

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 25-20165

Honorable David M. Lawson

MATTHEW WEISS,

Defendant.

OPINION AND ORDER DENYING MOTION FOR RECONSIDERATION

On July 1 of this year, the Court filed an opinion and order granting the defendant's motion to suppress evidence obtained from a search of certain electronic devices and denying his motion to suppress evidence obtained from his iCloud account. The government has appealed the decision on the first motion, and the defendant now seeks reconsideration of the denial of the other motion.

The Court held in its original opinion that a search warrant obtained by the FBI to obtain digital information could not provide an independent source for the evidence seized from the computers and cell phones, which previously had been seized under an unconstitutional warrant. However, that same federal search warrant properly supported the search and seize the defendant's iCloud files because it was not tainted by any law-enforcement misconduct related to those files. The state authorities had obtained a search warrant for the iCloud data that was cabined by specific date references, but Apple, Inc. produced files that had been created outside that date range. The Court determined that there was no evidence that law enforcement personnel reviewed any of the allegedly offending data before the FBI sought a separate federal search warrant for the iCloud data; even if the state authorities looked at data that preceded the authorized date range in the state search warrant, there was no evidence that the information prompted the FBI to obtain its own search warrant for the iCloud account; there was no evidence that the extra-date-range data were

material to the federal magistrate’s decision to issue the search warrant; and the production of iCloud data in response to the federal search warrant did not offend the Fourth Amendment.

Weiss argues in his motion for reconsideration that the Court was mistaken when it said there was no evidence that the University of Michigan Police Department reviewed iCloud data outside the scope of its warrant to Apple, Inc., and that the mistake was outcome determinative because the data produced under the federal search warrant was the fruit of an unconstitutional search. He is wrong on both counts. The opinion contained no “mistake,” since it accurately states that the parties had not adduced evidence showing that files were reviewed outside the date restrictions in the warrant. (Weiss says he has new evidence suggesting otherwise, but he did not present it with his original motion. More on that below.) Moreover, the paragraph of the opinion which contains the purported “mistake” goes on to explain that “*even assuming* that the UMPD reviewed data outside the scope of the warrant, the FBI’s subsequent search warrant — which contained no time limitations — would serve as an independent source of that data.” ECF No. 68, PageID.663 (emphasis added). Because there is no “mistake” and no misstatement that would change the prior ruling, the motion for reconsideration will be denied.

I.

The factual and procedural background of the charges against Weiss and his motions to suppress are set forth in several prior orders. *See generally* ECF No. 34, 68, 69. The history of the case as pertinent to the present motion is summarized briefly here.

In December 2022, the University of Michigan Information Technology Services department (UMITS) discovered unauthorized login attempts affecting several users’ accounts. The login attempts were connected to defendant Weiss, who was then a member of the University’s football coaching staff. The University of Michigan Police Department (UMPD) obtained

warrants on January 10, 2023 to seize several digital devices used by Weiss. The next day, on January 11, 2023, the UMPD obtained warrants authorizing a full forensic search of each of the devices. This Court later determined that the forensic search warrants were unconstitutionally overbroad because they contained no date limitation and did not direct officers to search for any specific category of evidence, thereby violating the Fourth Amendment's particularity requirement. ECF No. 68, PageID.639-42.

On January 20, 2023, the UMPD obtained another search warrant, this time directed to Apple, Inc. The warrant sought various data associated with defendant Weiss's Apple account, including "[a]ll iCloud data associated with any backups of iPhones associated with this account" and "all files, including photographs and videos, stored in iCloud or other server or Apple facilitated format" ECF No. 32-9, PageID.270. The iCloud warrant expressly was limited to "records, data, or information . . . between the dates of 08-29-2022 through 01-05-2023" and directed officers to search "for evidence of the crime of Unlawful Access to a Computer." *Ibid.* Apple produced data in response to the warrant on February 3, 2023. ECF No. 44-2, PageID.384. Its response warned that "certain files within the iCloud backup data may contain aggregated data where Apple was unable to apply a date filter." *Id.* at PageID.385.

