Clerk of the Superior Court
*** Electronically Filed ***
R. McLellan, Deputy
12/16/2024 9:51:52 PM
Filing ID 19022774

KRISTIN K. MAYES
Attorney General
Firm Bar No. 014000
NICHOLAS KLINGERMAN
State Bar No. 028231
Assistant Attorney General
2005 N. Central Avenue
Phoenix, Arizona 85004
Telephone 602-542-3881
crmfraud@azag.gov
Attorneys for Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA

THE STATE OF ARIZONA, Plaintiff, vs. **MARK MEADOWS (018)** Defendants.	Case No.: **CR2024-006850-018** **STATE'S RESPONSE TO MEADOWS MOTION TO SUPPRESS SEARCH WARRANT** (Assigned to the Hon. Sam Myers)

Defendant's motion to suppress SW2024-020330[1] should be denied. First, Meadows does not claim ownership of the phones or the associated iCloud accounts, and therefore does not have standing. Even assuming he has standing to challenge the warrant, however, the affidavit alleges facts establishing probable cause, the warrant is not overbroad and is sufficiently particular, and to the extent that *Apple* did not follow the

[1] This search warrant was also incorrectly labeled SW2024-002330. See Facts section for explanation.

terms of the search warrant, the data has not been reviewed and can be filtered out. And to the extent the warrant was invalid, the exclusionary rule does not apply.

DISCUSSION

I. Relevant Facts.

On May 7, 2024, Agent William Knuth appeared before the Honorable Joseph Kreamer to present a search warrant to obtain a number of documents from Apple with regard to this case. SW2024020330, Dkt # 22, 05/07/2024 Minute Entry. Judge Kreamer returned the affidavits and search warrants to Agent Knuth, noting that revisions needed to be made. *Id.* Agent Knuth appeared before Judge Kreamer again on May 9, 2024, and Judge Kreamer issued the warrant at that time. SW2024020330, Dkt # 24, 05/09/2024 Minute Entry.[2] The search warrant was initially labeled SW2024002330 in error. SW2024020330, Dkt # 15, Search Warrant. Judge Kreamer appears to have hand-corrected a copy in the record. SW2024020330, Dkt # 10, Corrected Search Warrant. The 25-page detailed Affidavit for SW2024020330 does not appear to have been similarly hand-corrected, so it contains the incorrect search warrant number of SW2024002330. SW2024020330, Dkt # 27, Warrant Affidavit.

Agent Knuth served a copy of the original warrant on Apple with the number listed as SW2024002330, which did not contain Judge Kreamer's hand-correction to the search

[2] The State requested transcripts for the May 7 and May 9, 2024, search warrant proceedings before the Honorable Joseph Kreamer. The State may supplement this Motion upon receipt of those transcripts.

warrant number of SW2024020330. Ex. 1, Bates 024455-024459. As a result, the response from Apple was labeled as SW2024002330. *Id.*

The Affidavit in support of SW2024-020330 (labeled as SW2024-002330) contains the following excerpts that reference Meadows:

At page 7:

> Mark Meadows. Meadows was Donald Trump's Chief of Staff in 2020. Meadows communicated with several of the co-conspirators in the creation of the fake electors scheme via email. Including extensive communication with fake elector Kelli Ward.

At page 8:

> Trump himself was unwilling to accept that he lost the election, but Meadows had confided in a staff member in early November that Trump had lost the election. Nevertheless, Trump wanted to keep fighting the election results, and Meadows wanted to help Trump.

At page 8:

> The Trump Campaign next filed a suit on November 8, 2020, in *Trump v. Hobbs,* Maricopa County Superior Court No. CV2020-014248. The claims relating to the Presidential Election were dismissed five days later because the lawsuit would not have changed the outcome of the election. That prompted Kelli Ward to text Meadows, "WTH," ask Meadows "[a]re our lawyers in AZ afraid of being blackballed by the left," and conclude "it sounds like that's a total cop out."

At page 10:

> Trump Campaign officials and other unindicted coconspirators also tried to contact the Supervisors. For example, Arizona Congressional Representative Andy Biggs sent a text message to Meadows on November 8, 2020, that he "placed some calls to the board of supervisors without connecting so far," later writing, "I can give you some idea what's going on with the county supervisors." Kelli Ward sent Meadows a text message on November 13, 2020, "Just talked to POTUS. He may call the Chairman of the Maricopa Board of Supervisors," who was then Clint Hickman. Hickman later received

a call from the White House Switchboard on New Year's Eve, but he did not answer.

At pages 12–13:

> Discussions about using the Republican electors to change the outcome of the election began as early as November 4, 2020. Those plans evolved during November based on memos drafted by Trump Campaign attorney Kenneth Chesebro.
>
> As an example, Rick Perry who was the United States Secretary of Energy texted Meadows on November 4, 2020, "HERE's an AGRESSIVE STRATEGY: Why can't the states of GA NC PENN and other R controlled state houses declare this is BS (where conflicts and election not called that night) and just send their own electors to vote and have it go to the SCOTUS."
>
> Similarly, Tommy Long, who was the mayor of Millersville, North Carolina, texted Meadows on November 5, 2020, that Trump should "urge GOP officials in close states to expose shenanigans and, if necessary, to refuse to seat Biden electors in the event of a fake count." That same day, Donald Trump Jr. texted Meadows a more developed plan revolving around the electors: "It's very simple If through our lawsuits and recounts the Secretary of States on each state cannot 'certify' that states vote the State Assemblies can step in and vote to put forward the electoral slate Republicans control Pennsylvania, Wisconsin, Michigan, North Carolina etc. we get Trump electors."
>
> Arizona congressman Andy Biggs similarly texted Meadows on November 6, 2020:
>
> I'm sure you have heard of this proposal. It is to encourage the state legislatures to appoint a look doors [sic] in the various states where there's been shenanigans. If I understand right most of those states have Republican Legislature's [sic]. It seems to be comport with glorified [sic] Bush as well as the Constitution. And, well highly controversial, it can't be much more controversial than the lunacy that were sitting out there now. And It would be pretty difficult because he would take governors and legislators with collective will and backbone to do that. Is anybody on the team researching and considering lobbying for that?
>
> Meadows responded "I love it."

At page 14:

> The memo eventually made its way to members of the Trump Campaign who reluctantly went along with Chesebro's plan to have the Republican electors vote in all six listed states. Aside from the possibility of Georgia, they concluded that there were no pending lawsuits that could change the outcome of the election in the remaining six states. Trump Campaign officials also had general concerns about Rudy Giuliani's efforts. Advisor Jason Miller wrote Meadows on December 6, 2020, for example, "[a]II guidance appreciated, as the legal turf war thing is new to me!"

There is no dispute that Meadows was Trump's Chief of Staff during the relevant timeframe in 2020. Meadows is a public figure who is internationally known—there is nothing conclusory about that. The Affidavit establishes that as a high-ranking Trump official, Meadows's communications with Arizona Senator Biggs on November 6, 2020, near the inception of the scheme and conspiracy, could reasonably be construed as authorizing it.

Upon receipt of the responsive documents from Apple, the State followed the procedure laid out in Judge Kreamer's September 19, 2024, minute entry. CR2024-006850, Dkt # 1450-1467. State's counsel reached out to Defendants' counsel and asked if they wanted to be present while the State's investigator sorted the responsive documents into separate folders for each Defendant. Ex. 2. None of the Defendants informed the State that they wanted to be present for the sorting of documents. Ex. 3. The State's investigative team then separated the documents into folders for the individual Defendants. Then, the State forwarded separately to each Defendant's counsel a copy of only those documents related to the individual Defendant so that each Defendant could conduct a privilege review. The State has not yet reviewed the documents for content, pursuant to the Court's

Order, because, to date, none of the Defendants have notified the State that they have completed the privilege review.

II. To the Extent Meadows Disclaims Ownership of the Phones and Documents Returned, He Lacks Standing to Challenge the Search Warrant.

As an initial matter, throughout Meadows's motion, he does not claim ownership of the phone numbers and associated iCloud accounts. *See, e.g.*, Meadows Motion to Suppress, Dkt. #1995, at 1 (referring to the applicable warrant as being "for information associated with three phone numbers that the State alleges are connected to Meadows"), 3 ("The alleged association of name to phone number appears only on the affidavit."), 18–19 (arguing the warrant did not "connect[] any person (let alone Meadows) to any particular email address or phone number"). He also notes that the information returned by Apple includes data from seven iCloud accounts and implies that they are not all his, arguing that "other third parties' rights" were violated." Dkt. #1995, at 7.

