

This opinion is subject to revision before publication.

**UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES**

UNITED STATES
Appellee

v.

Kenneth P. ARMOUR II, Senior Airman
United States Air Force, Appellant

No. 26-0116
Crim. App. No. 2025-10

Argued April 28, 2026—Decided August 24, 2026

Military Judges: Nathan R. Allred (Article 30a, UCMJ,
proceedings) and Ryan D. Brunson (arraignment
and pretrial motions)

For Appellant: *Captain John M. Fredericks* (argued);
Lieutenant Colonel Allen S. Abrams.

For Appellee: *Major Kate E. Lee* (argued); *Colonel*
Matthew D. Talcott and *Mary Ellen Payne, Esq.*

Judge JOHNSON delivered the opinion of the Court,
in which Chief Judge MAGGS, Judge OHLSON,
Judge SPARKS, and Judge HARDY joined.

Judge JOHNSON delivered the opinion of the Court.

This case arises from an interlocutory appeal under Article 62, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 862 (2024), in a pending court-martial. Appellant¹ was charged with two specifications of conspiracy to distribute child pornography, in violation of Article 81, UCMJ, 10 U.S.C. § 881 (2018), and one specification each of possession, viewing, receipt, and distribution of child pornography, in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2018).

The military judge granted a motion to suppress the search of Appellant’s electronic devices for evidence of child sexual abuse material (CSAM). After the Government executed a new search authorization for the devices, the military judge granted a second motion to suppress. The military judge found the new search was not genuinely independent of the prior unlawful search because the Government had retained continuous possession of the previously seized devices, effectively freezing the probable cause that otherwise would have grown stale.

On the Government’s interlocutory appeal, the AFCCA held that the military judge abused his discretion by suppressing evidence based upon an erroneous view of the independent source doctrine. *United States v. Armour*, 86 M.J. 515, 518 (A.F. Ct. Crim. App. 2025). Accordingly, the AFCCA vacated the military judge’s second suppression ruling. *Id.* at 526.

We granted review to determine “[w]hether this Court should affirm the military judge’s suppression ruling because information gained from multiple unlawful searches affected law enforcement agents’ decision to seek a search authorization and the search authority’s decision to grant it.” *United States v. Armour*, __ M.J. __ (C.A.A.F. 2026)

¹ Although Senior Airman Armour was the appellee at the United States Air Force Court of Criminal Appeals (AFCCA), this opinion refers to him as Appellant, his role in the appeal to this Court.

(order granting review). For the reasons set forth below, we answer the granted issue in the negative and affirm the decision of the AFCCA.

I. Background

On August 1, 2021, the National Center for Missing and Exploited Children (NCMEC) published a report that a Kik messaging application account with the username “after-matter” had uploaded and shared files containing CSAM. NCMEC reported that “aftermatter” logged in from four different internet protocol (IP) addresses and uploaded CSAM from three others. One of those seven IP addresses was traced to a physical address in Dalzell, South Carolina, with an internet connection serviced by Charter Spectrum (the Spectrum IP address).² The NCMEC report stated that the Spectrum IP address was associated with a “suspect login” to the “aftermatter” account but did not link it to the upload or transmission of suspected CSAM.

Sumter County, South Carolina Sheriff’s Office (SCSO) Investigator (Inv) KF obtained a warrant for subscriber information associated with the Spectrum IP address. The warrant indicated that the Spectrum IP address was registered to BB at a residence in Dalzell, South Carolina (the Dalzell address). Upon learning that BB was a member of the Air Force, Inv KF contacted the Air Force Office of Special Investigations (OSI), which opened a parallel investigation.

A. The January search

In January 2022, Inv KF obtained a warrant to search the Dalzell address and seize electronic devices. Although the Spectrum IP address had not been linked to any upload or transmission of CSAM, the supporting affidavit stated that Inv KF had viewed media from the Spectrum IP address and confirmed it to be CSAM. The affidavit did not

² The physical locations of the other IP addresses, including the addresses used to upload CSAM, were masked by the use of virtual private networks.

mention any of the other IP addresses associated with the “aftermatter” account.