True to that warning, the iCloud data Apple produced included files from beyond the warrant's specified timeframe, including photographs last modified in 2020. *See* ECF No. 54-1. Detective James Cargill of the UMPD stated in an email in 2025 that he reviewed and "tagged" 14 of the files returned from Apple, all of which were "sign on related screenshots." ECF No. 54-2, PageID.547. As discussed in greater detail below, documents provided to the Court after Weiss's motions to suppress were decided show that the files that Detective Cargill accessed were outside the date range of the UMPD's iCloud warrant.

The UMPD began to share information about its investigation with the FBI in February 2023. The FBI opened its own investigation into Weiss in early March 2023. On March 27, 2023, the FBI sought and obtained a federal warrant to search several of Weiss's digital devices. The search warrant also sought the files Apple previously produced in response to the UMPD's search warrant, described as "[t]he contents of an Apple, Inc. return, obtained pursuant to State of Michigan Search Warrant 2390300063(10), for the Apple user identified as Matthew Eric Weiss . . . between the dates of August 29, 2022, through January 5, 2023, contained on the CARGILL-CYBERCRIMES forensic computer, device ID D3BF44C5-1570-4773-8524-EFEF8182F4FB." ECF No. 32-7, PageID.257. Weiss asserts in the reply in support of his motion for reconsideration that the government later obtained a second federal warrant for his iCloud data, although he does not provide a copy of it or say where it can be found in the record. *See* ECF No. 78, PageID.786-87.

A federal grand jury indicted Weiss in March 2025 for multiple counts of unauthorized computer access in violation of 18 U.S.C. § 1030 and aggravated identity theft in violation of 18 U.S.C. § 1028A. Weiss moved to suppress the evidence obtained from his devices because the warrants authorizing the forensic searches of them were unconstitutionally overbroad. He also moved to suppress the iCloud data provided by Apple because the UMPD obtained data that exceeded the date range of the search warrant.

On July 1, 2026, the Court granted Weiss's motion to suppress evidence obtained from the electronic devices, finding that the UMPD's forensic search warrants violated the Fourth Amendment for lack of particularity and no exception to the exclusionary rule applied. However, it declined to suppress the iCloud evidence because (1) the evidence presented by the parties did not show that the UMPD exceeded the scope of the state warrant; and (2) even if the UMPD did

exceed the state warrant's scope, the later federal warrant acted as an independent source of the data. The operative language from that opinion reads:

The iCloud data that the government seeks to use against Weiss is not the product of an illegal search in the same way as the data stored on his devices. The only evidence clearly showing that law enforcement reviewed any of the iCloud data before the FBI sought its federal warrant is an email from Detective James Cargill of UMPD, which states that he reviewed and “tagged” 14 of the files returned from Apple. ECF No. 54-2, PageID.547. The parties have not shown that the 14 files were outside the temporal scope of the search warrant. And, to the extent that UMPD did exceed the scope of the warrant in its initial search, Weiss has not pointed to any evidence showing that UMPD's review of this handful of files was a substantial or motivating factor in the FBI's decision to open an investigation and apply for a federal warrant, and the application for a federal warrant does not include any evidence derived from Apple's production. In other words, there is no evidence that the 14 files that Detective Cargill “tagged” prompted the FBI's decision to seek a warrant or were material to the federal magistrate's decision to issue one. Therefore, even assuming that the UMPD reviewed data outside the scope of the warrant, the FBI's subsequent search warrant — which contained no time limitations — would serve as an independent source of that data. . . . The government's use of the iCloud data does not run afoul of the Fourth Amendment.

ECF No. 68, PageID.663.