"Fourth Amendment rights are personal rights which … may not be vicariously asserted." *State v. Jean*, 243 Ariz. 331, 334, ¶ 10 (2018) (quoting *Rakas v. Illinois*, 439 U.S. 128, 140 (1978)); *State v. Huffman*, 169 Ariz. 465, 467 (App. 1991) ("A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by the search of a third person's premises or property has not had any of his Fourth Amendment rights infringed.") The proponent of a motion to suppress has the burden of establishing that his own personal rights were violated by the challenged search. *State v. Harris*, 131 Ariz. 488, 490 (App. 1982).

To the extent Meadows is disclaiming ownership of the phone numbers and associated iCloud and email accounts, he does not meet his burden of establishing that his own personal rights were violated. And if he is arguing the State obtained documents owned by third parties, he cannot assert constitutional rights on their behalf. *Jean*, 243 Ariz. at 334, ¶ 11 ("Jean cannot complain about the search by arguing that it invades another person's constitutional rights."). Meadows cannot simultaneously disclaim ownership of the phone numbers and associated accounts and challenge the validity of the search warrant, and the motion to suppress should be denied for this reason.

III. The Apple Search Warrant Was Valid.

Even assuming Meadows has standing to challenge the warrant, which the State maintains he does not, the warrant was valid. To be valid, a search warrant must be issued by a neutral, disinterested magistrate; must be supported by probable cause; and must particularly describe the thing to be seized and place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979). Once issued, a search warrant is presumed to be valid. *Greehling v. State*, 136 Ariz. 175, 176 (1983); *see also Mehrens v. State*, 138 Ariz. 458, 460–61 (1983). "It is then the individual's burden to prove the invalidity of the search and seizure." *Greehling*, 136 Ariz. at 176; *see also Mehrens*, 138 Ariz. at 460–61.

A. Probable Cause.

Probable cause exists when the facts known to a police officer "would warrant a person of reasonable caution in the belief that contraband or evidence of a crime is present." *State v. Sisco*, 239 Ariz. 532, 535, ¶ 8 (2016) (quoting *Florida v. Harris*, 568 U.S. 237, 243 (2013). "[A]ll that is 'required is the kind of fair probability on which reasonable and

prudent people, not legal technicians, act.'" *Id.* (quoting *Florida v. Harris*, 568 U.S. at 244) (cleaned up). "A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" *Illinois v. Gates*, 462 U.S. 213, 236 (1983); *see also State v. Hyde*, 186 Ariz. 252, 272 (1996) (trial court "must grant deference" to magistrate's decision). A trial court reviewing a warrant must "determine whether the totality of the circumstances indicates a substantial basis for the magistrate's decision." *State v. Hyde*, 186 Ariz. 252, 272 (1996).

Meadows is charged in this case as 1 of 18 defendants with 9 felony counts including conspiracy, fraud schemes, and forgery related to the filing of fake elector certificates for the 2020 presidential election. The theories of the case also include accomplice liability under A.R.S. § 13–301, *et seq*. This was a sweeping offense involving many co-conspirators and requiring extensive communication by phone and email, as detailed in the affidavit. SW2024020330, Dkt # 27 ("Warrant Affidavit"). Meadows's communications and interactions with those co-conspirators during the three months around the election, certifications, and eventually the inauguration are relevant and necessary to the probable cause determination. *See* Ariz. R. Evid. 801(d)(2)(E).

Meadows argues the warrant and affidavit do not provide a substantial basis for the magistrate's decision because they contained "two general statements about Meadows's alleged connection to the crimes and his association with the other defendants"; it contained a vague unattributed statement to a staff member that he wanted to "help Trump"; most of the text messages about the fake elector scheme detailed in the affidavit were sent *to* him, with him only responding to one of them that he "love[d]" the plan; the text messages

detailed in the affidavit as sent to Meadows end November 13, but the fake electors did not sign the false electoral vote documents until mid-December; and the affiant's statement of experience did not indicate he had extensive experience in fraud investigations or in "drafting and executing search warrants for voluminous electronic information." Dkt. #1995, at 8–11.

Taking a "more flexible, all-things-considered approach" to the question of probable cause, *Harris*, 568 U.S. at 244, substantial evidence exists supporting the magistrate's finding. Meadows's position as chief of staff to Donald Trump, together with his communications with the fake electors and other co-conspirators, along with the acts of his co-conspirators is more than sufficient to establish probable cause here. The affidavit establishes that as a high-ranking Trump official, Meadows's communications with Arizona Senator Biggs on November 6, 2020, near the inception of the scheme and conspiracy, could reasonably be construed as authorizing it. Warrant Affidavit, at 12–13. Further, a witness known to investigators (not an anonymous informant offering a tip) stated that Meadows had said he "wanted to help Trump," despite knowing Trump had lost the election. Warrant Affidavit, at 8. And the affidavit details how many of the plans were communicated by emails, texts, and phone calls, and how the conspirators were in touch with the White House, where Meadows was chief of staff. Warrant Affidavit, at 10–19. That the various messages detailed plans in November that were not carried out until December does not change the analysis. The State did not seek the warrant based on Meadows's mere association or his position—under a totality of the circumstances, the

above facts "would warrant a person of reasonable caution in the belief that contraband or evidence of a crime" was present on Meadows's phones. *Sisco*, 239 Ariz. at 535, ¶ 8.[3]

Meadows also claims that the affidavit establishes that others communicated "to" Meadows and nothing more, conceding the one Biggs communication. However, the Affidavit states that Meadows communicated "with" others in the conspiracy extensively. Warrant Affidavit, at 7. The nature, content, and context of the messages establish that Meadows participated in those communications and was a co-conspirator.

The State is not required to establish probable cause that Meadows committed overt acts in furtherance of the conspiracy, only that he joined it. Once an individual joins a conspiracy, he is responsible for the acts of coconspirators. The *Olea* Court explained:

> The requirement of an overt act as one of the elements of conspiracy does not mean that each individual charged with the crime of conspiracy must commit an overt act. Rather, the proof is sufficient if only one of the parties to a conspiracy commits an act toward the execution of the goal of the conspiracy. *State v. Green*, 116 Ariz. 587, 570 P.2d 755 (1977); *State v. Aguirre*, 27 Ariz.App. 637, 557 P.2d 569 (1976). Any one act by any one or more of the conspirators may be attributed to all of the members of the conspiracy. *State v. Dupuy*, 116 Ariz. 151, 568 P.2d 1049 (1977).

State v. Olea, 139 Ariz. 280, 295, 678 P.2d 465, 480 (App. 1983); *see also* Senate Fact Sheet, S.B. 1354, 48th Leg., 2nd Reg. Sess. (Feb. 7, 2008) (citing *State v. Phillips*, 202 Ariz. 427 (2002), and stating that the 2008 amendments to § 13–303 "[e]xpands accomplice liability of a person to include any offense that is a natural and probable or reasonable foreseeable consequence of the offense for which that person was an accomplice").

[3] At times, Meadows references the incorrect standard, the one for arrests. *See* Dkt. #1995, at 9–10 (arguing the "conclusory statements about Meadows" were insufficient "to establish probable cause that he committed a crime").

With these facts, the State could search Meadows's phone for evidence that others in the conspiracy were committing crimes in furtherance of the conspiracy. The Court may issue a search warrant pursuant to A.R.S. § 13–3912(4), "[w]hen property or things to be seized consist of any item or constitute any evidence which tends to show that a particular public offense has been committed... ." Here, in the search warrant affidavit, the State cited evidence establishing that coconspirators made statements in communications to Meadows that outlined the entire conspiracy. The State established probable cause that evidence tending to show a public offense was committed could reasonably be expected to be found on Meadows's phone.

Finally, Meadows dismisses the expertise of the Affiant, Agent Knuth. Dkt. # 1995, at 10–11. Knuth has been a law enforcement officer for more than 20 years, "and investigated cases related to traffic, theft, *fraud*, burglary, narcotics, domestic violence, [and] civil complaints," before serving as a detective in investigating violent crimes against children and homicide, then served as a sergeant, retired, and joined the Arizona Attorney General's Office, where he received training in fraud investigations and has more recently worked on election integrity cases. Warrant Affidavit, at 4 (emphasis added). Meadows cites no case supporting his argument that this is somehow insufficient to draft a warrant affidavit for a case about a sweeping conspiracy to commit fraud committed in plain sight, nor does he explain how it affects probable cause analysis. This argument necessarily fails.

