11(a) of the Missouri Constitution. In November 2020, Governor Parson was elected to a full term of office.

2 Section 610.010 *et seq.* All statutory references are to the Revised Statutes of Missouri 2016.

3 Sansone also requested a copy of the Governor's Office's document retention policy. In her initial response to Sansone's request, Madden provided website addresses for the Secretary of State's records retention schedules. Sansone did not assert any Sunshine Law violation claims based on Madden's response to this request, and it is not at issue in this appeal.

4 Additionally, Sansone's second amended petition alleged four counts of violations of the Open Records Law and State and Local Records Law in Chapter 109. The court granted the Governor's Office's motion to dismiss these counts, and Sansone does not appeal their dismissal.

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

5 There was conflicting evidence in the summary judgment record as to whether Greitens had a government-issued cell phone. There was no dispute between the parties that the number of a government-issued cell phone is an open record subject to disclosure. Sansone's Point IV, which concerns the failure to produce Greitens's cell phone number, challenges the court's decision that the Governor's Office had the authority to close Greitens's personal cell phone number.

6 Section 610.025 provides in full:

> Any member of a public governmental body who transmits any message relating to public business by electronic means shall also concurrently transmit that message to either the member's public office computer or the custodian of records in the same format. The provisions of this section shall only apply to messages sent to two or more members of that body so that, when counting the sender, a majority of the body's members are copied. Any such message received by the custodian or at the member's office computer shall be a public record subject to the exceptions of section 610.021.

7 It is not lost on this court that a public official's use of the Confide application has the practical effect of side-stepping the reach of Missouri's Sunshine Law via ephemeral messaging applications that delete communications before any request for their disclosure can be made. And, as Sansone's counsel noted at the oral argument of this case, it may be time to "update" Missouri's Sunshine Law that was originally enacted in 1973—well before cellular phone technology existed and, likewise, well before ephemeral messaging applications existed. But, it is not within the power of the judicial branch of government to "create" statutory law; that power is vested with the legislative branch of government. Unless and until the legislature "updates" Missouri's Sunshine Law to account for cellular phone technology and associated data, we cannot add words to the statute to accommodate Sansone's legitimate concerns about the use of ephemeral messaging applications by public officials. Nothing in this opinion should be interpreted to suggest that we condone the use of ephemeral messaging applications by public officials; but, the limitation on the Governor's Office's use of such messaging technology may be found in Chapter 109—not Chapter 610.

8 In this point, Sansone appears to challenge only the court's application of the burden of persuasion with regard to his claims concerning his request for the Confide messages, as those are the only records that he asserted were "destroyed." To the extent that he challenges the court's application of the burden of persuasion with regard to his request for Greitens's personal cell phone number, we note that the court found that the phone number was "without question" a public record of a public governmental body under Section 610.010(6). The burden of persuasion thus shifted to the Governor's Office, who asserted that the phone number was exempt from disclosure under Sections 610.021(4) and 407.1500. Although the court ultimately determined as a matter of law that the phone number was exempt from disclosure based on a different statutory section, *see* Point IV, *infra*, the record indicates that the court properly applied the burden of persuasion with regard to this claim.

9 *See, e.g.,* Brian X. Chen, *I Shared My Phone Number. I Learned I Shouldn't Have*, N.Y. TIMES (Aug. 15, 2019), https://www.nytimes.com/2019/08/15/technology/personaltech/i-shared-my-phone-number-i-learned-i-shouldnt-have.html; Henry Kenyon, *Cell Phone Account Fraud, A New Threat to Individuals' Private Data*, CQ ROLL CALL WASHINGTON DATA PRIVACY BRIEFING (Aug. 2, 2018).

10 Even if the phone numbers in *LeMon* were for mobile phones, the mobile phones at that time were not "smartphones" that allowed the user to do more than make and receive phone calls. *See* Steven Tweedie, *The World's First Smartphone, Simon, Was Created 15 Years Before the iPhone*, BUSINESS INSIDER, (June 14, 2015), https://www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6 (noting that "the first true smartphone" debuted in 1992).

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

11 Sansone also argues that the court erred deciding that the record was properly closed on a different basis than that asserted by the Governor's Office in its response to his request. We agree with the circuit court that, before it could decide whether the Governor's Office knowingly or purposely violated the Sunshine Law by failing to produce the record and was entitled to relief under Section 610.027, it had to first find that the Governor's Office wrongfully withheld the record. Even though the Governor's Office may have withheld the record for the wrong reason, it did not, as a matter of law, wrongfully withhold the record because it had the authority to do so under Section 610.010(13); therefore, Sansone is not entitled to relief under Section 610.027.

12 In his second amended petition, Sansone asserted that he was entitled to an injunction to enforce Section 109.270, which provides:

> All records made or received by or under the authority of or coming into the custody, control or possession of state or local officials in the course of their public duties are the property of the state or local government and shall not be mutilated, destroyed, transferred, removed or otherwise damaged or disposed of, in whole or in part, except as provided by law.

Sansone does not cite Section 109.270 or assert this argument on appeal; therefore, we consider it abandoned. *Geiler v. Liberty Ins. Corp.,* 621 S.W.3d 536, 548 (Mo. App. 2021).

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

183 Wash.2d 863
Supreme Court of Washington,
En Banc.

Glenda NISSEN, an individual, Respondent,
v.
PIERCE COUNTY, a public agency, Pierce County Prosecuting Attorney's Office, a public agency, and Prosecutor Mark Lindquist, Petitioners.

No. 90875–3.
|
Argued June 11, 2015.
|
Decided Aug. 27, 2015.

Synopsis
Background: Sheriff's detective brought action under Public Records Act (PRA) against county and county prosecutor's office, seeking disclosure of call logs from prosecutor's personal cellular telephone and text messages. The Superior Court, Thurston County, Christine A. Pomeroy, J., granted defendants' motion to dismiss. Defendant appealed. The Court of Appeals, 183 Wash.App. 581, 333 P.3d 577, reversed and remanded. Defendants filed petitions for review.

Holdings: The Supreme Court, en banc, Yu, J., held that:

record prepared, owned, used, or retained by agency employee in the scope of employment was "prepared, owned, used, or retained by a state or local agency," under PRA;

records an agency employee prepares, owns, uses, or retains on a private cellular telephone within the scope of employment can be a "public record";

call and text message logs prepared and retained by telephone company with respect to county employee's private cellular telephone were not "public records" of the county;

content of work-related text messages sent and received by county prosecutor were "public records," and

public employees are responsible for self-segregating private and public records contained on their private devices.

Affirmed and remanded with instructions.

Procedural Posture(s): On Appeal; Motion to Dismiss; Motion to Dismiss for Failure to State a Claim.

Attorneys and Law Firms

****48** Mark Evans Lindquist, Pierce County Prosc. Office, Daniel Ray Hamilton, Attorney at Law, Tacoma, WA, Philip Albert Talmadge, Talmadge/Fitzpatrick, Stewart Andrew Estes, Keating, Bucklin & McCormack, Inc., P.S., Seattle, WA, for Petitioners.

Michele Lynn Earl–Hubbard, Allied Law Group LLC, Seattle, WA, for Respondent.

****49** Anita Hunter, Washington Federation of State Employees, Olympia, WA, amicus counsel for Washington Federation of State Employees.