Weiss filed a timely motion for reconsideration on July 15, 2026 and later supplemented the record on leave granted. The supplemental information shows that Detective Cargill accessed the files produced by Apple on three different days in February 2023, ECF No. 80-3, PageID.849, and “tagged” 14 files, each of which had a “Last Modified Date/Time” in March or April of 2020, ECF No. 80-2, PageID.837-48. (Weiss asserts that the documents were “tagged” twice, so the 14 tagged items actually represent seven unique files. ECF No. 80, PageID.802 n.2.) The results confirm that Cargill viewed files that were created or modified prior to August 29, 2022, the beginning of the date range provided in the UMPD's iCloud warrant. Therefore, the factual premise underlying Weiss's motion for reconsideration — that Cargill exceeded the scope of the warrant in his review — is correct. Still, the government opposes the motion for reconsideration

due to the lack of persuasive information that anything Cargill might have learned affected the FBI's decision to obtain a warrant to search the iCloud account.

II.

Under Eastern District of Michigan Local Rule 7.1(h), reconsideration of non-final orders may be granted only on limited grounds:

(A) The court made a mistake, correcting the mistake changes the outcome of the prior decision, and the mistake was based on the record and law before the court at the time of its prior decision;

(B) An intervening change in controlling law warrants a different outcome; or

(C) New facts warrant a different outcome and the new facts could not have been discovered with reasonable diligence before the prior decision.

E.D. Mich. LR 7.1(h)(2). “[A] motion for reconsideration is not properly used as a vehicle to re-hash old arguments or to advance positions that could have been argued earlier but were not.” *Smith ex rel. Smith v. Mount Pleasant Pub. Schs.*, 298 F. Supp. 2d 636, 637 (E.D. Mich. 2003) (citing *Sault Ste. Marie Tribe of Chippewa Indians v. Engler*, 146 F.3d 367, 374 (6th Cir. 1998) (construing Federal Rule of Civil Procedure 59(e))).

A.

Weiss argues that the Court made a “mistake” under LR 7.1(h)(2)(A) when it stated that the parties had not shown that the 14 files in Apple’s iCloud data production reviewed by UMPD Detective James Cargill were outside the temporal scope of the iCloud warrant. He points to an FBI memorandum, cited in the original briefing on the motion, in which FBI Special Agent Kelly Reller discussed her review of the contents of the Apple return (which was first produced to UMPD and later obtained by the FBI). The return, Weiss asserts, includes a single iCloud backup saved in a .zip file with a “creation time” of April 1, 2020, at 2:34 a.m. He observes that the backup would only have consisted of data predating its creation, meaning that every file in the backup

predated April 1, 2020. In other words, he argues, the *only* data that Apple produced, and the *only* data the UMPD would have seen during its initial review, was data from outside the scope of the iCloud warrant.

A “mistake” is “[a]n error, misconception, or misunderstanding; an erroneous belief.” *Mistake*, Black’s Law Dictionary (12th ed. 2024). The primary “mistake” Weiss identifies is the Court’s statement that “[t]he parties have not shown that the 14 files [tagged by Detective Cargill] were outside the temporal scope of the search warrant.” ECF No. 68, PageID.663. However, this statement accurately represents the state of the record as it existed at the time of the decision. Weiss’s original motion asserted that the UMPD ignored the date restriction on the iCloud warrant, discovered six images of screenshots taken in the year 2020, and found no evidence within the warrant’s date range. ECF No. 29, PageID.140. He asserted that the federal government used the screenshots to procure a second warrant. *Id.* at PageID.143. He did not cite any evidence substantiating these assertions. In his reply, Weiss provided two additional exhibits: an FBI “302” memorandum documenting Special Agent Reller’s review of the iCloud return on May 18, 2023, which included files last modified in 2020, ECF No. 54-1 (Exhibit A); and an email thread from late 2025 in which Detective Cargill acknowledged that he “look[ed] at and tagged 14 items” in the return, ECF No. 54-2, PageID.547 (Exhibit B). These two documents do not show that the UMPD reviewed files outside the scope of the warrant. At most, they show that (1) the UMPD reviewed an unspecified set of files, which might have been inside or outside the UMPD warrant’s date range; and (2) the FBI reviewed files from 2020 after obtaining its own warrant, which authorized the search of those files. Therefore, the Court did not make a mistake by concluding that the evidence in the record failed to establish that the UMPD exceeded the scope of the warrant.