The point of probable cause for a search warrant is to identify facts leading to a commonsense conclusion that the State may find evidence of a crime, not to prove conclusively that a crime was committed. The search warrant affidavit demonstrates that

Meadows was told about the plan in early November, knew Trump had lost the election but wanted to help keep him in office anyway, communicated frequently with coconspirators, the plan he "loved" in early November was actually executed in December, and attempts were made to keep Trump in office despite losing the election—like Meadows had wanted to accomplish—on January 6 by other coconspirators. Common sense supports the Court's conclusion that probable cause existed to search Meadows's communications for evidence proving his involvement in the conspiracy.

Meadows does not meet his burden of showing the warrant was unsupported by probable cause.

B. The Search Warrant Was Not Overbroad, Nor Lacking in Particularity.

The Fourth Amendment mandates that "no Warrants shall issue … [unless] particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The specificity of a search warrant has two parts: particularity and breadth. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). Both are necessary to avoid "general, exploratory searches and seizures." *State v. Ray*, 185 Ariz. 89, 92–93 (App. 1995). "Particularity is the requirement that the warrant must clearly state what is sought[, while] [b]readth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *Hill*, 459 F.3d at 973. Meadows contends that the Apple search warrant both lacked particularity and was overbroad.

1. *Meadows does not show the warrant was overbroad.*

"When deciding whether a warrant is too general, the trial court must consider the nature of the property sought to be recovered." *State v. Ray*, 185 Ariz. 89, 93 (App. 1995). The Ninth Circuit considers three factors in analyzing the breadth of a warrant:

> (1) whether probable cause existed to seize all items of a category described in the warrant; (2) whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not; and (3) whether the government could have described the items more particularly in light of the information available.

United States v. Flores, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Lei Shi*, 525 F.3d 709, 731–32 (9th Cir. 2008)).

The affidavit detailed that Meadows participated in a wide-ranging conspiracy that was conducted in part via text messages, phone calls, and emails; specifically, it detailed that Meadows was communicating this way with co-conspirators. As detailed in the affidavit, the conspiracy commenced at the latest on Election Day (November 3, 2020); continued through the swearing-in of President Joseph Biden on January 20, 2021; related lawsuits continued through June 15, 2021; and fake electors were still making public statements in support of the failed scheme as late as 2022. The warrant allowed the government to search just three months (from November 1, 2020 through February 1, 2021) of Apple account information, including: (1) Meadows's account information and billing records; and (2) electronic data stored locally, and in the cloud, consisting of (a) call detail records, (b) messaging, (c) contact lists, (d) emails, and (e) geolocation information. Warrant Affidavit, at 2. The warrant was further limited to evidence of forgery, tampering with a public record, presentment of a false instrument for filing, fraudulent schemes and

artifices, fraudulent schemes and practices, conspiracy, and changing the vote of an elector by corrupt means or inducement. Warrant Affidavit, at 1.

The scope of the warrant, which covered only Meadows's accounts and was limited to just three months of certain types of data shown by the affidavit to be the means of communications of the conspiracy, was supported by probable cause. *See Flores*, 802 F.3d at 1044 (probable cause supported Facebook warrant with no temporal limitation where it was limited to defendant's account and "authorized the government to seize only evidence of violations of" certain offenses); *see also United States v. McCall*, 84 F.4th 1317, 1327–28 (11th Cir. 2023) (concluding that time-based limitation was the "preferred method of limiting the scope of a search warrant for a cloud account"); *United States v. Pilling*, 721 F. Supp. 3d 1113, 1123 (D. Idaho 2024) (defendant's use of emails to communicate about facts relevant to the offenses rendered it "reasonable to conclude that additional relevant evidence would likely be found").

Meadows argues the affidavit does not connect the criminal activity to the phone numbers nor the phone numbers listed next to his name as his. Dkt. #1995, at 13–14. The criminal activity is linked to him and any phone accounts he uses because he used a phone to communicate and receive communications from co-conspirators. Probable cause exists that evidence of the conspiracy will be present on one or more of Meadows's phones. The State was not required to limit its search to just one phone; given the nature of data sharing and cloud storage, responsive documents may be in any number of phones and accounts Meadows used. And to the extent he is disclaiming ownership of the phones, he would not have standing to challenge the warrants. *See Huffman*, 169 Ariz. at 467.

Regarding the second factor, the objective standards for differentiating items, by restricting the time to a small window and detailing the offenses under investigation, as well as detailing within the affidavit the types of communications that had already been found, the investigating officers had a means of differentiating between items that are responsive and not responsive. *See United States v. Zelaya-Veliz*, 94 F.4th 321, 337 (4th Cir. 2024) (warrants authorizing government to search all information disclosed by Facebook were nonetheless confined by reference to the suspected criminal offenses); *Pilling*, 721 F. Supp. 3d at 1123–24 (warrant authorizing items limited to evidence related to certain violations and limited to certain types of files (e.g. emails or email attachments) was not overbroad). *Cf. Flores*, 802 F.3d at 1044 (warrant with no temporal limitation that provided "procedures for electronically stored information" was not overbroad).

Meadows argues the warrant needed to be more specific in order for the search to filter out sensitive data. But the warrant *is* limited to evidence related to the offenses, and it is limited to a relatively small window of time related to the offenses. *United States v. Zelaya-Veliz*, 94 F.4th 321, 337 (4th Cir. 2024) (warrants authorizing government to search all information disclosed by Facebook were nonetheless confined by reference to the suspected criminal offenses); *United States v. Good Voice*, 602 F. Supp. 3d 1150, 1168 (D.S.D. 2022) (warrant for Facebook account detailing statutory violations alleged and containing temporal limit sufficiently particular). Meadows cites *Pilling*, an informative case on the issue in which the trial court suppressed evidence obtained through an Apple warrant, but did not suppress evidence obtained through a Google warrant. Dkt. #1995, at 14. Regarding the Apple warrant, the court assumed there was no affidavit attached during

execution, which meant the warrant "authorized a search of the defendant's entire iCloud account for 'fruits, contraband, evidence, and instrumentalities of violations' of five statutes."[4] 721 F. Supp. 3d at 1124–25. The statutes were broad, and without an affidavit detailing the offenses, it "authorized a search of vast swaths of data but failed to particularly identify the things to be seized." *Id.* at 1127–28. In fact, the court noted "the outcome may have been different if" the affidavit had been incorporated into the Apple warrant. *Id.* at 1127. Here, unlike the broad warrant without an affidavit in *Pilling*, the temporal limitation narrowed the scope of the returned information, and the statutory citations and detailed affidavit narrowed the scope of what investigators could search. *Pilling* does not aid Meadows's argument.

Regarding the third factor, the State's description of the items was adequately particular in light of the information available. With electronic searches, "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes." *United States v. Ulbricht*, 858 F.3d 71, 101–02 (2d Cir. 2017) *overruled on other grounds by Carpenter v. United States*, 585 U.S. 296 (2018); *United States v. Ray*, 541 F. Supp. 3d 355, 393–94 (S.D.N.Y. 2021)

[4] The Ninth Circuit strictly requires that affidavits be attached to warrants at the time of execution and be expressly incorporated, or they cannot be read to narrow the search. *United States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir. 1982); *see also United States v. Luk*, 859 F.2d 667, 676 (9th Cir. 1988). That is not the rule in every circuit. *See, e.g.*, *United States v. Hurwitz*, 459 F.3d 463, 471–72 (4th Cir. 2006); *Baranksi v. Fifteen Unknown Agents*, 452 F.3d 433, 440–45 (6th Cir. 2006). Arizona does not appear to have a specific rule. *See, e.g.*, *State v. Woratzeck*, 130 Ariz. 499, 501–02 (App. 1981) (reference to attachment and officer's possession of affidavit sufficient).

(rejecting argument that initial search of electronic data should have been limited by keyword); *United States v. Weigand*, 482 F. Supp. 3d 224, 242 (S.D.N.Y. 2020) (approving of warrant that permitted preliminary search of entire devices rather than specific folders, because "few people keep documents of their criminal transactions in a folder marked 'drug records'") (quoting *United States v. Riley*, 906 F.2d 941, 845 (2d Cir. 1990)); *United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Maine 2011) ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching."); *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (S.D.N.Y. 2008) (lack of search methodology or keyword terms did not render search warrant overbroad). Further, "a warrant need not be more specific than knowledge allows." *United States v. Ivey*, 91 F.4th 915, 918 (8th Cir. 2024) (warrant for entire cell phone was not an impermissible general warrant) (quoting *United States v. Bishop*, 910 F.3d 335, 337–38 (7th Cir. 2018).