Martin S. Garfinkel, Schroeter Goldmark & Bender, Seattle, WA, amicus counsel for International Association of Fire Fighters.

Aimee Strand Iverson, WA Education Association, Federal Way, WA, amicus counsel for Washington Education Association.

Jeffrey Julius, Vick, Julius, McClure, P.S., Seattle, WA, amicus counsel for Washington Council of Police and Sheriffs.

Jeffrey Julius, Vick, Julius, McClure, P.S., Seattle, WA, amicus counsel for Washington State Patrol Troopers Association.

Scott R. Peters, Pierce County Prosecuting Attorney, Tacoma, WA, amicus counsel for Pierce County Prosecuting Attorneys Association.

Ramsey E. Ramerman, City of Everett, Everett, WA, amicus counsel for Washington State Association of Municipal Attorneys.

Peter B. Gonick, Callie Anne Castillo, WA State Attorney General Office, Olympia, WA, amicus counsel for Attorney General of Washington.

Judith A. Endejan, Garvey Schubert Barer, Seattle, WA, amicus counsel for Washington COAlition for Open Government.

William John Crittenden, Patrick Denis Brown, Attorney at Law, Seattle, WA, amicus counsel for League of Women Voters of Washington.

Nancy Lynn Talner, Douglas B. Klunder, Attorney at Law, Seattle, WA, amicus counsel for Aclu.

Pamela Beth Loginsky, Washington Assoc. of Prosecuting Atty., Olympia, WA, amicus counsel for Washington Association of Prosecuting Attorneys.

Opinion

YU, J.

***869** ¶ 1 Five years ago we concluded that the Public Records Act (PRA), chapter 42.56 RCW, applied to a record stored on a personal computer, recognizing that "[i]f government employees could circumvent the PRA by using their home computers for government business, the PRA could be drastically undermined." *O'Neill v. City of Shoreline,* 170 Wash.2d 138, 150, 240 P.3d 1149 (2010). Today we consider if the PRA similarly applies when a public employee uses a private cell phone to conduct government business. We hold that text messages sent and received by a public employee in the employee's official capacity are public records of the employer, even if the employee uses a private cell phone.

BACKGROUND

¶ 2 This case involves two requests for public records that Glenda Nissen, a sheriff's detective, sent to Pierce County (County). Both requests asked for records related to Pierce County Prosecutor Mark Lindquist. One request stated:

> Please produce any and all of Mark Lindquist's cellular telephone records for number 253–861–[XXXX [1]] or any other cellular telephone he uses to conduct his business including text messages from August 2, 2011.

Clerk's Papers (CP) at 15. The other stated:

> ***870** The new public records request is for Mark Lindquist's cellular telephone records for number 253–861–[XXXX] for June 7, [2010]. [2]

Id. at 17 (second alteration in original). The telephone number identified in these requests is connected to Lindquist's private cell phone. There is no dispute that Lindquist personally bought the phone, personally pays for its monthly service, and sometimes uses it in the course of his job.

¶ 3 In response to these requests, Lindquist obtained and provided the County with two types of records. The first, which the parties refer to as the "call log," is similar to an itemized statement customers might receive from their service provider each month. ****50** It contains information about the dates and times of calls made and received, the length of those calls, and the phone number of the incoming or outgoing call. Lindquist's service provider, Verizon Wireless, generated the call log and provided it to Lindquist at his request. He voluntarily produced it to the County.

¶ 4 The second type of record reveals information about text messages Lindquist sent and received over two days ("text message log"). The text message log does not reveal the content of those messages. Instead, similar to the call log, it itemizes the date and time of each message and provides the telephone number of the corresponding party. Lindquist also obtained the text message log from Verizon after receiving Nissen's PRA requests and produced it to the County.

¶ 5 The County reviewed the call and text message logs and disclosed partially redacted copies to Nissen. Accompanied by an exemption log, the redactions conceal line items for calls and text messages that Lindquist self-described as personal in nature. The remaining unredacted portions relate to calls and text messages that the County and ***871** Lindquist admit might be work related. *See* CP at 490 (Decl. of Mark Lindquist in Supp. of Mot. To Intervene & Join) ("I authorized the release of records of calls that were related to the conduct of government or the performance of any governmental or proprietary function."); Pierce County's Pet. for Review at 3 ("[T]he Prosecutor authorized the release of records of calls that 'may be work related.' "); Lindquist's Pet. for Review at 10 ("[T]he Petitioner provided those communications that may be 'work related.' "). Thus nearly half of the text messages Lindquist sent or received and many of his phone calls during the relevant period potentially related to his job as the elected prosecutor. The County did not

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

produce the contents of any text message, however, though copies of them exist on Verizon's servers. [3]

¶ 6 Dissatisfied with the County's disclosures, Nissen sued the County in Thurston County Superior Court. She sought an in camera review of Lindquist's text messages and the call and text message logs to determine if all of the information is a public record. Lindquist intervened and moved for a temporary restraining order and preliminary injunction to enjoin further disclosure of records related to his cell phone. He argued that compelling him to disclose his text messages would violate the state and federal constitutions and was prohibited by state and federal statutes. CP at 502–18. That same day the County moved to dismiss Nissen's complaint under CR 12(b)(6). It argued the records at issue could not be public records as a matter of law, because they related to a personal cell phone rather than a county-issued one.

¶ 7 The trial court consolidated the two motions for a hearing. After argument, the trial judge granted the County's CR 12(b)(6) motion, determining as a matter of law that records of private cell phone use can never be public records ***872** under the PRA. The Court of Appeals reversed. *Nissen v. Pierce County,* 183 Wash.App. 581, 333 P.3d 577 (2014). Applying the PRA's definition of "public record," the Court of Appeals held that Lindquist's text messages were public records because he "prepared" them in his official capacity. *Id.* at 593–94, 333 P.3d 577 (citing RCW 42.56.010(3)). The court further held that the factual record was not sufficiently developed on the issue of whether the call logs also qualify as "public record[s]," noting that the issue turned on whether Lindquist used or retained the logs in his capacity as prosecuting attorney. *Id.* at 595, 333 P.3d 577.

¶ 8 We granted the County's and Lindquist's petitions for review, *Nissen v. Pierce County,* 182 Wash.2d 1008, 343 P.3d 759 (2015), and now affirm in part and remand with further instructions.

****51** STANDARD OF REVIEW

¶ 9 We review de novo a CR 12(b)(6) order dismissing a complaint. Dismissal is proper only if we conclude that "the plaintiff cannot prove 'any set of facts which would justify recovery.' " *Kinney v. Cook,* 159 Wash.2d 837, 842, 154 P.3d 206 (2007) (quoting *Tenore v. AT & T Wireless Servs.,* 136 Wash.2d 322, 330, 962 P.2d 104 (1998)). Motions to dismiss are granted "only in the unusual case in which plaintiff includes allegations that show on the face of the complaint that there is some insuperable bar to relief." *Hoffer v. State,* 110 Wash.2d 415, 420, 755 P.2d 781 (1988) (quoting 5 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE § 357, at 604 (1969)).

¶ 10 Our standard of review in PRA cases is also de novo. *Neigh. All. of Spokane County v. Spokane County,* 172 Wash.2d 702, 715, 261 P.3d 119 (2011).