In his motion for reconsideration, Weiss adds a crucial detail: that Apple produced *only one* iCloud backup, which was created in 2020. ECF No. 71, PageID.753. Therefore, *any* iCloud files that Cargill reviewed must have been outside the date range of the UMPD’s warrant. However, Weiss did not make this clear in his original briefing; he stated that “Apple improperly produced an iCloud back-up from April 1, 2020,” ECF No. 47, PageID.470, but he did not specify that this was the only backup that Apple produced to the UMPD. Weiss asserts in his motion for reconsideration that this was clear from the record because Agent Reller’s 302 memorandum describes a review of files from 2020, *see* ECF No. 54-1, but it is not stated on the face of Reller’s memorandum that Apple’s production comprised *solely* of a single backup from 2020. Although the files described in the memorandum were from a single .zip file, and all were last modified in 2020, the memorandum does not specify that Apple produced *only* a single .zip file or that the memorandum encompassed her entire review of Apple’s warrant return. Some additional evidence — or, at least, some additional explanation from counsel — was necessary to establish that the only material Apple produced was from 2020.

Relatedly, Weiss observes that Cargill’s email states that he viewed “sign on related screenshots,” ECF No. 54-2, PageID.547, and Reller’s memorandum also discusses screenshots of login screens. That Reller and Cargill reviewed files containing similar content does not necessarily establish that they were reviewing the same files, or that all the files came from before 2020. According to Weiss, the post-decision subpoena to the UMPD revealed that the six images referenced in Reller’s memorandum “are identical in name, creation date, and appearance” to the files tagged by Cargill. ECF No. 80, PageID.802. But that evidence was not before the Court at the time of decision. The Court was not mistaken in concluding that the evidence before it failed to show that Cargill reviewed files outside the scope of the UMPD’s warrant.

Weiss also argues that it was unnecessary to develop a record on this issue because the government failed to dispute his assertions that the UMPD exceeded the scope of the warrant when it obtained the iCloud files. But Weiss has not provided any authority showing that the Court was bound to accept as true his unsubstantiated (albeit undisputed) factual assertions. On the contrary, “[t]he burden of production . . . rests on the person seeking to suppress evidence.” *United States v. Smith*, 783 F.2d 648, 650 (6th Cir. 1986). The central factual premise of Weiss’s motion was that the UMPD disregarded the date limitations on the iCloud warrant. The Court did not make a mistake in observing that the evidence in the record did not substantiate this premise.

B.

Weiss asserts that correcting the Court’s “mistake” changes the outcome. The Court held that the federal warrant was an independent source of the iCloud files *even if* the UMPD exceeded the scope of the warrant in its initial review. But Weiss asserts that this conclusion was incorrect because the federal warrant was prompted by an unconstitutional search of Weiss’s devices, and the “prompting” analysis necessarily carries over to the iCloud files, requiring their exclusion as well. He also takes issue with the Court’s factual conclusion that the federal warrant was not prompted by the iCloud files because, according to Weiss, the federal government only elected to search certain data and devices possessed by the UMPD, creating the inference that the FBI knew what data would have evidentiary value beforehand.

As explained in the earlier opinion, the independent source rule states that the government must show both that “the initial illegal search did not prompt officers to seek a warrant for the second search,” *United States v. Williams*, 656 F. App’x 751, 753 (6th Cir. 2016) (citing *Murray v. United States*, 487 U.S. 533, 542 (1988)), and that “a neutral magistrate would have issued the search warrant even if she was not presented with the information obtained from the illegal search,”

ibid. (citing *United States v. Jenkins*, 396 F.3d 751, 761 (6th Cir. 2005)). Weiss does not question the second requirement, but he contends that the Court should have concluded that the information obtained from the UMPD's iCloud search warrant prompted the government to obtain its own search warrant for that data, which undermines the Court's independent source rationale. The Court disagrees.

1.