Meadows suggests that the State should have sent keywords to Apple, as the State used with the X Corp./Twitter account; but the affidavit itself demonstrates the difficulty of this. For example, in the exchange with Andy Biggs in which Meadows responded, "I love it," Biggs's message contains the typo, "a look doors," instead of "electors," and would not have been found by the suggested keyword search. Warrant Affidavit, at 12–13. Broader keywords, such as "legislature," do little to narrow the scope, while likely still missing responsive documents. Similar results would occur if limited to communications between particular people; the limitation would be too narrow (e.g., Biggs is not an indicted

co-conspirator), or so broad as to be unhelpful. *See McCall*, 84 F.4th at 1327–28 (noting subject-based limitation may be so broad as to be meaningless before concluding that time-based limitations are preferable); *see also United States v. Pilling*, 721 F. Supp. 3d 1113, 1123 (D. Idaho 2024) (limiting search to emails between parties identified the government would have "created a substantial risk of excluding relevant records," such as relevant documents sent to other parties).

In a footnote, Meadows notes that some agencies use keyword searches after the information has been turned over, and may use independent third parties or screened-off teams to do that portion of the review. Dkt. #1995, at 15. This approach has been used in federal cases and is contemplated by the Federal Rules of Criminal Procedure. *See, e.g.*, *Lindell v. United States*, 82 F.4th 614, 420 (8th Cir. 2023) (detailing government's use of "filter protocols to safeguard confidential, private, and privileged materials on plaintiff's phone); *see also* Fed. R. Crim. P. 41(e)(2)(B). But "[n]othing in the language of the Constitution or in [the Supreme] Court's decisions interpreting that language suggests that … search warrants also must include a specification of the precise manner in which they are to be executed." *Dalia v. United States*, 441 U.S. 238, 257 (1979). Rather, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection 'against unreasonable searches and seizures.'" *Id.* As noted above, the State has not actually looked at any of the documents due to the court order requiring a privilege review by parties first. It is unclear if the volume of documents will require keyword searches to include or exclude documents, how the

documents are organized, if responsive documents can be easily segregated, or if Apple produced documents outside the temporal bounds of the warrant. To the extent these are issues, they can be resolved before the State reviews any documents.

In sum, because Meadows's involvement in the sweeping conspiracy took place in part on his phone, probable cause existed to seize the items described in the warrant; the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not, including a temporal limitation, the cited offenses, and the narrative of the offenses; and (3) keywords or subject-matter limitations would have either been too broad or too narrow, and the temporal limitation was adequate. *Flores*, 802 F.3d at 1044. The warrant was not overbroad.

2. *Meadows does not show that the warrant was insufficiently particular.*

As noted above, "[p]articularity is the requirement that the warrant must clearly state what is sought." *Hill*, 459 F.3d at 973. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another." *State v. Robinson*, 139 Ariz. 240, 241 (App. 1984) (quoting *Stanford v. Texas*, 379 U.S. 476 (1965)); *State v. Roark*, 198 Ariz. 550, 552, ¶ 8 (App. 2000). It also prevents confusion or uncertainty by the executing law enforcement officer as to the scope of the permissible search. *Id.* And the description need not be perfect; "[t]he practical accuracy rather than the technical precision governs in determining whether a search warrant adequately describes the premises to be searched." *United States v. Williams*, 687 F.2d 290, 292 (9th Cir. 1982).

Meadows cites two inapposite cases to argue the State sought a general warrant for Meadows's phone accounts. In *People v. Herrera*, 357 P.3d 1227, 1228 (Colo. 2015), the State's warrant only covered "indicia of ownership" and texts between two particular accounts. While scrolling by hand through the device, the detective saw a folder labeled with a different name (not included in the warrant) and confirmed they were relevant to a different investigation. *Id.* The State sought admission of those documents as being included under the "indicia of ownership" portion of the warrant, or under the plain-view exception to the warrant requirement. *Id.* The Court concluded the State's reading of the warrant text rendered *every* message on the phone relevant to "indicia of ownership," and ultimately a general warrant. *Id.* Unlike *Herrera*, the information sought in this case must be relevant to the listed offenses, and the State is not seeking to expand the scope of the case or the warrant. The investigators who will eventually sift through the data (after privilege review by the parties) will have the warrant and affidavit available to reference to determine what is and is not relevant and responsive.

Similarly, in *United States v. Cardwell*, 680 F.2d 75, 77 (9th Cir. 1982), the warrant sought only "books and records" of certain parties "which are instrumentalities of crime" involving one provision of the internal revenue code. There were no further details about a *particular* criminal episode, just anything relevant to that statute. *Id.* Here, the affidavit details the particular events to which the evidence sought must relate, and the warrant is limited in scope to the time during which those events occurred.

Meadows also contends that the time limitation was insufficient "[w]ithout any other limitations," but the warrant was indeed limited to the listed offenses, and the

affidavit provided other details. He next argues, "some of the seized information, such as the Contacts category, is not date-restricted at all, suggesting that the date limitation was not effective or adhered to," and that the data in the contact information contained passwords.[5] Again, the State has not seen this data; to the extent it is irrelevant, private, privileged, or beyond the scope of the warrant itself, it can be filtered out.

As noted above, Meadows is accused of being involved in a sweeping conspiracy involving multiple actors all over the country communicating over the phone. The warrant was supported by probable cause, was limited to evidence of detailed offenses, and was limited to a three-month window. Contrary to Meadows's arguments, the warrant was sufficiently particular.

C. The State Is Unaware Whether Apple Produced Data Outside the Scope of the Search Warrant.

Meadows's last claim is that Apple produced data not specifically included in the search warrant. Because the State is operating under an order not to review the data, the State was unaware of this before the motion was filed and cannot take corrective action without reviewing the data. Further, it is unclear whether the data received actually is outside the bounds of the warrant—for example, the State sought geolocation data, which is frequently included in photo metadata. To the extent there *is* a problem, Meadows's own case citation indicates that any remedy would be redaction of content exceeding the scope of the warrant, *see United States v. Maxwell*, 45 M.J. 406, 420–23 (C.A.A.F. 1996)

[5] If the contacts existed in Meadows's accounts during the relevant time period, they were within the dates provided in the warrant. Those same contacts may be particularly relevant if they help identify who Meadows was communicating with.

(considering course of action where AOL returned more data than requested by investigators), not invalidation of the warrant itself due to Apple's error. Parties can meet and confer about what to do next, but so long as the order is in place forbidding State review of the documents, the State cannot remedy any alleged errors.

D. If the warrant was insufficient, the good faith exception applies.

Even if the warrant was faulty, the good faith exception to the exclusionary rule applies in this case. *See State v. Weakland*, 246 Ariz. 67, 69–70, ¶¶ 6–10 (2019). The exclusionary rule allows suppression of evidence obtained in violation of the defendant's Fourth Amendment rights; it is not designed to redress injury from the violation, but to "deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236–37 (2011). Thus, deliberate, reckless, or grossly negligent conduct may lead to suppression of evidence, but when law enforcement acts "with an objectively 'reasonable good-faith belief' that their conduct is lawful," then deterrence is less effective. *Id.* at 238 (quoting *United States v. Leon*, 468 U.S. 807, 909 (2011)). This is particularly apt where an officer has acted with objective good faith in obtaining a search warrant from a judge or magistrate, because "[i]t is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment." *Leon*, 468 U.S. at 921. "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.* As such, a warrant must "be so obviously defective that no reasonable officer could have believed it was valid" to warrant suppression. *Messerschmidt v. Millender*, 565 U.S. 535, 555 (2012). "The occasions on which this

standard will be met may be rare, but so too are the circumstances in which it will be appropriate to impose personal liability on a lay officer in the face of judicial approval of his actions." *Id.* at 556.

Meadows argues that law enforcement did not act in good faith because the warrant was based on the same factual basis as other warrants, the email addresses and phone numbers were not connected to the specific communications cited in the affidavit of probable cause, the data received was voluminous and involved third-party data where "associated with [listed] accounts,"[6] and there were 19 listed phone numbers, which rendered the search "sweeping." Dkt. #1995, at 17–18. He also argues the State acted in "callous disregard for the rights of the account holders, including unindicted third parties," and did not propose a protocol for review other than the privilege pre-review by the parties. Dkt. #1995, at 18.