ANALYSIS

¶ 11 Before turning to the questions this case presents, it is helpful to clarify the questions it does not. This case does ***873** not involve a public employer seizing an employee's private cell phone to search for public records. It does not involve a records request for every piece of data on a smartphone. And it does not involve a citizen suing a public employee for access to the employee's phone. Instead, this is an action against an agency for two types of records that, while potentially related to the agency's public business, are in the exclusive control of the agency's employee. This case asks whether those records can nonetheless be "public records" the agency must disclose and, if so, whether there are limits to how the agency may search for and review those records.

¶ 12 With that in mind, we first interpret the PRA to determine if a record of government business conducted on a private cell phone is a "public record," as the PRA defines the term. We then apply that definition to the specific records here—the call and text message logs and text messages. Finally, we address the mechanics of searching for and obtaining public records held by or in the control of public employees. As explained below, we hold that text messages sent or received by Lindquist in his official capacity can be public records of the County, regardless of the public or private nature of the device used to create them; and we order Lindquist to obtain, segregate, and produce those public records to the County.

I. THE PRA REACHES EMPLOYEE–OWNED CELL PHONES WHEN USED FOR AGENCY BUSINESS

¶ 13 Our analysis begins with the text of the PRA. By its plain language, the PRA applies "when an 'agency' is requested to disclose 'public records.' " *Dawson v. Daly,* 120 Wash.2d 782, 788, 845 P.2d 995 (1993). Because those are both defined terms, we must interpret the statutory definitions to decide

WESTLAW © 2023 Thomson Reuters. No claim to original U.S. Government Works.

if records of public business an employee conducts on his or her private cell phone are public records. ***874** *Senate Republican Campaign Comm. v. Pub. Disclosure Comm'n,* 133 Wash.2d 229, 239, 943 P.2d 1358 (1997). The PRA defines "agency" very broadly as

> all state agencies and all local agencies. "State agency" includes every state office, department, division, bureau, board, commission, or other state agency. "Local agency" includes every county, city, town, municipal corporation, quasi-municipal corporation, or special purpose district, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency.

RCW 42.56.010(1). This definition in turn affects what information is a "public record" since it is incorporated into the statutory definition of that term. Under the PRA, a "public record" is

> any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function *prepared, owned, used, or retained by any state or local agency* regardless of physical form or characteristics.

RCW 42.56.010(3) (emphasis added).

¶ 14 The definitions of "agency" and "public record" are each comprehensive ****52** on their own and, when taken together, mean the PRA subjects "virtually any record related to the conduct of government" to public disclosure.[4] *O'Neill,* 170 Wash.2d at 147, 240 P.3d 1149. This broad construction is deliberate and meant to give the public access to information about every aspect of state and local government. *See* LAWS OF 1973, ch. 1, § 1(11). As we so often summarize, the PRA "is a strongly worded mandate for broad disclosure of public records." *Yakima County v. Yakima Herald–Republic,* 170 Wash.2d 775, 791, 246 P.3d 768 (2011) (quoting *Soter v. Cowles Publ'g Co.,* 162 Wash.2d 716, 731, 174 P.3d 60 (2007) (quoting *Hearst Corp. v. Hoppe,* 90 Wash.2d 123, 127, 580 P.2d 246 (1978))).

***875** A. Agency Employees Working within the Scope of Employment Create Public Records

¶ 15 Despite that mandate, the County argues public employees can avoid the PRA simply by using a private cell phone, even if they use it for public business and even if the same information would be a public record had they used a government-issued phone instead.[5] The County finds this large gap in the PRA by isolating the statute's definition of "agency," which does not expressly refer to individual employees as agencies. RCW 42.56.010(1). Since county employees like Lindquist are not literally a "county," the County argues its employees and the records they control are completely removed from the PRA's scope.

¶ 16 While that reasoning may have superficial appeal, it misses the central question here. We cannot interpret statutory terms oblivious to the context in which they are used. *Dep't of Ecology v. Campbell & Gwinn, LLC,* 146 Wash.2d 1, 10–11, 43 P.3d 4 (2002). As this case does not ask if a public employee is an "agency" with independent obligations separate from those the PRA imposes on the employer, interpreting "agency" in isolation is unhelpful. Nissen's request was directed at the County, not Lindquist.[6] Our task instead is to decide if *records* that a public employee generates while working for an agency are "public records" that the agency must disclose. Thus we must ***876** interpret the statutory definitions of "agency" and "public record" together, keeping in mind the purpose those definitions are intended to further. *See Hearst Corp.,* 90 Wash.2d at 128, 580 P.2d 246.

¶ 17 One characteristic of a public record is that it is "prepared, owned, used, or retained by any state or local agency." RCW 42.56.010(3). The County is correct that every agency the PRA identifies is a political body arising under law (e.g., a county). But those bodies lack an innate ability to prepare, own, use, or retain any record. They instead act exclusively through their employees and other agents, and when an employee acts within the scope of his or her employment, the employee's actions are tantamount to "the actions of the [body] itself." *Houser v. City of Redmond,* 91 Wash.2d 36, 40, 586 P.2d 482 (1978) (as to cities); *Hailey v.*

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

King County, 21 Wash.2d 53, 58, 149 P.2d 823 (1944) (as to counties). Integrating this basic common law concept into the PRA, a record that an agency employee prepares, owns, uses, or retains in the scope of employment is necessarily a record "prepared, ****53** owned, used, or retained by [a] state or local agency." RCW 42.56.010(3).

¶ 18 That interpretation is the only logical one considering how agencies conduct business and carry out their obligations under the PRA. *See Dawson,* 120 Wash.2d at 789, 845 P.2d 995 (public records were "prepared by the prosecutor's office" because two employees created and compiled them). If the PRA did not capture records individual employees prepare, own, use, or retain in the course of their jobs, the public would be without information about much of the daily operation of government. Such a result would be an affront to the core policy underpinning the PRA—the public's right to a transparent government. That policy, itself embodied in the statutory text, guides our interpretation of the PRA. RCW 42.56.030; LAWS OF 1973, ch. 1, § 1(11); *Hearst Corp.,* 90 Wash.2d at 128, 580 P.2d 246.

***877** B. The PRA Captures Work Product on Employee Cell Phones

¶ 19 With that understanding, it is clear that an agency's "public records" include the work product of its employees. And we find nothing in the text or purpose of the PRA supporting the County's suggestion that only work product made using agency property can be a public record. To the contrary, the PRA is explicit that information qualifies as a public record "regardless of [its] physical form or characteristics." RCW 42.56.010(3). In *O'Neill* we held that a city official stored a public record on a private computer in her home by using the computer for city business, 170 Wash.2d at 150, 240 P.3d 1149, which is consistent with the idea that employees can use their own property and still be within the scope of their employment. *Dickinson v. Edwards,* 105 Wash.2d 457, 467–68, 716 P.2d 814 (1986). There is no reason to treat cell phones differently. We hold that records an agency employee prepares, owns, uses, or retains on a private cell phone within the scope of employment can be a public record if they also meet the other requirements of RCW 42.56.010(3).