To start, these arguments are not properly presented on a motion for reconsideration because they "could have been argued earlier but were not." *Smith*, 298 F. Supp. 2d at 637. The government raised the independent source argument in substance (if not in name) when it asserted in its original briefing that the UMPD's purported disregard of the limitations of the first warrant was immaterial because the FBI searched the same files pursuant to its own federal warrant. ECF No. 44, PageID.369-74. Weiss's objections to applying the independent source doctrine were aired out in his reply brief in support of his motion to suppress the evidence obtained from his devices, ECF No. 49, PageID.484-89, which was expressly incorporated by reference in his reply regarding his motion to suppress the iCloud data, ECF No. 47, PageID.472 & n.1. And Weiss's reconsideration motion also does not point to any "law before the Court at the time of decision," E.D. Mich. LR 7.1(h)(2)(A), demonstrating that the Court's independent source analysis was incorrect. Nonetheless, the Court will address the merits of Weiss's new arguments.

2.

Weiss first challenges the factual basis of the Court's independent source rationale. His opening brief observes that the federal government elected to search certain devices and materials only based on their anticipated evidentiary value, which, he asserts, necessarily implies that the federal government knew what the UMPD had found before it sought the warrant. The

government, however, insists it did not know that the UMPD had reviewed the iCloud data at all until after it sought the warrant. This assertion is corroborated by a December 16, 2025 email from Agent Reller to Detective Cargill in which Reller inquired “whether or not UMPD ever decrypted and reviewed that Apple return prior to giving it to the FBI” because she did not “see any record of its review in the forensics report or the UMPD case file.” ECF No. 54-2, PageID.548. But it is not necessary to credit the government’s assertions because Weiss’s argument is unpersuasive on its own terms. As a matter of logic, the fact that the government chose *not* to search certain devices because they were *not* expected to contain relevant evidence does not mean that the government *did* choose to search certain devices because it *knew* that they *did* contain relevant evidence. Moreover, the basis of the government’s suspicion that the iCloud files might contain relevant evidence is laid out in in the search warrant affidavit, which does not mention the return Apple made on the UMPD warrant.

Weiss’s reply points to several more items of evidence that, he asserts, show that the federal government’s decision to seek a warrant was prompted by what it or the UMPD discovered in the iCloud data. Weiss first points to Agent Reller’s notes of her conversation with Detective Cargill on February 17, 2023. *See* ECF No. 58-3. The last page contains notations stating, “Follow up on ATS” and “ATS system.” *Id.* at PageID.590. Weiss suggests that the “ATS” notation refers to institutional victim Keffer Development Services’ Athletic Training System. The government has stated in earlier briefing that “the results of the UMPD warrant for Weiss’s iCloud data . . . linked Weiss to an intrusion of the Athletic Training System.” ECF No. 32, PageID.178. He also points to an email from Reller on March 3, 2023 asking how the iCloud return was stored, ECF No. 49-8, PageID.510, and some post-warrant communications and a memorandum from April and May of 2023 regarding Apple’s production, ECF No. 79-1 through 4. (The exhibits filed in ECF No.

79 were submitted to the Court after its decision, so they should not be considered for the purpose of E.D. Mich. LR 7.1(h)(2)(A). But because they could be considered as “new facts” under subsection (C) of the same rule, which Weiss invokes in the alternative, the Court will consider these new exhibits together with the other evidence Weiss relies on for the sake of consolidating the discussion in one section.).

Agent Reller’s “ATS” notations are the most helpful for Weiss’s argument. The reference to “ATS” in her notes dated February 17, 2023, combined with the government’s statement that Weiss was linked to the breach of the Athletic Training System through the use of the iCloud data, suggest that some information about what was contained in the iCloud backup made its way to the FBI before the federal government sought a search warrant. The government has not explained where Cargill’s information about ATS could have come from, other than through the iCloud files (although the government did not have an opportunity to address this point because Weiss brought it up for the first time in the reply brief in support of his motion for reconsideration). But even accepting for the sake of argument that Cargill’s information about ATS that he relayed to Reller was derived from the iCloud data, Weiss has not shown that it had any effect on the FBI’s decision to seek a federal warrant. Notably, Reller’s request to open an FBI investigation, prepared a month later, features a summary of the evidence found on Weiss’s devices and the suspected crimes, but it does not include any discussion of Keffer or the ATS breach. ECF No. 58-5. The two references to “ATS” also are miniscule compared to the volume of information the UMPD and the FBI shared regarding the results of the devices searches, detailed in the original opinion and order, ECF No. 68, PageID.626-28, 649-50, which served as the basis of the Court’s conclusion that the device searches prompted the federal warrant to search the devices. Although the federal government