While executing the search, Inv KF observed mail addressed to Appellant at the Dalzell address. A subsequent search of the South Carolina Division of Motor Vehicles (DMV) database confirmed that both Appellant and BB resided at the Dalzell address.

B. The February search

Because Appellant was then deployed overseas, OSI requested authorization to search Appellant and his deployed residence. Supporting affidavits stated that Inv KF had informed OSI that the Spectrum IP address was used to upload CSAM; the Spectrum IP address was registered to BB at the Dalzell address; packages addressed to Appellant were discovered at the Dalzell address; and a search of the DMV database verified Appellant and BB resided at the Dalzell address. The affidavits stated that Inv KF reviewed media files uploaded via the Spectrum IP address which depicted CSAM. The affidavits did not mention any of the IP addresses that Kik had identified as associated with CSAM and were silent as to the dates Appellant physically resided at the Dalzell address.

On February 10, 2022, OSI searched Appellant and his deployed residence for evidence of CSAM, seizing an iPhone, an iPad, two laptops, and an SD card. OSI turned the seized devices over to SCSO. However, after a state magistrate judge denied SCSO’s application for a warrant to search them, SCSO notified OSI it would not move forward with the prosecution and returned the devices to OSI.

In July 2023, OSI took over the investigation. The Department of Defense Cyber Crime Center (DC3) analyzed the seized devices and discovered evidence of possession, viewing, receipt, and distribution of CSAM on the iPhone and iPad.

C. The first motion to suppress

The defense moved to suppress evidence recovered as a result of the February search. The defense argued that

there was no probable cause because there was no nexus between the reported CSAM and BB, Appellant, or the places and items searched. The defense also argued that even if there was a substantial basis to support a finding of probable cause, the evidence should be excluded because the supporting affidavits were written with reckless disregard for the truth.

The military judge granted the motion, finding the February OSI affidavits “included a false statement and were written with a reckless disregard for the truth.” According to the military judge, “even a cursory review of the NCMEC report makes quite apparent” that the Spectrum IP address was not associated with any upload of CSAM. The military judge found that while Inv KF’s affidavit in support of the January search was not intentionally false, “she recklessly disregarded the truth with respect to the assertion that the uploads of suspect CSAM were ‘from’ or ‘via’ the [Spectrum IP] address.” Further, he found that OSI “demonstrated a reckless disregard for the truth by relying on the unsupported assertion of [Inv KF] even while OSI possessed, and the lead case agent had reviewed, the original NCMEC report, which plainly shows that [Inv KF’s] assertions were factually untrue.”

The military judge held that the Government failed to show the remaining statements in the affidavit established probable cause. Declining to apply the inevitable discovery exception and good faith exception to the exclusionary rule, he granted the motion to suppress the February seizure and subsequent searches of Appellant’s devices. The military judge denied the Government’s motion for reconsideration but granted the Government a continuance to seek a new search authorization for the seized devices.

D. The March search

On March 24, 2025, OSI submitted a new affidavit in support of a request for search authorization for the devices seized in the February search. Among other things, the March affidavit described the SCSO warrant for Spectrum subscriber information and the response; the January 2022

search of the Dalzell address revealing packages addressed to Appellant at that address; and the DMV database search that verified Appellant resided there. The affidavit stated that Appellant resided at the Dalzell address at the time of the NCMEC CyberTipline reported activity and deployed in October 2021, three months after the last reported activity. The affidavit explained why the “aftermatter” login from the Spectrum IP address gave investigators reason to believe Appellant’s devices would contain CSAM: “Because [Appellant] shared the residence at [BB’s Dalzell address] with then-Senior Airman [BB] during the time period of the CSAM uploads described in the NCMEC CyberTipline Report, there is reason to believe he had access to the residential Internet connection” when the “aftermatter” account was accessed via the Spectrum IP address.

Trial counsel and the OSI affiant met with Colonel (Col) MT, base operations group commander, to request search authorization. Col MT questioned the three-year lapse of time since the initial seizure and was told there was a problem with the first search authorization’s use of the words “upload” and “login.” After receiving assurance that there was no reason not to sign the search authorization, Col MT granted search authorization for devices seized in the February search. Once again, DC3 found evidence of possession, viewing, receipt, and distribution of CSAM on Appellant’s iPhone and iPad. *Armour*, 86 M.J. at 521.