¶ 20 Applying the PRA to employee cell phone use is not new. Though an issue of first impression in this court, many state and local agencies implementing the PRA already conclude that using a private cell phone to conduct public business can create a public record. Over the last several years, agencies have begun adopting policies about private cell phone use and advising employees of the agencies' obligation to preserve all public records. Just as examples:

- "Employees utilizing cell phones for City business must not utilize written cell phone capabilities such as text messaging or email for City business unless such phone is synchronized with the City's computer system so that such electronic records can be maintained according to the State records retention requirements." ***878** CITY OF PROSSER, PERSONNEL POLICY MANUAL 32 (2009) (Policy 403: Cell Phone Allowance).

- "All county business generated on personal mobile devices are subject to the Public Records Act.... Text messages sent and received on a personal mobile device are not stored in any other form. Employees shall not use texting for any County business." THURSTON COUNTY ADMINISTRATIVE MANUAL (2012) § 10 (Personal Mobile Device Policy).

- "Employees should be aware that work-related texts and voice messages on cell phones are public records subject to the Public Records Act. Employees have a duty to maintain such records in accordance with the Washington Local Government Record Retention Schedules." CITY OF GRANDVIEW, PERSONNEL POLICY MANUAL 88 (2013) (use of personal cellular telephones to conduct city business), http://www.grandview.wa.us/wp-content/uploads/2013/03/Personnel–Policy–Manual1.pdf.

These policies are comparable to many others around the state and are consistent with the attorney general's understanding of the PRA. *See* WAC 44–14–03001(3). While these interpretations do not bind us, *O'Neill,* 170 Wash.2d at 149, 240 P.3d 1149, they discredit the County's assertion that private cell phone use has always been treated as outside the PRA.

****54** ¶ 21 Similarly unpersuasive is the County's warning that every "work-related" personal communication is now a public record subject to disclosure. Traditional notions of principal-agency law alleviate this concern. For information to be a public record, an employee must prepare, own, use, or retain it *within the scope of employment.* An employee's communication is "within the scope of employment" only when the job requires it, the employer directs it, or it furthers

the employer's interests. *Greene v. St. Paul–Mercury Indem. Co.,* 51 Wash.2d 569, 573, 320 P.2d 311 (1958) (citing *Lunz v. Dep't of Labor & Indus.,* 50 Wash.2d 273, 310 P.2d 880 (1957); ***879** *Roletto v. Dep't Stores Garage Co.,* 30 Wash.2d 439, 191 P.2d 875 (1948)). This limits the reach of the PRA to records related to the employee's public responsibilities. For instance, employees do not generally act within the scope of employment when they text their spouse about working late or discuss their job on social media. Nor do they typically act within the scope of employment by creating or keeping records purely for private use, like a diary. None of these examples would result in a public record "prepared, owned, used, or retained" by the employer agency in the usual case. [7]

¶ 22 Agencies can act only through their employee-agents. With respect to an agency's obligations under the PRA, the acts of an employee in the scope of employment are necessarily acts of the "state and local agenc[ies]" under RCW 42.56.010(3). We therefore reject the County's argument that records related to an employee's private cell phone can never be public records as a matter of law. Instead, records an employee prepares, owns, uses, or retains within the scope of employment are public records if they meet all the requirements of RCW 42.56.010(3). This inquiry is always case- and record-specific. *Cf. Predisik v. Spokane Sch. Dist. No. 81,* 182 Wash.2d 896, 906, 346 P.3d 737 (2015).

II. APPLYING THE PRA TO THE CALL AND TEXT MESSAGE LOGS AND TEXT MESSAGES

¶ 23 We next apply RCW 42.56.010(3) to the records at issue here—the call and text message logs and text messages. To be a public record under RCW 42.56.010(3), information must be (1) a writing (2) related to the conduct of government or the performance of government functions that is (3) prepared, owned, used, or retained by a state or local agency. *Confederated Tribes of the Chehalis Reservation* ***880** *v. Johnson,* 135 Wash.2d 734, 746, 958 P.2d 260 (1998). The first element is not in dispute—the parties agree that the call and text message logs and text messages are "writings" under the PRA. *See* RCW 42.56.010(4). The remaining two elements are discussed in turn.

A. Records Relating to the Conduct of Government

¶ 24 Public records must "relat[e] to the conduct of government or the performance of any governmental or proprietary function." RCW 42.56.010(3). This language casts a wide net. In *Confederated Tribes,* for example, we held that records of money paid by Indian tribes into a common fund related to the conduct of the government even though the records related primarily to tribal gaming operations. 135 Wash.2d at 739–43, 958 P.2d 260. Since the state received money from the common fund, we determined tribal contributions impacted state government and therefore records of those contributions were public records. *Id.* at 748, 958 P.2d 260.

¶ 25 We adopted a similarly broad interpretation in *Oliver v. Harborview Med. Ctr.,* 94 Wash.2d 559, 618 P.2d 76 (1980), which involved medical records of patients hospitalized at a state-owned facility. The records there unquestionably related to individual patients and did not explicitly discuss government operations, but we still held that the records "relat[ed] to the conduct of government" under RCW 42.56.010(3). From them the public could learn about the "administration ****55** of health care services, facility availability, use and care, methods of diagnosis, analysis, treatment and costs, all of which are carried out or relate to the performance of a governmental or proprietary function." *Oliver,* 94 Wash.2d at 566, 618 P.2d 76.

¶ 26 Together these cases suggest records can qualify as public records if they contain any information ***881** that refers to or impacts the actions, processes, and functions of government. [8]

B. Records Prepared, Owned, Used, or Retained by an Agency

¶ 27 As explained previously, a public record must also be "prepared, owned, used, or retained" by an agency, which includes an agency employee acting within the scope of employment. But the parties still quarrel over the meaning of these verbs, which requires that we further interpret RCW 42.56.010(3). Statutory interpretation starts with the plain meaning of the language; the plain meaning controls if it is unambiguous. *Campbell,* 146 Wash.2d at 11–12, 43 P.3d 4. We may use a dictionary to discern the plain meaning of an undefined statutory term. *HomeStreet, Inc. v. Dep't of Revenue,* 166 Wash.2d 444, 451, 210 P.3d 297 (2009) (citing *Garrison v. Wash. State Nursing Bd.,* 87 Wash.2d 195, 196, 550 P.2d 7 (1976)).

¶ 28 "*Prepared.*" "Prepare" is defined as "to put together"; to "MAKE, PRODUCE"; "to put into written form." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1790 (2002). This interpretation is consistent with previous cases that treat "preparing" a record as creating it. *See Dawson,* 120 Wash.2d at 787, 845 P.2d 995 (agency prepared record by "creat[ing] one of the files"); *Oliver,* 94 Wash.2d at 566, 618 P.2d 76 (records of patient's hospitalization prepared by the hospital).

¶ 29 "*Owned.*" To "own" a record means "to have or hold [it] as property." WEBSTER'S, *supra,* at 1612; *see also O'Neill v. City of Shoreline,* 145 Wash.App. 913, 925, 187 P.3d 822 (2008).

¶ 30 "*Used.*" We previously addressed what it means for an agency to "use" a record. We broadly interpreted the term in *Concerned Ratepayers Ass'n v. Pub. Util. Dist. No. 1 of* ***882** *Clark County,* 138 Wash.2d 950, 960, 983 P.2d 635 (1999), holding that the "critical inquiry is whether the requested information bears a nexus with the agency's decision-making process." A record that is prepared and held by a third party, without more, is not a public record. But if an agency "evaluat[es], review[s], or refer[s]" to a record in the course of its business, the agency "uses" the record within the meaning of the PRA. *Id.* at 962, 983 P.2d 635.