First, as discussed above, the warrant was supported by probable cause, particular, and not overbroad. To exclude evidence for insufficient indicia of probable cause, "the affidavit must be so clearly insufficient that it provided no hint as to why police believed they would find incriminating evidence." *McCall*, 84 F.4th at 1325 (cleaned up). Meadows is accused of participating in a sweeping conspiracy involving dozens of actors, carried out via emails, text messages, and phone calls, among other things. The affidavit provided sufficient indicia of probable cause to search his Apple account for

[6] Again, the State has not looked at the data; to the extent the data returned by Apple was indeed outside the scope of the warrant, it can be filtered out. If it is merely not relevant, it can also be filtered out.

communications. *Id.* at 1325–26 (not unreasonable to believe that relationship with gunmen would be reflected in iCloud account). Further, the State could not narrow its request to Apple based on information it did not know. *Ivey*, 91 F.4th at 918 (warrant need not be more specific than knowledge allows). And the fact that 19 phone numbers were requested is a reflection of the sweeping nature of the offense itself—as the affidavit shows, the list includes a phone number for nearly every defendant. Warrant Affidavit, at 1–2. Of the 19 numbers in the warrant, only 3 relate to Meadows. The remaining 17 belong to others. To the extent Meadows believes they should not have been included in the warrant, he has no standing to argue on their behalf.

Regarding the protocol, as stated above, a detailed protocol for how to segregate responsive from non-responsive documents was not required to appear on the face of the warrant. *Dalia*, 441 U.S. at 257. The trial court has issued an order that requires privilege review by defendants first, so no content review of the documents has been conducted by the State. Further, the State *asked* Defendants if they wanted to be present for the separation of responsive documents, but none requested to be present. *See* Exs. 2 and 3. Because of the Court's order, and particularly in light of the extremely short time frame of documents requested by the warrant, there is no need for an additional protocol here.

Meadows cites several federal cases in which warrant applications were denied without prejudice because of a lack of particularity and no protocol for review in place. Dkt. #1995, at 19. Significantly, these are federal cases operating under federal case law and rules, and the government merely had to amend the search warrant; they are not cases regarding the suppression of evidence obtained via warrant. *See, e.g.*, *In re Black iPhone*

4, 27 F. Supp. 3d 74, 80 (D.D.C. 2014). One case, *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1171 (9th Cir. 2010), discusses an order returning property where the government did detail protocols for segregating material in search warrant and then failed to follow them. They are inapposite.

Further, protocols are not required in every federal circuit, *see, e.g.*, *Wellington v. Daza*, No. 17 CV 00732 JAP/LF (D.N.M. June 5, 2018) (noting that the 10th Circuit has not required such protocols), let alone by Arizona courts. And if this Court were to determine that such protocols were indeed necessary, "the only error of the officers would be to have failed to anticipate that holding." *See Ray*, 541 F. Supp. 3d at 395.

With regard to warrants like the one here, as the Eleventh Circuit has stated, "Because courts struggle to decide how probable cause and particularity apply to the information that law enforcement collects from a cloud account, it is unsurprising that police officers might struggle as well." *McCall*, 84 F. 4th at 1324; *see also Zelaya–Veliz*, 94 F. 4th at 340–41 (where Facebook search was overbroad and contained no temporal limitation, law was "unsettled" and reasonably well-trained officer would not have known it was illegal); *United States v. Chavez*, 423 F. Supp. 3d 194, 208 (W.D.N.C. 2019) (overbroad Facebook warrant was a "close enough question" that executing officers could reasonably have believed it was valid); *United States v. Shipp*, 392 F. Supp. 3d 300, 312 (E.D.N.Y. 2019) (though court was concerned with breadth of Facebook warrant, "other district courts have declined to suppress evidence obtained pursuant to facially similar warrants… [and] reliance on the Facebook Warrant … was not objectively unreasonable").

Reliance on the search warrant was not objectively unreasonable, and suppression is not warranted.

CONCLUSION

For the reasons stated above, the State requests the Court deny Meadows's motion to suppress the Apple search warrant.

Respectfully submitted December 16, 2024.

KRISTIN K. MAYES
ATTORNEY GENERAL

/s/ Nicholas Klingerman
NICHOLAS KLINGERMAN
Assistant Attorney General
Criminal Division

ORIGINAL of the foregoing e-filed
this 16th day of December, 2024 with:

Clerk of the Court
Maricopa County Superior Court
175 West Madison Street
Phoenix, Arizona 85003

The Honorable Bruce Cohen
Maricopa County Superior Court

COPY of the foregoing emailed
this 16th day of December, 2024 to:

Brad Miller
Office@BradLMiller.com
Counsel for K. Ward 001

Andrew Pacheco
apacheco@rrulaw.com
Steve Binhak
binhaks@binhakslaw.com
Counsel for T. Bowyer 002

John Dosdall
criminaldocket@jacksonwhitelaw.com
Counsel for N. Cottle 003

Timothy La Sota
tim@timlasota.com
Michael Columbo
mcolumbo@dhillonlaw.com
Gerald Urbanek
gurbanek@dhillonlaw.com
Jesse D. Franklin-Murdock
jfranklin-murdock@dhillonlaw.com
Counsel for J. Hoffman 004

Andrew Marcantel
Andy@AttorneysForFreedom.com
Counsel for A. Kern 005

Dennis Wilenchik
admin@wb-law.com
Diw@wb-law.com
Lacy Cooper
Lacy@azbarristers.com
Alan M. Dershowitz
alandersh@gmailcom
Counsel for J. Lamon 006

Danny Evans
Danny.Evans@maricopa.gov
Amanda Lauer
Amanda.Lauer@maricopa.gov
Counsel for R. Montgomery 007

Jeffrey Cloud
jcloud@jcloudlaw.com
Counsel for S. Moorhead 008

Richard Jones
Richard.Jones@Maricopa.gov
Counsel for G. Safsten 010

Brad Miller
Office@BradLMiller.com
Counsel for M. Ward 011

Mark Williams
markwilliamsesq@yahoo.com
Counsel for R. Giuliani 012

Ashley Adams
aadams@azwhitecollarcrime.com
Counsel for J. Eastman 013

Michael Bailey
mbailey@tullybailey.com
Counsel for B. Epsthyn 014

Thomas Jacobs
tjacobs@jacobsArizonalaw.com
Counsel for C. Bobb 016

Kurt Altman
admin@altmanaz.com
Patricia Gitre
patgitre@patriciagitre.com
Counsel for M. Roman 017

Anne Chapman
anne@mscclaw.com
peggy@mscclaw.com
George Terwilliger III
George@gjt3law.com
Counsel for M. Meadows 018

/s/ Krista Wood

State v. Mark Meadows, et al.

CR2024-006850-018

EXHIBIT 1

CLERK OF THE SUPERIOR COURT
FILED
05-09-2024 12:20pm
A. Rowe, Deputy

SEARCH WARRANT

COUNTY OF MARICOPA, STATE OF ARIZONA

020330

No. SW 2024-~~002330~~

TO ANY PEACE OFFICER IN THE STATE OF ARIZONA

Proof by affidavit having been made this day to me by Special Agent William Knuth #460, a peace officer in the State of Arizona being first duly sworn, upon oath, deposes and says that there is probable cause to believe that:

IN/ON THE PROPERTY DESCRIBED AS:

Within the electronic data of Apple, headquartered at One Apple Park Way, Cupertino, CA 95014

IS NOW BEING POSSESSED OR CONCEALED CERTAIN PROPERTY OR THINGS DESCRIBED AS:

Regarding cellular account(s):

(480) 239-0025
(602) 292-5646
(623) 326-0578
(520) 405-7724
(928) 961-2973
(480) 285-7747
(714) 943-9983
(609) 529-9982
(619) 977-8100
(828) 506-9509
(202) 603-9094
(828) 200-2544
(928) 486-4220
(480) 980-7020
(713) 292-3207
(928) 486-4290
(347) 224-6792
(303) 720-9374
(202) 904-0334

1. All records or other information regarding the identification of the account, to include full name, subscriber names, user names, screen names, or other identities; mailing addresses, residential addresses, business addresses, email addresses, telephone numbers, and other contact information; billing records.
2. Electronic data stored on the device including locally stored and "cloud" stored data consisting of (1) call detail records; (2) instant messages, text/sms/mms/chat messages; (3) contact list; (4) emails; and, (5) geolocation information.
3. The information is being requested for the time periods between **November 1st, 2020 and February 1st, 2021**.
4. It is requested that a letter of authentication be provided with the records produced for the listed account(s).
5. It is requested that these records for the listed account(s) be provided in Arizona time UTC -7.

WHICH PROPERTY OR THINGS:

(x) Were used as a means for committing a public offense.
(x) Constitutes evidence tending to show that a public offense has been committed.