might have had information about ATS, the record does not suggest that the FBI opened an investigation or sought a warrant *because of* that information.

The other documents cited in Weiss’s reply do not change this conclusion. Reller’s March 6, 2023 email asking about where the Apple data was stored, ECF No. 49-8, PageID.510, establishes at most that the FBI knew about the existence of the iCloud return — not that the FBI knew what information was contained within it or that this information influenced its decision to seek a federal warrant to search the iCloud account *or* the devices. And the emails and memorandum submitted as supplemental exhibits, *see* ECF No. 79, all postdate the FBI’s federal search warrant and do not discuss the substantive content of the files produced by Apple.

3.

Next, Weiss challenges the legal basis of the Court’s independent source rationale. He asserts that the federal search warrant could not be an independent source of the iCloud data because, as the Court found, the federal warrant was prompted by an unconstitutional search of the devices. However, he does not provide any authority for the proposition that an otherwise valid warrant to search one thing cannot serve as an independent source of evidence because the warrant was prompted by a *separate* unlawful search of something else. Although the independent source doctrine sometimes is described as applying to “evidence that has been discovered by means wholly independent of *any* constitutional violation,” *Nix v. Williams*, 467 U.S. 431, 443 (1984) (emphasis added), the Supreme Court’s cases applying the doctrine have focused on the causal connection between the unconstitutional search that uncovered the challenged evidence and the purportedly independent source of the evidence. For instance, the Supreme Court held that a warrant was an independent source of evidence discovered in a defendant’s apartment when it was not “derived from or related in any way to the initial entry” and “[n]o information obtained during

the initial entry or occupation of the apartment was needed or used by the agents to secure the warrant.” *Segura v. United States*, 468 U.S. 796, 814 (1984). This conclusion found support in the Court’s prior cases holding that “evidence will not be excluded as ‘fruit’ unless the illegality is at least the ‘but for’ cause of the discovery of the evidence.” *Id.* at 815 (citing *Brown v. Illinois*, 422 U.S. 590, 599 (1975) (identifying the relevant question as whether “the evidence to which instant objection is made has been come at by exploitation of [a prior] illegality or instead by means sufficiently distinguishable to be purged of the primary taint” (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963))). Similarly, *Murray* stated that a warrant would not be “a genuinely independent source of the information and tangible evidence at issue here . . . if the agents’ decision to seek the warrant was prompted by what they had seen during the initial [unlawful] entry, or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant.” 487 U.S. at 542. But if knowledge of contraband “was not the result of the earlier [illegal] entry there is no reason why the independent source doctrine should not apply.” *Id.* at 541.

In line with these cases, the Court held that the federal search warrant was an independent source of the iCloud files because it did not result from Detective Cargill’s alleged search of those files; the files did not prompt the FBI’s decision to seek a warrant for the iCloud files, and they were not presented to the magistrate judge before he signed the search warrant. Although *Murray* supports the notion that a warrant cannot serve as an independent source of evidence derived from a prior unlawful search if the warrant was prompted by that same evidence, it does not hold that the “prompting” exception to the inevitable discovery rule extends to evidence unrelated to what was found in the search that prompted the later warrant. So, although the federal warrant to search the devices could not serve as an independent source of the evidence derived from the state’s

device searches that prompted the government to procure it, it does not follow that the federal warrant to search the iCloud account is ineligible as to serve as an independent source of evidence that originated elsewhere. This is consistent with *Segura*'s statement that "evidence will not be excluded as 'fruit' unless the illegality is at least the 'but for' cause of the discovery of the evidence." 468 U.S. at 815. Since Detective Cargill's search of the iCloud files cannot be said to be the "but for" cause of the federal search warrant, the iCloud evidence need not be suppressed where it was searched independently through that warrant.