¶ 31 "*Retained.*" To "retain" a record means "to hold or continue to hold [it] in possession or use." WEBSTER'S, *supra,* at 1938.

C. The Text Messages Are Potentially Public Records; the Call and Text Message Logs Are Not

¶ 32 We now apply those definitions to decide if the complaint sufficiently alleges that the call logs and text messages are "public records." Absent an allegation that the County used the call and text message logs, the logs in this case are not public records. The call and text message logs were prepared and retained by Verizon, and Nissen does not contend that the County evaluated, reviewed, or took any other action with the logs necessary to "use" them. *Concerned Ratepayers,* 138 Wash.2d at 962, 983 P.2d 635. Though they evidence the acts of a public employee, the call and text message logs played no role in County business as records themselves. We hold that the complaint fails to allege the call and text message logs are "public records" of the County within the meaning of RCW 42.56.010(3) because the County did nothing with them.

¶ 33 We reach a different conclusion as to text messages. Nissen sufficiently alleges that Lindquist sent and received text messages in his official capacity "to take actions retaliating against her and other official misconduct." CP at 14. When acting ****56** within the scope of his employment, Lindquist prepares outgoing text messages by "putting them into written form" and sending them. Similarly, he ***883** "used" incoming text messages when he reviewed and replied to them while within the scope of employment. Since the County and Lindquist admit that some text messages might be "work related," the complaint sufficiently alleges that those messages meet all three elements of a "public record" under RCW 42.56.010(3).

¶ 34 Transcripts of the content of those text messages are thus potentially public records subject to disclosure, consistent with the procedure discussed below.

III. SEARCHING FOR PUBLIC RECORDS WITHIN AN EMPLOYEE'S CONTROL

¶ 35 We finally turn to the mechanics of searching for and obtaining public records stored by or in the control of an employee. The County and Lindquist suggest that various provisions of the state and federal constitutions categorically prohibit a public employer from obtaining public records related to private cell phone use without consent.[9] Because an individual has no constitutional privacy interest in a *public* record,[10] Lindquist's challenge is necessarily grounded in the constitutional rights he has in personal information comingled with those public records. We are mindful that today's mobile devices often contain "a 'wealth of detail about [a person's] familial, political, professional, religious, and sexual associations.' " *State v. Hinton,* 179 Wash.2d 862, 869, 319 P.3d 9 (2014) (alteration in original) (quoting *United States v. Jones,* 565 U.S. ——, 132 S.Ct. 945, 955, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring)). As nearly two-thirds of Americans can now communicate, access the Internet, store documents, and manage appointments on their smartphone, cell phones ***884** are fast becoming an indispensable fixture in people's private and professional lives. Text messaging is the most widely used smartphone feature; e-mail is not far behind. Aaron Smith, *U.S. Smartphone Use in 2015,* PEW RESEARCH CTR.

(Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us–smartphone–use–in–2015.

¶ 36 Yet the ability of public employees to use cell phones to conduct public business by creating and exchanging public records—text messages, e-mails, or anything else—is why the PRA must offer the public a way to obtain those records. Without one, the PRA cannot fulfill the people's mandate to have "full access to information concerning the conduct of government on every level." LAWS OF 1973, ch. 1, § 1(11). As noted earlier, many counties, cities, and agencies around the state recognize the need to capture and retain public records created on personal devices. Some of those entities provide employees with a way to preserve public records and avoid any inquiry into their private affairs by, for example, syncing work-related documents, e-mails, and text messages to an agency server or other place accessible to the employer. The County apparently has no such policy.

¶ 37 While a policy easing the burden on employees of preserving public records is certainly helpful, it cannot be a precondition to the public's right to access those records. If it were, the effectiveness of the PRA would hinge on "the whim of the public officials whose activities it is designed to regulate." *Mead Sch. Dist. No. 354 v. Mead Educ. Ass'n,* 85 Wash.2d 140, 145, 530 P.2d 302 (1975). The legislature tasks us with interpreting the PRA liberally and in light of the people's insistence that they have information about the workings of the government they created. RCW 42.56.030. Of course, the public's statutory right to public records does not extinguish an individual's constitutional rights in private information. But we do not read the PRA as a zero-sum choice between personal liberty and government accountability. Instead, we turn to well-settled principles of public disclosure ****57** law and hold that an employee's ***885** good-faith search for public records on his or her personal device can satisfy an agency's obligations under the PRA.

¶ 38 Though technology evolves, segregating public records from nonpublic ones is nothing new for agencies responding to a PRA request. Whether stored in a file cabinet or a cell phone, the PRA has never authorized "unbridled searches" of every piece of information held by an agency or its employees to find records the citizen believes are responsive to a request. *Hangartner v. City of Seattle,* 151 Wash.2d 439, 448, 90 P.3d 26 (2004). The onus is instead on the agency—necessarily through its employees—to perform "an adequate search" for the records requested. *Neigh. All.,* 172 Wash.2d at 720–21, 261 P.3d 119. To satisfy the agency's burden to show it conducted an adequate search for records, we permit employees in good faith to submit "reasonably detailed, nonconclusory affidavits" attesting to the nature and extent of their search. *Id.* at 721, 261 P.3d 119. The PRA allows a trial court to resolve disputes about the nature of a record "based solely on affidavits," RCW 42.56.550(3), without an in camera review, without searching for records itself, and without infringing on an individual's constitutional privacy interest in private information he or she keeps at work.

¶ 39 Federal courts implementing the Freedom of Information Act (FOIA), Pub. L. No. 89–487, 80 Stat. 250, allow individual employees to use the same method to self-segregate private and public records. *See, e.g., Media Research Ctr. v. U.S. Dep't of Justice,* 818 F.Supp.2d 131, 139–40 (D.D.C.2011) (declarations sufficient to determine e-mails were not sent in employee's official capacity); *Consumer Fed'n of Am., v. Dep't of Agric.,* 455 F.3d 283, 288–89 (D.C.Cir.2006) (affidavits from employees about character of electronic calendars); *Bloomberg, LP v. U.S. Sec. & Exch. Comm'n,* 357 F.Supp.2d 156, 163 (D.D.C.2004) (affidavits about "telephone logs" and message slips); ***886** *Judicial Watch, Inc. v. Clinton,* 880 F.Supp. 1, 11–12 (D.D.C. 1995); *Gallant v. Nat'l Labor Relations Bd.,* 26 F.3d 168, 171 (D.C.Cir.1994). While "[a]n agency cannot require an employee to produce and submit for review a purely personal document when responding to a FOIA request[,] ... it does control the employee to the extent that the employee works for the agency on agency matters." *Ethyl Corp. v. U.S. Envt'l Prot. Agency,* 25 F.3d 1241, 1247 (4th Cir.1994). Thus, where a federal employee asserts a potentially responsive record is personal, he or she must provide the employer and "the courts with the opportunity to evaluate the facts and reach their own conclusions" about whether the record is subject to FOIA. *Grand Cent. P'ship, Inc. v. Cuomo,* 166 F.3d 473, 480–81 (2d Cir.1999). We already incorporate FOIA's standard for adequate searches into the PRA, *Neigh. All.,* 172 Wash.2d at 720, 261 P.3d 119, and we similarly adopt FOIA's affidavit procedure for an employee's personally held public records.