Such public offense(s) being investigated are:

A.R.S. § 13-2002; Forgery
A.R.S. § 13-2407; Tampering with a Public Record
A.R.S. § 39-161; Presentment of False Instrument for Filiing
A.R.S. § 13-2310; Fraudulent Schemes and Artifices
A.R.S. § 13-1003; Conspiracy
A.R.S. § 13-2311; Fraudulent Schemes and Practices
A.R.S. § 16-1006; Changing vote of an elector by corrupt means or inducement

You are therefore commanded in the [x] daytime [ ] or in the night according to A.R.S. §13-3917, to make a search of the above named or described person(s), premise(s), and vehicle(s) for the herein above described person(s), property or things, and if you find the same or any part thereof, to retain such in the custody of the Arizona Attorney General's Office, as provided by A.R.S. §13-3920.

You must execute this search warrant within five calendar days from its issuance and return to a magistrate within three court business days after the warrant is executed as directed by A.R.S. §13-3918.

This Search Warrant is sealed until otherwise ordered by this Court or another court of competent jurisdiction.

GIVEN UNDER MY HAND AND DATED THIS 9th day of May, 2024.

Judge of the Maricopa County Superior Court

State v. Mark Meadows, et al.

CR2024-006850-018

EXHIBIT 2

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:51:36 PM
Attachments:	image001.png

From: Wood, Krista
Sent: Monday, September 23, 2024 1:50 PM
To: Altman Law Office <admin@altmanaz.com>; Amanda Lauer <Amanda.Lauer@maricopa.gov>; Andrea Yirak <andrea@attorneysforfreedom.com>; Andrew Pacheco <APacheco@rrpklaw.com>; Andy Mercantel <Andy@attorneysforfreedom.com>; Anne Chapman <anne@mscclaw.com>; Ashley Adams <Aadams@azwhitecollarcrime.com>; Brad Miller Office <office@bradmiller.com>; Brian Gifford <briang@wb-law.com>; Chase Wortham <Chase@azwhitecollarcrime.com>; Danny Evans <Danny.Evans@maricopa.gov>; David Warrington (Dhillon Law) <DWarrington@dhillonlaw.com>; Dennis Wilenchik <diw@wb-law.com>; Emma Wittmann <Emma@attorneysforfreedom.com>; G Urbanek <gurbanek@dhillonlaw.com>; George Terwilliger III <George@gjt3law.com>; J Cloud <jcloud@jcloudlaw.com>; J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>; Jackson White Law <criminaldocket@jacksonwhitelaw.com>; Jennifer Zook <jzook@rrpklaw.com>; Josh Kolsrud <Josh@kolsrudlawoffices.com>; Kathy Brody <kathy@mscclaw.com>; Lacy Cooper <lacy@azbarristers.com>; Lee Stein <lee@mscclaw.com>; M Columbo <mcolumbo@dhillonlaw.com>; Mark Williams <markwilliamsesq@yahoo.com>; Matt Brown <matt@brownandlittlelaw.com>; Mike Bailey <MBailey@TullyBailey.com>; Moises Morales <Moises@attorneysforfreedom.com>; Patricia Gitre <patgitre@patriciagitre.com>; Peggy McClellan <peggy@mscclaw.com>; Richard Jones <Richard.Jones@maricopa.gov>; Steve Binhak <binhaks@binhaklaw.com>; Thomas Jacobs <tjacobs@jacobsazlaw.com>; Tim LaSota <tim@timlasota.com>; Wilenchik Law Firm <admin@wb-law.com>
Cc: Klingerman, Nicholas <Nicholas.Klingerman@azag.gov>; Hunley, Kimberly <Kimberly.Hunley@azag.gov>; Martinez, Gilda <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing

the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,
Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

State v. Mark Meadows, et al.

CR2024-006850-018

EXHIBIT 3

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:52:53 PM
Attachments:	image002.png image003.png

From: Anne M. Chapman <anne@mscclaw.com>
Sent: Wednesday, September 25, 2024 8:52 AM
To: Wood, Krista <Krista.Wood@azag.gov>
Cc: Peggy McClellan <peggy@mscclaw.com>; Brenda Studebaker <brenda@mscclaw.com>; Kathy Brody <kathy@mscclaw.com>
Subject: RE: State v. Ward et al; Cloud storage review

Thanks, Krista. At least initially, we will not elect to observe the processing of the files. Please send electronically to us directly.

Thank you
Anne

MITCHELL STEIN CAREY CHAPMAN PC
ATTORNEYS AT LAW

Anne M. Chapman
MITCHELL | STEIN | CAREY | CHAPMAN, PC
2600 North Central Avenue, Suite 1000
Phoenix, AZ 85004
anne@mscclaw.com

Chambers TOP RANKED USA 2024 Anne Chapman

Main: 602-358-0290
Fax: 602-358-0291
Direct: 602-388-1232
Mobile: 602-501-0239
www.mscclaw.com

From: Wood, Krista <Krista.Wood@azag.gov>
Sent: Monday, September 23, 2024 1:50 PM

To: Altman Law Office <admin@altmanaz.com>; Amanda Lauer <Amanda.Lauer@maricopa.gov>; Andrea Yirak <andrea@attorneysforfreedom.com>; Andrew Pacheco <APacheco@rrpklaw.com>; Andy Mercantel <Andy@attorneysforfreedom.com>; Anne M. Chapman <anne@mscclaw.com>; Ashley Adams <Aadams@azwhitecollarcrime.com>; Brad Miller Office <office@bradmiller.com>; Brian Gifford <briang@wb-law.com>; Chase Wortham <Chase@azwhitecollarcrime.com>; Danny Evans <Danny.Evans@maricopa.gov>; David Warrington (Dhillon Law) <DWarrington@dhillonlaw.com>; Dennis Wilenchik <diw@wb-law.com>; Emma Wittmann <Emma@attorneysforfreedom.com>; G Urbanek <gurbanek@dhillonlaw.com>; george@gjt3law.com; J Cloud <jcloud@jcloudlaw.com>; J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>; Jackson White Law <criminaldocket@jacksonwhitelaw.com>; Jennifer Zook <jzook@rrpklaw.com>; Josh Kolsrud <Josh@kolsrudlawoffices.com>; Kathy Brody <kathy@mscclaw.com>; Lacy Cooper <lacy@azbarristers.com>; Lee Stein <lee@mscclaw.com>; M Columbo <mcolumbo@dhillonlaw.com>; Mark Williams <markwilliamsesq@yahoo.com>; Matt Brown <matt@brownandlittlelaw.com>; Mike Bailey <MBailey@TullyBailey.com>; Moises Morales <Moises@attorneysforfreedom.com>; Patricia Gitre <patgitre@patriciagitre.com>; Peggy McClellan <peggy@mscclaw.com>; Richard Jones <Richard.Jones@maricopa.gov>; Steve Binhak <binhaks@binhaklaw.com>; Thomas Jacobs <tjacobs@jacobsazlaw.com>; Tim LaSota <tim@timlasota.com>; Wilenchik Law Firm <admin@wb-law.com>
Cc: Klingerman, Nicholas <Nicholas.Klingerman@azag.gov>; Hunley, Kimberly <Kimberly.Hunley@azag.gov>; Martinez, Gilda <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,
Krista

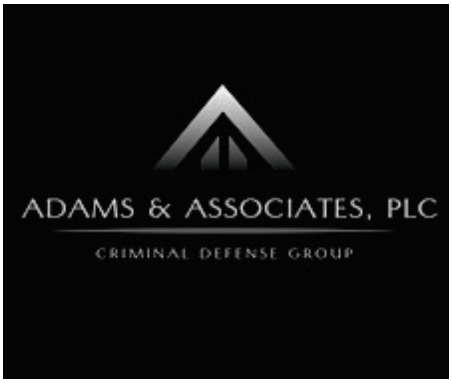
Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:52:12 PM
Attachments:	image001.png image002.png

From: Ashley Adams <aadams@azwhitecollarcrime.com>
Sent: Monday, September 23, 2024 5:06 PM
To: Wood, Krista <Krista.Wood@azag.gov>
Subject: Re: State v. Ward et al; Cloud storage review

Hi, Krista. We appreciate you sending us Mr. Eastman's e mails directly. We do not need to look over the State's shoulder. You have been very easy to work with, and we appreciate this.