E. The second motion to suppress

The defense moved to suppress evidence recovered as a result of the January 2022 search³ and the March 2025 search of Appellant’s devices. The defense argued that the fruits of the January search, specifically the discovery of packages addressed to Appellant at the Dalzell address,

³ The defense challenged both the Spectrum warrant and the search of the Dalzell residence. In his reply brief, Appellant concedes he lacks standing to challenge the Spectrum warrant. Therefore, we consider only his challenge to the January search of the Dalzell address, which yielded packages addressed to Appellant at that address.

must be suppressed for the same reason the February search was suppressed—that is, both were based on affidavits containing recklessly false statements that CSAM was uploaded via the Spectrum IP address. According to the defense, the March search must be suppressed because OSI then used the fruits of the unlawful January search in its March search affidavit.⁴

The Government countered that Appellant lacked standing to challenge the January search because he had no expectation of privacy in an address where he no longer resided. But even if he had standing, the Government argued, the new affidavit provided sufficient information known prior to the tainted February search to establish probable cause to conduct the March search. Therefore, the Government concluded the independent source doctrine saved the March search.

The military judge found the March search authorization “does not contain the offending information, but instead accurately and matter-of-factly establishes a nexus between the NCMEC report that launched this investigation and the ultimate seizure of [Appellant’s] devices.” Applying the two-prong test set forth in *Murray v. United*

⁴ Additionally, the defense argued there was no probable cause for the January and March searches because the supporting affidavits neither established that Appellant lived at the Dalzell address on the dates CSAM was uploaded nor excluded the possibility that others could have accessed the Spectrum IP address to upload CSAM on those dates. According to the defense, the good faith exception did not apply and exclusion of the evidence was appropriate where the military judge found the supporting affidavits were written with reckless disregard for truth.

The military judge found that Col MT had a substantial basis for finding probable cause to seize and search Appellant’s devices without reaching Appellant’s arguments about the January search. Because we affirm on other grounds the AFCCA’s decision reversing the military judge’s suppression ruling, *infra* p. 13, we do not reach the issue of the lawfulness of the January search, including probable cause, or any applicable exceptions to the exclusionary rule.

States, 487 U.S. 533, 542 (1988), he concluded the March search authorization was an independent source of *information* supporting probable cause because (1) the decision to seek a new search authorization was prompted by information already known as of February 2022; and (2) no information obtained during the illegal search was presented to Col MT, the search authority.

Nevertheless, the military judge found the March search was not genuinely independent of the tainted February search. The military judge opined that but for the fact that the Government seized Appellant’s devices in February 2022 and retained continuous possession, preserving them in the same condition for years, there would not have been probable cause to believe evidence of CSAM would be found on his devices. The military judge noted that his prior ruling that the February search was unlawful “is at this point the law of the case.” In his view, probable cause existed only because the Government’s unlawful February seizure prevented probable cause from growing stale. Thus, he concluded, the Government could not prove the March search was an independent source of the *evidence*—the iPhone and iPad—obtained in the earlier, tainted search, and the evidence must be excluded.⁵

II. Standard of review

In an Article 62, UCMJ, appeal, we review the military judge’s decision directly, viewing the evidence in the light most favorable to the party that prevailed at trial—in this case, Appellant. *United States v. Hurtado*, 86 M.J. 431, 434 (C.A.A.F. 2026). We review the military judge’s

⁵ The military judge denied the Government’s motion for reconsideration. He noted that even if his independent source analysis was inapt, the exclusionary rule would apply because “[i]t remains true that on seven separate occasions, law enforcement asserted false information, made with reckless disregard [sic] for the truth, concerning the actual nexus between the upload of child pornography and the residence shared by [Appellant].”

suppression ruling for an abuse of discretion. *United States v. Shields*, 83 M.J. 226, 230 (C.A.A.F. 2023). An abuse of discretion occurs when the military judge’s “‘findings of fact are clearly erroneous, the court’s decision is influenced by an erroneous view of the law, or the military judge’s decision on the issue at hand is outside the range of choices reasonably arising from the applicable facts and the law.’” *Id.* (quoting *United States v. Finch*, 79 M.J. 389, 394 (C.A.A.F. 2020)).