¶ 40 Therefore, we hold agency employees are responsible for searching their files, devices, and accounts for records responsive to a relevant PRA request. Employees must produce any public records (e-mails, text messages, and any other type of data) to the employer agency. The agency then proceeds just as it would when responding to a request for public records in the agency's possession by reviewing each record, determining if some or all of the record is exempted from production, and disclosing the record to the requester.

See generally *Resident Action Council v. Seattle Hous. Auth.,* 177 Wash.2d 417, 436–37, 327 P.3d 600 (2013).

¶ 41 Where an employee withholds personal records from the employer, he or she must submit an affidavit with facts sufficient to show the information is not a "public record" under the PRA. So long as the affidavits give the requester and the trial court a sufficient factual basis to determine that withheld material is indeed nonresponsive, the agency has performed an adequate search under the PRA. When done in good faith, this procedure allows an ***887** agency to fulfill its responsibility to search for and disclose public records without unnecessarily treading on the constitutional rights of its employees.

****58** ¶ 42 We recognize this procedure might be criticized as too easily abused or too deferential to employees' judgment. Certainly the same can be said of any search for public records, not just for records related to employee cell phone use. But we offer two specific responses. First, an employee's judgment would often be required to help identify public records on a cell phone, even in an in camera review. Text messages, for example, are short communications whose meaning may not be self-apparent. Unlike a chain of e-mails where the preceding messages are often replicated in the body of each new reply, text messages may contain only a few words. The employee then might be needed to put that message into context to determine if it meets the statutory definition of a "public record."

¶ 43 Second, those criticisms spotlight why agencies should develop ways to capture public records related to employee cell phone use. The people enacted the PRA "mindful of the right of individuals to privacy," LAWS OF 1973, ch. 1, § 1(11), and individuals do not sacrifice all constitutional protection by accepting public employment. *City of Ontario v. Quon,* 560 U.S. 746, 756, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). Agencies are in the best position to implement policies that fulfill their obligations under the PRA yet also preserve the privacy rights of their employees. E-mails can be routed through agency servers, documents can be cached to agency-controlled cloud services, and instant messaging apps can store conversations. Agencies could provide employees with an agency-issued device that the agency retains a right to access, or they could prohibit the use of personal devices altogether. That these may be more effective ways to address employee cell phone use, however, does not diminish the PRA's directive that we liberally construe it here to promote access to all public records. RCW 42.56.010(3).

***888** CONCLUSION

¶ 44 We affirm the Court of Appeals in part. Records that an agency employee prepares, owns, uses, or retains on a private cell phone within the scope of employment can be "public records" of the agency under RCW 42.56.010(3). Nissen's complaint thus sufficiently alleges that at least some of the text messages at issue may be public records subject to disclosure. Because it is impossible at this stage to determine if any messages are in fact public records, on remand the parties are directed as follows. Lindquist must obtain a transcript of the content of all the text messages at issue, review them, and produce to the County any that are public records consistent with our opinion. The County must then review those messages—just as it would any other public record—and apply any applicable exemptions, redact information if necessary, and produce the records and any exemption log to Nissen. As to text messages that Lindquist in good faith determines are not public records, he must submit an affidavit to the County attesting to the personal character of those messages. The County must also produce that affidavit to Nissen.

¶ 45 We note that the County responded to Nissen's records requests and produced records in a timely manner based on what we presume was its good-faith interpretation of the PRA. Though we now hold that interpretation is incorrect, penalties are not warranted at this early stage before the County has had the opportunity to comply with our opinion and supplement its response to Nissen's requests accordingly. We reserve for the trial court the issue of penalties going forward.

MADSEN, C.J., and JOHNSON, OWENS, FAIRHURST, STEPHENS, WIGGINS, GONZÁLEZ, and MCCLOUD, JJ., concur.

All Citations

183 Wash.2d 863, 357 P.3d 45, 43 Media L. Rep. 3150

 © 2023 Thomson Reuters. No claim to original U.S. Government Works.

Footnotes

1 Though redacted in the record before us, the requests contained the full 10–digit telephone number.

2 The County has not challenged the breadth or specificity of these requests, and we pass no opinion.

3 The messages apparently no longer exist on Lindquist's phone. In conjunction with her PRA requests, however, Nissen's lawyer contacted Verizon and asked it to preserve all "communications and data [on Lindquist's account] ... pending the issuance of a subpoena or other legal process." CP at 200. The propriety of that request is not before us.

4 Disclosing that a public record exists in response to a request does not mean the record will ultimately be produced. Agencies must consider whether any applicable exemption precludes production of part or all of a record. *Sanders v. State,* 169 Wash.2d 827, 836, 240 P.3d 120 (2010).

5 The County admits that this is the natural result of its interpretation of the PRA. Wash. Supreme Court oral argument, *Nissen v. Pierce County,* No. 90875–3 (June 11, 2015), at 3 min., 4 sec., and 6 min., 57 sec., *audio recording by* TVW, Washington State's Public Affairs Network, http://www.tvw.org.

6 Whether an elected official is independently subject to the PRA is an unsettled question. *See Bldg. Indus. Ass'n of Wash. v. McCarthy,* 152 Wash.App. 720, 746, 218 P.3d 196 (2009). Here, however, Nissen did not sue Lindquist, either in his individual or official capacity. She instead sued the County, alleging that Lindquist's use of his cell phone resulted in public records of the County; Lindquist is a party only because he intervened to enjoin disclosure. The relevant question then is not whether Lindquist is individually subject to the PRA but, rather, whether records he handles in his capacity as the prosecutor are county public records.

7 We offer these generic illustrations in response to hypotheticals raised by the County and some amici. Of course, the facts of every case vary. We do not intend these illustrations to have precedential effect.

8 It is worth repeating that records an employee maintains in a personal capacity will not qualify as public records, even if they refer to, comment on, or mention the employee's public duties.

9 They primarily cite to the Fourth Amendment to the United States Constitution and article I, section 7 of the Washington Constitution.

10 *See Nixon v. Adm'r of Gen. Servs.,* 433 U.S. 425, 457, 97 S.Ct. 2777, 53 L.Ed.2d 867 (1977) (noting public officials have "constitutionally protected privacy rights in matters of personal life *unrelated to any acts done by them in their public capacity* " (emphasis added)).

End of Document © 2023 Thomson Reuters. No claim to original U.S. Government Works.

2018

Missouri Secretary of State Records Services Division Electronic Communications Records Guidelines for Missouri Government

FOR STATE AND LOCAL GOVERNMENT

Updated May 14, 2019

Approved by:

Local Records Board **August 21, 2018**

State Records Commission **May 13, 2019**

Purpose and Overview

These guidelines will assist state and local government agencies in developing policies to manage communications, regardless of format (memos, text messages, emails, or any format devised in the future). These communications, or messages, have always been records. The retention period of a given record is based on its on content and function. For hard copy communications, such as written memoranda and letters, the agency of origin maintains these through filing. With files maintained only electronically (for instance, email) the agency manages the server storage of these records. For non-government controlled formats (examples include: text messages and social media) the service provider is not responsible for maintaining the records; it is the responsibility of the agency that owns the phone, device or account, to maintain that record for its retention period. Private phones, email accounts and computers, that are used to send, receive, or otherwise handle public, or official, business are also subject to records retention requirements. It is the responsibility of the account owner to preserve and maintain these records.