7502 E. Monterey Way
Scottsdale, AZ 85251
Office: (480) 219-1366
Cell: (602) 524-3801
Facsimile: (480) 219-1451
aadams@azwhitecollarcrime.com
www.azwhitecollarcrime.com

From: "Wood, Krista" <Krista.Wood@azag.gov>
Date: Monday, September 23, 2024 at 1:50 PM
To: Altman Law Office <admin@altmanaz.com>, Amanda Lauer <Amanda.Lauer@maricopa.gov>, Andrea Yirak <andrea@attorneysforfreedom.com>, Andrew Pacheco <APacheco@rrpklaw.com>, Andy Mercantel <Andy@attorneysforfreedom.com>, Anne Chapman <anne@mscclaw.com>, Ashley Adams <aadams@azwhitecollarcrime.com>, Brad Miller Office <office@bradmiller.com>, Brian Gifford <briang@wb-law.com>, Chase Wortham <Chase@azwhitecollarcrime.com>, Danny Evans <Danny.Evans@maricopa.gov>,

"David Warrington (Dhillon Law)" <DWarrington@dhillonlaw.com>, Dennis Wilenchik <diw@wb-law.com>, Emma Wittmann <Emma@attorneysforfreedom.com>, G Urbanek <gurbanek@dhillonlaw.com>, George Terwilliger III <George@gjt3law.com>, J Cloud <jcloud@jcloudlaw.com>, J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>, Jackson White Law <criminaldocket@jacksonwhitelaw.com>, Jennifer Zook <jzook@rrpklaw.com>, Josh Kolsrud <Josh@kolsrudlawoffices.com>, Kathy Brody <kathy@mscclaw.com>, Lacy Cooper <lacy@azbarristers.com>, Lee Stein <lee@mscclaw.com>, M Columbo <mcolumbo@dhillonlaw.com>, Mark Williams <markwilliamsesq@yahoo.com>, Matt Brown <matt@brownandlittlelaw.com>, Mike Bailey <MBailey@TullyBailey.com>, Moises Morales <Moises@attorneysforfreedom.com>, Patricia Gitre <patgitre@patriciagitre.com>, Peggy McClellan <peggy@mscclaw.com>, Richard Jones <Richard.Jones@maricopa.gov>, Steve Binhak <binhaks@binhaklaw.com>, Thomas Jacobs <tjacobs@jacobsazlaw.com>, Tim LaSota <tim@timlasota.com>, Wilenchik Law Firm <admin@wb-law.com>
Cc: "Klingerman, Nicholas" <Nicholas.Klingerman@azag.gov>, "Hunley, Kimberly" <Kimberly.Hunley@azag.gov>, "Martinez, Gilda" <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,

Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:53:52 PM
Attachments:	image001.png

From: admin altman <admin@altmanaz.com>
Sent: Wednesday, September 25, 2024 3:16 PM
To: Wood, Krista <Krista.Wood@azag.gov>
Cc: Kurt Altman <kurt@altmanaz.com>; Ashley Fitzwilliams <ashley@altmanaz.com>; Patricia Gitre <patgitre@patriciagitre.com>
Subject: Re: State v. Ward et al; Cloud storage review

Hi Krista,

We'll forgo a field trip to your office…this time. Please separate out our client's information and provide us a copy.

Thanks,
Ashley

ALTMAN LAW & POLICY
12621 N. Tatum Blvd., #102
Phoenix, AZ 85032
admin@altmanaz.com
www.altmanaz.com

> On Sep 23, 2024, at 1:50 PM, Wood, Krista <Krista.Wood@azag.gov> wrote:
>
> Good morning,
>
> As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.
>
> Now that all subjects of the search warrants are represented by counsel, as we advised

previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,
Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:52:53 PM
Attachments:	image002.png image003.png

From: Anne M. Chapman <anne@mscclaw.com>
Sent: Wednesday, September 25, 2024 8:52 AM
To: Wood, Krista <Krista.Wood@azag.gov>
Cc: Peggy McClellan <peggy@mscclaw.com>; Brenda Studebaker <brenda@mscclaw.com>; Kathy Brody <kathy@mscclaw.com>
Subject: RE: State v. Ward et al; Cloud storage review

Thanks, Krista. At least initially, we will not elect to observe the processing of the files. Please send electronically to us directly.

Thank you
Anne

MITCHELL STEIN CAREY CHAPMAN PC
ATTORNEYS AT LAW

Anne M. Chapman
MITCHELL | STEIN | CAREY | CHAPMAN, PC
2600 North Central Avenue, Suite 1000
Phoenix, AZ 85004
anne@mscclaw.com

Chambers TOP RANKED USA 2024 Anne Chapman

Main: 602-358-0290
Fax: 602-358-0291
Direct: 602-388-1232
Mobile: 602-501-0239
www.mscclaw.com

From: Wood, Krista <Krista.Wood@azag.gov>
Sent: Monday, September 23, 2024 1:50 PM

To: Altman Law Office <admin@altmanaz.com>; Amanda Lauer <Amanda.Lauer@maricopa.gov>; Andrea Yirak <andrea@attorneysforfreedom.com>; Andrew Pacheco <APacheco@rrpklaw.com>; Andy Mercantel <Andy@attorneysforfreedom.com>; Anne M. Chapman <anne@mscclaw.com>; Ashley Adams <Aadams@azwhitecollarcrime.com>; Brad Miller Office <office@bradmiller.com>; Brian Gifford <briang@wb-law.com>; Chase Wortham <Chase@azwhitecollarcrime.com>; Danny Evans <Danny.Evans@maricopa.gov>; David Warrington (Dhillon Law) <DWarrington@dhillonlaw.com>; Dennis Wilenchik <diw@wb-law.com>; Emma Wittmann <Emma@attorneysforfreedom.com>; G Urbanek <gurbanek@dhillonlaw.com>; george@gjt3law.com; J Cloud <jcloud@jcloudlaw.com>; J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>; Jackson White Law <criminaldocket@jacksonwhitelaw.com>; Jennifer Zook <jzook@rrpklaw.com>; Josh Kolsrud <Josh@kolsrudlawoffices.com>; Kathy Brody <kathy@mscclaw.com>; Lacy Cooper <lacy@azbarristers.com>; Lee Stein <lee@mscclaw.com>; M Columbo <mcolumbo@dhillonlaw.com>; Mark Williams <markwilliamsesq@yahoo.com>; Matt Brown <matt@brownandlittlelaw.com>; Mike Bailey <MBailey@TullyBailey.com>; Moises Morales <Moises@attorneysforfreedom.com>; Patricia Gitre <patgitre@patriciagitre.com>; Peggy McClellan <peggy@mscclaw.com>; Richard Jones <Richard.Jones@maricopa.gov>; Steve Binhak <binhaks@binhaklaw.com>; Thomas Jacobs <tjacobs@jacobsazlaw.com>; Tim LaSota <tim@timlasota.com>; Wilenchik Law Firm <admin@wb-law.com>
Cc: Klingerman, Nicholas <Nicholas.Klingerman@azag.gov>; Hunley, Kimberly <Kimberly.Hunley@azag.gov>; Martinez, Gilda <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,
Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:56:43 PM
Attachments:	image924155.png image567033.png

From: Dennis Wilenchik <diw@wb-law.com>
Sent: Thursday, October 10, 2024 12:32 PM
To: Wood, Krista <Krista.Wood@azag.gov>; 'Lacy A. N. Cooper' <Lacy@azbarristers.com>
Subject: RE: State v. Ward et al; Cloud storage review

Thanks- look forward to seeing it

Sincerely Yours,

WILENCHIK & BARTNESS
ATTORNEYS AT LAW
A PROFESSIONAL CORPORATION FOUNDED IN 1991

www.wb-law.com

Dennis I. Wilenchik
Attorney at Law
diw@wb-law.com

The Wilenchik & Bartness Building
2810 North Third Street
Phoenix, Arizona 85004
P 602-606-2810 | F 602-606-2811

From: Wood, Krista <Krista.Wood@azag.gov>
Sent: Thursday, October 10, 2024 11:08 AM
To: 'Lacy A. N. Cooper' <Lacy@azbarristers.com>
Cc: Dennis Wilenchik <diw@wb-law.com>
Subject: RE: State v. Ward et al; Cloud storage review

Hi Lacy,

We also have:

1. SW2024-020292 regarding Twitter @jim_lamon
2. SW2024-020329 regarding Google Cloud – I believe that was provided to you this morning
3. SW2024-020330 regarding Apple Cloud – this information (if any exists for your client) should be provided by tomorrow (hopefully today).

If there's anything additional you need, please let me know.

Sincerely,
Krista

From: Lacy A. N. Cooper [mailto:Lacy@azbarristers.com]
Sent: Thursday, October 10, 2024 9:37 AM
To: Wood, Krista
Cc: Dennis Wilenchik
Subject: Re: State v. Ward et al; Cloud storage review

Hi Krista,

My understanding is that the only search warrant materials that purportedly belong to our client, Jim Lamon, are the records/emails associated with the email account jimlamon1@gmail.com, which were obtained pursuant to search warrant # SW2024-020310. Can you please confirm?

I also understand from your email that these materials are contained in their own separate subfolder within the production made by Google. If this is correct, please provide the subfolder at your convenience. We do not need to be present to view you copying the subfolder for disclosure to us.