4.

Weiss also takes issue with the Court's characterization of the FBI's warrant as having "no time limitations." See ECF No. 68, PageID.663. He says that there actually were "*two different* federal warrants that covered the iCloud data," only one of them had an effectively unlimited date range, and the government's independent source argument in the initial briefing only relied on the date-limited version. ECF No. 78, PageID.786 & n.1. The upshot of this point is that the FBI's warrant could not serve as an independent source of the iCloud data outside of the UMPD's warrant's date restrictions because the FBI warrant *itself* had the same date restrictions.

Weiss does not say where this second warrant can be found in the record (if it can be found at all). More to the point, the existence of a second warrant for the iCloud data would not help his argument; the Court's supposed reliance on a warrant for the iCloud data that *does* contain date limitations would be a harmless error that does not change the result if there were a second warrant for the same data that *did not* contain date limitations.

All told, though, Weiss's premise that the federal warrant the Court relied on for the independent source theory had date limitations is defective. Weiss locates the purported date restriction in a description of the iCloud data provided in the federal search warrant: "[t]he contents

of an Apple, Inc. return, obtained pursuant to State of Michigan Search Warrant 2390300063(10), for the Apple user identified as Matthew Eric Weiss [contact information redacted] *between the dates of August 29, 2022, through January 5, 2023*, contained on the CARGILL-CYBERCRIMES forensic computer” ECF No. 32-7, PageID.215 (emphasis added). Read in context, the dates are included for the purpose of describing the warrant through which the Apple return was obtained, rather than to limit the scope of the FBI’s search. Furthermore, the government specifically argued in the initial briefing that “the federal warrant authorized the search of the data produced by Apple without any date restriction,” ECF No. 44, PageID.371, and Weiss did not dispute this characterization in his reply to the original motion response. Only in a reply brief in support of a motion for reconsideration did Weiss raise this issue. Even if Weiss’s characterization were accurate (it is not), it is far too late at this point to bring this issue before the Court.

* * *

Weiss has not shown that the Court made a mistake in its analysis or that the purported mistake made a difference to the result. The motion for reconsideration relying on Local Rule 7.1(h)(2)(A) will be denied.

C.

Finally, Weiss cites subsection (C) of LR 7.1(h)(2), which allows reconsideration if the movant advances “new facts” that would cause a “different outcome,” provided the new facts “could not have been discovered with reasonable diligence” during the initial go round. The new facts that he relies on come from a subpoena return from the UMPD confirming that Detective Cargill reviewed files outside the date range of the UMPD’s warrant.

Weiss gets the benefit of the doubt on the “reasonable diligence” part. He asserts that the federal government refused or was unable to provide the UMPD records because they were not in

the federal government’s possession or control, and “[r]easonable diligence does not require a defendant to subpoena law enforcement for records of the investigation against him.” ECF No. 71, PageID.758. The government does not dispute Weiss’s characterization of what reasonable diligence required in this situation, and the Court concludes that he has satisfied that component of subsection (C).

However, for the reasons stated above, the new facts identified by Weiss do not require — or even justify — a different outcome. The Court stated in its opinion and order that the independent source doctrine would permit the admission of the iCloud data *even if* Cargill had exceeded the scope of the warrant. For the reasons discussed earlier, the independent source holding was correct. The result therefore would not change even if the Court had access to the UMPD subpoena materials before making its decision.

III.

Weiss has not shown that the Court made a mistake in its earlier decision to deny his motion to suppress the fruits of the warrant to search his iCloud account based on the record before it. Nor has he shown that a different result is justified even if his factual premise is accepted, or that new facts require a different result.

Accordingly, the motion for reconsideration (ECF No. 71) is **DENIED**.

s/David M. Lawson
DAVID M. LAWSON
United States District Judge

Date: October 13, 2026