Scope

The following guidelines are designed to provide assistance to state and local government agencies when creating electronic messaging policies for their offices and are intended to address records as defined by 109 RSMo. Employee personal records and information, which do not fall under the definition of a record per 109.210(5) RSMo, are outside the scope of these guidelines. Throughout these guidelines, reference may be made to personal or work cell phone and e-mail accounts. The same concerns apply whether the message originates from a personal or work account, or device. Content is key. If the message references public business or official duties, then it is a record and falls under the appropriate retention schedule. Please note that public records in Missouri are governed under two distinct statutes 109 RSMo, which deals with records management and retention, and 610 RSMo, the "Sunshine Law" which governs access to public records. These guidelines address the development of a total records policy, which will incorporate both statutes, however the primary discussion is directed to issues under 109 RSMo.

Official Records per Missouri Statutes

As referenced above, a public record is any "document, book, paper, photograph, map, sound recording or other material, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of official business. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included within the definition of records as used in sections 109.200 to 109.310 RSMo, and are hereinafter designated as "nonrecord" materials."

An email is an example of a format or "physical form" per 109.210 RSMo, the same as a punch card, paper letter, microfilm, etc. The physical form of the record is irrelevant, rather, it is the content of the email, or any other record, that determines how long it must be retained. The length of time a state record is to be retained can be found on the Missouri State Agency General Retention Schedule or an Agency Records Disposition Schedule that has been approved by the State Records Commission per 109.250(2). The length of time a local government record is to be retained can be found on Records Retention Schedules that have been approved by the Local Records Board per 109.255 RSMo.

The location of the record does not matter. Records stored within an agency, in a warehouse, on a personal device or on a third-party server must be maintained for their full retention period. If an agency is unsure if information qualifies as a record, they should review *What Is A Record?* at: http://www.sos.mo.gov/records/recmgmt/whatisarecord.asp.

Further Assistance

- The Division of Records Management assists agencies within state government with the continual process of renewing and revising their records management practices. State agencies can contact Records Management at 573-751-3319 or recman@sos.mo.gov.

- The Local Records Division advises, educates and encourages custodians of local government records in the use of sound records management and archival practices. Local agencies can contact the Local Records Program at 573-751-9047 or local.records@sos.mo.gov.

- The Missouri Sunshine Law portion of the Attorney General's website, available at https://ago.mo.gov/missouri-law/sunshine-law is a resource to help government officials understand Missouri Sunshine Law and its implications for Missouri's public and quasi-public governmental bodies, members of those bodies, those that conduct business with a public governmental body and private citizens. The Attorney General's Office can be contacted at 573-751- 3321 or sunshinelaw@ago.mo.gov.

Are All Communications Considered Records?

All communications are records, the function and content of the message will determine its retention period. Electronic messages do not have a different retention period than hard copy records. A "record" is defined as **any** "document, book, paper, photograph, map, sound recording or other material, **regardless of physical form or characteristics**, made or received pursuant to law or in connection with the transaction of official business" (109.210(5) RSMo). Transitory messages have a short retention, but messages that set, or form the basis for, policy have a longer retention period. In order to determine the retention, the function and content of the message must be determined by asking two questions:

- What is the message about (content)?
- Why was it sent and for what purpose (function)?

Once the type of record has been identified [See Appendix A for an example of how to identify records], use the appropriate retention schedule to determine the retention period. It should also be noted that during litigation, text messages, email and other communications are a standard part of discovery for court cases and must be maintained under a temporary hold until litigation is concluded, regardless of having met minimum retention.

To determine the retention of a record, state agencies should consult the appropriate retention schedule, located at: https://www.sos.mo.gov/records/recmgmt/introduction, or through the SMART System. Local government entities may find their retention schedules at: https://www.sos.mo.gov/archives/localrecs/schedules/.

Creating a Policy

The Office of the Secretary of State, Records Management and Local Records Divisions encourage government agencies to create internal policies to govern how their electronic messages are managed, what type of content may be communicated electronically, and their responsibilities for retaining electronic messages. When drafting a policy, an agency should consider the following:

- What agency business is appropriate to conduct via electronic message?
- Who is allowed to conduct agency business via electronic message? (every employee, specific employees, etc.)
- Will only messages relating to agency business be allowed on agency owned devices?
- Can personal devices be used for agency business?
- Who will decide what type of record it is? (i.e., who evaluates the record content and function?)
- How will the agency collect and store the messages?
- How will the retention policy be applied?
- What will happen to messages that have met retention?
- How will the policy be communicated to employees?
- How will compliance be monitored?

Drafting a Policy for Text Messages and other Third Party platforms

An agency cannot abrogate its responsibility for maintaining records. Social media and text messaging are just two examples of services in use by government where official records may be found, but not under the control of the government entity. It is incumbent on the entity to ensure that any records created on these third-party services are preserved; **it is not the responsibility of the service provider**. Therefore, policies for the use of these services are vital to meet recordkeeping obligations. Take, for example, text messaging.

Text messaging has become part of everyday communication. Sometimes texting is used by government employees to conduct official business, therefore it is the responsibility of the agency to create policies and procedures concerning the use of text messages for official business. The policy will also need to address what will happen with the text message once it has been identified as a record, and how to keep identifying information (phone numbers/names) and the order of the messages if multiple messages are part of the record.

Retention of Text Messages

Part of the policy for text messages should address how the text messages will be saved until they meet retention. There are multiple ways an agency can ensure it is meeting the requirements of record retention for text messages.

Policy may require a user to save/forward text messages through their phones' operating system to their official email. Alternatively, some other application/software solution may be sought to capture messages. If all else fails, contracting with a third party (i.e., service provider) to store and manage text messages may be a solution—note that this is the least satisfactory in terms of providing adequate response for records requests.

Once an agency determines the preferred method for capturing messages, it will need to decide how to store the messages and ensure the retention schedule is being applied.

Drafting a Policy for E-Mail

E-mail is routinely used to conduct official business and each agency needs to create policies and procedures to ensure records created via e-mail are being handled properly.

Effective management of e-mail records requires the participation of everyone within the agency to ensure that the policies and procedures outlined by the agency and the retention schedules are being followed. Review Policies and procedures regularly to ensure continued compliance with regulatory or legal requirements.

Retention of E-mails

Preserve e-mail that fulfills the definition of a record within a recordkeeping system. If the record is an open public record, maintain it in a format that makes it available to the public. Agencies must ensure their records are accurate and complete regardless of physical form or characteristics throughout the retention period. Several areas must be addressed to ensure e-mail messages are accurate and complete. The recordkeeping system must be able to capture the appropriate information, to ensure the records are easily accessible throughout their retention period, and to ensure the timely disposition of records once their retention period is met.

See Appendix B for more information regarding electronic message retention concerns.

Training and Compliance

Once a policy it established, it is important to ensure all agency personnel are familiar with, and understand their responsibilities when complying with the policy. The agency will need to be able to demonstrate compliance with the policies and procedures through a process of monitoring and auditing.