Thank you,

Lacy

SCHMITT SCHNECK
EVEN & WILLIAMS, P.C.
Lacy Cooper | Director
1221 East Osborn Road, Suite 105 | Phoenix, AZ 85014-5540
Office: (602) 277-7000 | Cell: (480) 980-6413
Email: lacy@azbarristers.com | Website: www.azbarristers.com

On Sep 23, 2024, at 1:50 PM, Wood, Krista <Krista.Wood@azag.gov> wrote:

Good morning,
As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses. Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.
Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.
If you have any questions, or would like to discuss further, please let me know.
Sincerely, Krista Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section
<image001.png>Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From: Wood, Krista
To: "Thomas F. Jacobs"
Cc: Hunley, Kimberly
Subject: RE: State v. Ward et al; Cloud storage review
Date: Tuesday, December 03, 2024 3:53:40 PM
Attachments: image001.png

From: Thomas F. Jacobs <tjacobs@jacobsazlaw.com>
Sent: Wednesday, September 25, 2024 1:26 PM
To: Wood, Krista <Krista.Wood@azag.gov>
Subject: Re: State v. Ward et al; Cloud storage review

Krista:

With respect to Christina Bobb, please forward the separated material for our client and we will examine it and report confidential/privilege issues.

Thomas Jacobs
271 North Stone Avenue
Tucson, AZ 85701
(520) 628-1622 (o)
(520) 907-8659 (c)

****

****

From: Wood, Krista <Krista.Wood@azag.gov>
Sent: Monday, September 23, 2024 1:50 PM
To: Altman Law Office <admin@altmanaz.com>; Amanda Lauer <Amanda.Lauer@maricopa.gov>; Andrea Yirak <andrea@attorneysforfreedom.com>; Andrew Pacheco <APacheco@rrpklaw.com>; Andy Mercantel <Andy@attorneysforfreedom.com>; Anne Chapman <anne@mscclaw.com>; Ashley Adams <Aadams@azwhitecollarcrime.com>; Brad Miller Office <office@bradmiller.com>; Brian

Gifford <briang@wb-law.com>; Chase Wortham <Chase@azwhitecollarcrime.com>; Danny Evans <Danny.Evans@maricopa.gov>; David Warrington (Dhillon Law) <DWarrington@dhillonlaw.com>; Dennis Wilenchik <diw@wb-law.com>; Emma Wittmann <Emma@attorneysforfreedom.com>; G Urbanek <gurbanek@dhillonlaw.com>; George Terwilliger III <George@gjt3law.com>; J Cloud <jcloud@jcloudlaw.com>; J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>; Jackson White Law <criminaldocket@jacksonwhitelaw.com>; Jennifer Zook <jzook@rrpklaw.com>; Josh Kolsrud <Josh@kolsrudlawoffices.com>; Kathy Brody <kathy@mscclaw.com>; Lacy Cooper <lacy@azbarristers.com>; Lee Stein <lee@mscclaw.com>; M Columbo <mcolumbo@dhillonlaw.com>; Mark Williams <markwilliamsesq@yahoo.com>; Matt Brown <matt@brownandlittlelaw.com>; Mike Bailey <MBailey@TullyBailey.com>; Moises Morales <Moises@attorneysforfreedom.com>; Patricia Gitre <patgitre@patriciagitre.com>; Peggy McClellan <peggy@mscclaw.com>; Richard Jones <Richard.Jones@maricopa.gov>; Steve Binhak <binhaks@binhaklaw.com>; Thomas F. Jacobs <tjacobs@jacobsazlaw.com>; Tim LaSota <tim@timlasota.com>; Wilenchik Law Firm <admin@wb-law.com>
Cc: Klingerman, Nicholas <Nicholas.Klingerman@azag.gov>; Hunley, Kimberly <Kimberly.Hunley@azag.gov>; Martinez, Gilda <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,

Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov

From:	Wood, Krista
To:	Hunley, Kimberly
Subject:	FW: State v. Ward et al; Cloud storage review
Date:	Tuesday, December 03, 2024 3:52:00 PM
Attachments:	image001.png

From: Richard Jones (OPD) <Richard.Jones@Maricopa.Gov>
Sent: Monday, September 23, 2024 2:01 PM
To: Wood, Krista <Krista.Wood@azag.gov>
Subject: RE: State v. Ward et al; Cloud storage review

If you'll just send me Mr. Safsten's (#010) subfolder, I'd appreciate it.

Thanks,
Richard Jones
Deputy Public Defender

From: Wood, Krista <Krista.Wood@azag.gov>
Sent: Monday, September 23, 2024 1:50 PM
To: Altman Law Office <admin@altmanaz.com>; Amanda Lauer (OLD) <Amanda.Lauer@maricopa.gov>; Andrea Yirak <andrea@attorneysforfreedom.com>; Andrew Pacheco <APacheco@rrpklaw.com>; Andy Mercantel <Andy@attorneysforfreedom.com>; Anne Chapman <anne@mscclaw.com>; Ashley Adams <Aadams@azwhitecollarcrime.com>; Brad Miller Office <office@bradmiller.com>; Brian Gifford <briang@wb-law.com>; Chase Wortham <Chase@azwhitecollarcrime.com>; Danny Evans (OLD) <Danny.Evans@maricopa.gov>; David Warrington (Dhillon Law) <DWarrington@dhillonlaw.com>; Dennis Wilenchik <diw@wb-law.com>; Emma Wittmann <Emma@attorneysforfreedom.com>; G Urbanek <gurbanek@dhillonlaw.com>; George Terwilliger III <George@gjt3law.com>; J Cloud <jcloud@jcloudlaw.com>; J Franklin-Murdock <jfranklin-murdock@dhillonlaw.com>; Jackson White Law <criminaldocket@jacksonwhitelaw.com>; Jennifer Zook <jzook@rrpklaw.com>; Josh Kolsrud <Josh@kolsrudlawoffices.com>; Kathy Brody <kathy@mscclaw.com>; Lacy Cooper <lacy@azbarristers.com>; Lee Stein <lee@mscclaw.com>; M Columbo <mcolumbo@dhillonlaw.com>; Mark Williams <markwilliamsesq@yahoo.com>; Matt Brown <matt@brownandlittlelaw.com>; Mike Bailey <MBailey@TullyBailey.com>; Moises Morales <Moises@attorneysforfreedom.com>; Patricia Gitre <patgitre@patriciagitre.com>; Peggy McClellan <peggy@mscclaw.com>; Richard Jones (OPD) <Richard.Jones@Maricopa.Gov>; Steve Binhak <binhaks@binhaklaw.com>; Thomas Jacobs <tjacobs@jacobsazlaw.com>; Tim LaSota <tim@timlasota.com>; Wilenchik Law Firm <admin@wb-law.com>
Cc: Klingerman, Nicholas <Nicholas.Klingerman@azag.gov>; Hunley, Kimberly <Kimberly.Hunley@azag.gov>; Martinez, Gilda <Gilda.Martinez@azag.gov>
Subject: State v. Ward et al; Cloud storage review

Good morning,

As we have previously discussed, we have received court authorization for a search warrant, signed by Judge Kreamer, of information related to your clients' cloud storage on either Google or Apple. The providers have given us responses pursuant to the court authorized search warrants; however, we have not reviewed those responses because of possible privileged information, including anything subject to attorney-client privilege, that may be present in the returned responses.

Now that all subjects of the search warrants are represented by counsel, as we advised previously, our intent is to provide you with your client's returned information so that you may review it for any privileged information. Judge Kreamer recently issued an order directing the State to provide this information and allow defense counsel the opportunity to review and identify any information subject to privilege. Once you have reviewed and identified any information you believe is subject to privilege, or should otherwise not be provided to the State, we would then have the opportunity to oppose that request. Ultimately, it will be up to Judge Kreamer to resolve any disputes.

Finally, I wanted to confirm with you the manner of providing this information to you. We have received a single response from Google and Apple that include all targets relevant to that provider. The provider sent a single file that includes sub-folders specific to each target. As far as providing you with the information, we can separate your client's information and provide you with a copy of the response specific to your client. Or, you can come to our office to view us separating the information specific to your client. Please advise at your earliest convenience, so that we may get this information to you.

If you have any questions, or would like to discuss further, please let me know.

Sincerely,
Krista

Krista Wood
Section Chief
Criminal Division – Fraud & Special Prosecutions Section

Arizona Attorney General Kris Mayes
2005 N. Central Ave., Phoenix, AZ 85004
Direct: 602-542-8425
Krista.Wood@azag.gov
http://www.azag.gov