III. Applicable law

“The exclusionary rule is a judicially created remedy for violations of the Fourth Amendment” that “applies to evidence directly obtained through violation of the Fourth Amendment as well as evidence that is the indirect product or ‘fruit’ of unlawful police activity.” *United States v. Wicks*, 73 M.J. 93, 103 (C.A.A.F. 2014) (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)). However, suppression is not an automatic remedy for every Fourth Amendment violation. *Id.* (citing *Herring v. United States*, 555 U.S. 135, 137 (2009)). “Evidence that would otherwise be suppressed is admissible if it meets a limited number of exceptions to the exclusionary rule” *Id.* One such exception occurs if the evidence was derived from an independent source. *Id.*

“[T]he independent source doctrine allows trial courts to admit evidence obtained in an unlawful search if officers independently acquired it from a separate, independent source.” *Utah v. Strieff*, 579 U.S. 232, 238 (2016). As this Court has noted:

The purpose of the independent source doctrine is to put “the police in the same, not a *worse*, position tha[n] they would have been in if no police error or misconduct had occurred” because if evidence with an independent source were excluded, this “would put the police in a worse position than they would have been in absent any error or violation.”

United States v. Garcia, 80 M.J. 379, 388 (C.A.A.F. 2020) (alteration in original) (quoting *Murray*, 487 U.S. at 537).

IV. Discussion

A. The military judge’s ruling was based upon an erroneous view of the independent source doctrine

The military judge abused his discretion by failing to conclude the March search was genuinely independent of the unlawful February search after finding that no information gained in the February search affected either OSI’s decision to seek search authorization or the search authority’s decision to grant it. In *Murray*, the Supreme Court held that the independent source doctrine applies not only to evidence discovered for the first time during an independent search, but also “to evidence initially discovered during, or as a consequence of, an unlawful search but later obtained independently from activities untainted by the original illegality.” 487 U.S. at 537. To establish that a search pursuant to a warrant is genuinely independent of a prior unlawful search, the government must show that no information gained from the unlawful search “affected either the law enforcement officers’ decision to seek a warrant or the magistrate’s decision to grant it.” *Id.* at 540.

Here, the military judge concluded that both prongs of the *Murray* test were satisfied. He found that OSI’s decision to seek search authorization for Appellant’s devices in March 2025 was prompted, not by information gathered in the unlawful February search, but by information known before then—specifically, the NCMEC report, the results of the January search of the Dalzell address, the Spectrum IP warrant return, and the DMV database search. Additionally, he found that the March affidavit did not make the same false statement that undermined the validity of the February search and did not contain any information discovered in the February search. Therefore, he found that no information obtained in the unlawful February search influenced the search authority’s decision to grant search authorization. These findings of fact are not clearly erroneous.

We agree with the AFCCA that “[t]he military judge’s analysis of the appropriateness of applying the independent source doctrine should have ended after he made these

findings.” *Armour*, 86 M.J. at 525. Having found that both prongs of the *Murray* test were satisfied, the military judge abused his discretion by failing to conclude the March search was genuinely independent of the unlawful February search.

Instead, the military judge concluded that the March search was not genuinely independent of the February search because the seized devices had been continuously retained in the government’s possession since the unlawful seizure, preventing the information in the NCMEC report from becoming “stale.” Like the AFCCA, we reject the military judge’s staleness rationale, finding no legal authority to support a theory of suppression which “would prevent the Government from rectifying a defective warrant when evidence originally seized remains in the Government’s possession.” *Id.*

In *Murray*, the Supreme Court rejected the notion “that objects ‘once seized cannot be cleanly reseized without returning the objects to private control.’” 487 U.S. at 541 (quoting *United States v. Silvestri*, 787 F.2d 736, 739 (1st Cir. 1986)). The Supreme Court could discern “no reason why the independent source doctrine should not apply” to the “reseizure of tangible evidence already seized . . . [s]o long as [the] later, lawful seizure is genuinely independent of an earlier, tainted one (which may well be difficult to establish where the seized goods are kept in the police’s possession).” *Id.* at 542.