Records Retention

Agencies may use, but should not rely on, third party providers to retain records, as that responsibility lies solely with the agency creating or receiving the records. All communication is a record of some classification. No communication should be automatically destroyed under any circumstances. The use of auto delete applications and programs should be prohibited by policy, as they do not allow a determination as to the appropriate retention period for a message. Even transitory messages, which may be destroyed immediately, should be evaluated before deletion. Agencies should ensure employees know their responsibility regarding the forwarding/saving of communications. Agencies should have a plan established for the easy retrieval of requested messages that have not yet met retention.

Retention periods for communications vary from transitory to permanent. The retention time will depend on the content and function of the record. If an agency is unsure how long a record needs to be retained state agencies should refer to the Missouri General Retention Schedule, their Agency Records Disposition Schedule or contact the Division of Records Management. Local agencies should refer to their Records Retention Schedules or contact the Local Records Division.

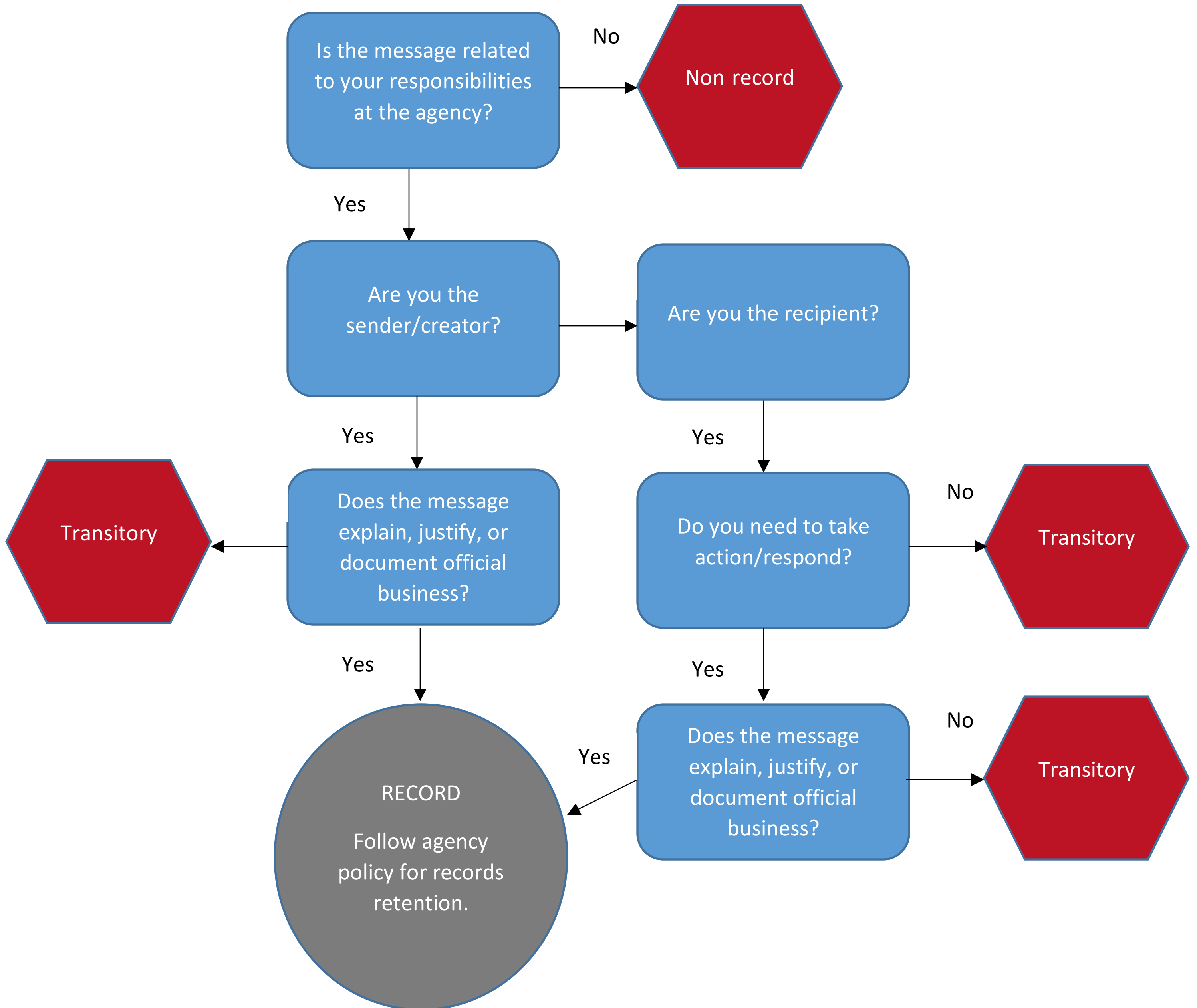
Sunshine Requests
Communications are subject to 610 RSMo, more commonly known as the Sunshine Law. Government records on cell phones (business **and** personal phones) are subject to Sunshine requests, and legal discovery. Cell phone providers are not obligated to respond to agency requests - unless it is specified in the Terms of Use or Terms of Service. For this reason, an agency policy should be established if government business is conducted via cell phone. E-mail accounts (business and personal) can be subject to a Sunshine request and legal discovery. An agency should ensure that electronic communications are stored in a manner that retains all of the necessary information.

If the cell phone is lost, broken, or the cell phone provider changes the Terms of Service, records stored solely on a device could be at risk. Policy should dictate that messages are captured as they are created. Agencies must have a plan and process in place for how records will be saved because without adequate preparation, there is nothing the agency can do to protect itself.

State Government Agencies should access their retention schedules through the SMART System. Or, they may be found at: https://www.sos.mo.gov/records/recmgmt/introduction

Local Governments may find their retentions schedules at:
https://www.sos.mo.gov/archives/localrecs/schedules/

Appendix A: Flowchart to determine if an electronic message is a record and its disposition[1]



[1] This is a generic representation for determining whether a communication is a record. Some Elected and Executive positions have different retention requirements—consult your record schedule.

Appendix B: Areas to Address for Electronic Record Retention

Transmission Data	Agencies should attempt to ensure that as much transmission data as possible is kept within the recordkeeping system. At a minimum the recordkeeping system must include the name of the sender(s), the recipient(s), and the date received. Text messages should include the phone number(s), and be maintained in order. Additionally, if receipt acknowledgements are a part of the e-mail system, users should include those as a part of the record when appropriate. (For example, it may be appropriate to request a receipt acknowledgement when distributing a new policy to staff.) It is important to note that many e-mail systems use aliases to identify users. Therefore, a means of deciphering who the alias belongs to must be maintained. The same is true for distribution lists. There must be a method to identify to whom the individual e-mail address or phone number belongs. However, when the e-mail is received from an e-mail system outside an agency's control, this may be an impossible task. Nonetheless, agencies must make a reasonable attempt to do so.
Authenticity	The system must ensure that once the record is a part of it, it cannot be altered.
Attachments	If an electronic message includes an attachment that meets the definition of a record, it must be maintained.
Calendars and Task Lists	Some e-mail systems include calendars and task lists for each user. If the information contained in the calendar or task list documents decisions, policies, procedures, resource expenditures, operations, or delivery of services, it may meet the definition of a record. Therefore, agencies must develop a method of retaining those records within the recordkeeping system.
Disposition	Materials' final destruction or transfer as determined by their retention period.
Temporary Hold	Once a record series and time period have been identified as part of litigation or audit, a temporary hold order must be placed on the covered records. Agencies must establish procedures to ensure that electronic records are included within the temporary hold order.