Moreover, there is no basis in the record for the military judge’s finding that probable cause for the March search very likely would have gone stale but for the Government’s retention of the evidence seized in February. It is true that “[t]imeliness informs probable cause. The passage of time may diminish the likelihood that what is sought will be found in the place to be searched.” *United States v. Macomber*, 67 M.J. 214, 220 (C.A.A.F. 2009) (citation omitted). For example, probable cause set forth in the search authorization arguably could have gone stale if law enforcement had returned the devices to Appellant and then sought to execute the same search three years later, because it is

unlikely that evidence of his use of the devices in 2021 would still exist in 2025. But here, precisely because the devices were frozen upon their seizure in February 2022, probable cause as to their contents at that time did not become stale with respect to the investigation into suspected CSAM reported by NCMEC in 2021.⁶ And the Government cannot be faulted for preventing staleness by not returning Appellant’s devices. As the AFCCA recognized, once “agents became aware that the items contained [CSAM] . . . it would have been unlawful for them to just simply hand the items back to [Appellant].” *Armour*, 86 M.J. at 526.

B. Because we conclude the military judge erred in granting the second suppression motion, we decline to decide other issues raised by the parties

As noted above, *supra* p. 5, the military judge found that Inv KF’s affidavit in support of the January search “recklessly disregarded the truth with respect to the assertion that the uploads of suspect CSAM were ‘from’ or ‘via’ the [Spectrum IP] address.” Additionally, the military judge found that OSI’s decision to seek search authorization for Appellant’s devices in March 2025 was prompted by information known before the February search—specifically, the NCMEC report, the results of the January search of the

⁶ We recognize that a delay in executing a search potentially could cause probable cause to become stale, such that a seizure that was lawful becomes unreasonable in violation of the Fourth Amendment. “Although there is no per se rule determining when an initially lawful seizure becomes unreasonable, . . . we recognize that ‘a seizure [can become] unreasonable because its length unduly intruded upon constitutionally protected interests.’” *United States v. Harborth*, 85 M.J. 469, 479 (C.A.A.F. 2025) (quoting *United States v. Jacobsen*, 466 U.S. 109, 124 n.25 (1984)); accord *United States v. Cote*, 72 M.J. 41, 41, 46 (C.A.A.F. 2013) (holding that the military judge did not abuse her discretion in suppressing the fruits of a search of the appellant’s hard drive conducted more than a year after the expiration of the time limitation specified in the search authorization). However, Appellant has not challenged the duration of the seizure of his devices. Therefore, we need not address this issue.

Dalzell address, the Spectrum IP warrant return, and the DMV database search.

With these factual findings in mind, we acknowledge Appellant’s “alternative” argument that the military judge properly suppressed the fruits of the March search, albeit for the wrong reason. According to Appellant, the January search was tainted by Inv KF’s affidavit containing the recklessly false statement that CSAM was uploaded via the Spectrum IP address. Appellant contends the March search fails both prongs of the *Murray* test and accordingly, should be suppressed, where (1) OSI sought authorization for the March search only because they discovered packages addressed to Appellant at the Dalzell address during the unlawful January search; and (2) OSI presented tainted information to the military search authority, influencing his decision to grant search authorization.

However, neither the military judge nor the AFCCA ruled on whether the January search was unlawful, whether the January search tainted the March search, or whether the exclusionary rule should apply to either of those searches. The granted issue asks whether the military judge’s second suppression ruling should be affirmed “because information gained from multiple unlawful searches affected law enforcement agents’ decision to seek a search authorization and the search authority’s decision to grant it.” *Armour*, __ M.J. at __. Having concluded the military judge erred in ruling the March search was not genuinely independent of the tainted February search, we answer the granted issue in the negative, holding the military judge erred in granting the second suppression motion on the basis of a misapplication of the law. We decline to rule in the first instance on whether the January search was unlawful or whether the March search was genuinely independent of the January search. We also express no opinion as to whether any other exception to the exclusionary rule saves any of the searches in this case.

V. Conclusion

We answer the granted issue in the negative. The decision of the United States Air Force Court of Criminal Appeals is affirmed. The case is remanded to the Judge Advocate General of the Air Force for further proceedings consistent with this opinion.