

COURT OF CRIMINAL APPEALS OF ALABAMA

State of Alabama v. Kala Blakely and Bartley Evan Blakely

Blakely · No. CR-2025-0337 · Decided February 6, 2026

SUMMARY

The Alabama Court of Criminal Appeals reviews the State's appeal from a Jefferson Circuit Court order suppressing forensic evidence obtained from the Blakelys' cellular telephones and evidence obtained from Google accounts under the fruit-of-the-poisonous-tree doctrine. The opinion addresses whether an October 2021 warrant authorized the forensic examination of seized electronic devices despite language contemplating a subsequent warrant. The court concludes that the circuit court made legal errors in interpreting the warrant and in requiring a second warrant, and it reverses and remands.

OPINION

State of Alabama v. Kala Blakely and Bartley Evan Blakely

PER CURIAM.

Rel: February 6, 2026 Notice: This opinion is subject to formal revision before publication in the advance sheets of Southern Reporter. Readers are requested to notify the Reporter of Decisions, Alabama Appellate Courts, 300 Dexter Avenue, Montgomery, Alabama 36104-3741 ((334) 229-0650), of any typographical or other errors, in order that corrections may be made before the opinion is published in Southern Reporter. Alabama Court of Criminal Appeals

OCTOBER TERM, 2025-2026

_____ CR-2025-0337 _____ State of Alabama v. Kala Blakely and Bartley Evan Blakely Appeal from Jefferson Circuit Court (CC-21-2007 and CC-21-2466) ANDERSON, Judge. The State of Alabama appeals from the Jefferson Circuit Court's pretrial order suppressing evidence of text messages recovered from cellular telephones belonging to Kala Blakely ("Kala") and Bartley Evan Blakely ("Bartley"), as well as evidence obtained pursuant to a November CR-2025-0337 2021 search warrant, under the "fruit of the poisonous tree" doctrine. See Rule 15.7(a), Ala. R. Crim. P. For the reasons that follow, we reverse the circuit court's order granting Kala and Bartley's motions to suppress and remand these matters to the circuit court. Facts and Procedural History On October 22, 2021, a Jefferson County grand jury indicted Kala for one count of attempted murder of A.B., Kala and Bartley's adopted daughter, see §§ 13A-4-2 and 13A-6-2, Ala. Code 1975, and one count of aggravated child abuse, see § 26-15-3.1, Ala. Code 1975. On December 10, 2021, a Jefferson County grand jury reindicted Kala for the attempted murder and aggravated child abuse of A.B., and it returned an indictment against Bartley for the attempted murder and aggravated child abuse of A.B. At the State's request, the circuit court ordered that the cases against both Kala and Bartley be joined because "the

Defendants [were] alleged to have participated in the same act or transaction; the offenses [were] part of a common conspiracy, scheme, or plan; and the offenses are otherwise so closely connected that it would be difficult to separate proof of one from proof of another." (C. 104; 157.)

2 CR-2025-0337 On or about April 9, 2025, Kala and Bartley each filed a "Motion to Suppress Unlawfully Obtained Digital Forensic Evidence," claiming that law-enforcement officers unlawfully obtained digital evidence from the Blakelys' cellular telephones. Specifically, they noted that the affidavit supporting the application for the search warrant leading to the seizure and search of the phones, submitted in October 2021 ("the October affidavit"), asked that law-enforcement officers be allowed to seize " '[a]ll mobile devices, tablets, pocket computers, personal data assistants, cellular telephones and any other portable mobile devices.' " (C. 458; 505.) The Blakelys argued that the October affidavit asked only for "permission to take a 'forensic image' of the data stored on the mobile devices," which "is a picture of all data stored on the phone but the image itself is not a review of the contents of the data," which was to be obtained "as a security measure to make sure the data is not altered or harmed prior to reviewing it." (C. 458; 505). The Blakelys asserted that the October affidavit did not seek permission for law-enforcement officers to search the digital-storage devices, which included their cellular telephones, and they further asserted that the search warrant that issued did not grant such authority. The Blakelys maintained that law- 3 CR-2025-0337 enforcement officers never obtained a second warrant to search the digital images obtained from the digital-storage devices, yet searched them anyway, and then produced the contents of the unlawful search to the Blakelys in discovery. The Blakelys attached a copy of the October affidavit and the resulting search warrant ("the October warrant") to their motions to suppress. The Blakelys also averred that, on November 8, 2021, a second search warrant ("the November warrant") was issued at the request of Investigator Justin Bowlin, an investigator with the Jefferson County District Attorney's Office, which related "exclusively to the Blakelys' Google Accounts and did not seek or authorize the search of the seized cell phone." (C. 458.) A copy of the affidavit filed by Inv. Bowlin regarding the Google accounts ("the November affidavit"), as well as the resulting November warrant, were also attached to the Blakelys' motions to suppress. In the October affidavit, Inv. Bowlin indicated that, based on his training and experience, he had "reason to believe that documents and particular digital device(s) and related storage devices may contain evidence identifying and linking, victim(s), suspects(s), and possible 4 CR-2025-0337 witness(es) to the crime of Aggravated Child Abuse." (C. 465.) The affidavit then stated, in pertinent part: "Evidence to be Searched and Seized

"This application seeks permission to search for and seize evidence of the crimes described above, that are currently located at [the address of the Blakelys' private residence]. "Items of Evidence to be Seized and Searched include: "Digital Storage Devices to be Seized may include: "a. All tower computers, laptop computers, tablet computers, notebook computers, servers, gaming consoles or gaming devices, and any related digital storage media" (C. 466.) This section of the affidavit continued detailing a lengthy list of a large variety of digital-storage devices, including, but not

limited to, all mobile devices, tablets, cellular telephones, digital cameras, navigation devices, and power cords. This section of the affidavit further stated, in pertinent part: "g. All evidence of user attribution including accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage, or any other evidence that may demonstrate attribution to a particular user or users; "h. All such seized evidence may be temporarily accessed for the purpose of determining user attribution and to isolate it from network access or connectivity to prevent user data from being modified, deleted, or accessed. 5 CR-2025-0337 "i. Once such items of evidence are seized and rendered isolated from network connectivity, an affiant will apply for a separate search warrant to search the seized items for physical evidence such as DNA and latent prints and any live and deleted digital data. "j. Documents related to the medical care and adoption, and correspondence between agencies facilitating adoption or care of any children." (C. 467 (emphasis added).) The October affidavit went on to set out a lengthy "Statement of Probable Cause," wherein Inv. Bowlin detailed the alleged factual basis of his belief, based on his training and experience, that sufficient probable cause existed to support the issuance of the warrant. Specifically, Inv. Bowlin declared that the victim, the Blakelys' 12-year-old adopted daughter, was treated for a severe infection at Children's Hospital and was sent home with a 10-day dose of "intense antibiotic treatment via a PICC line" (C. 467); that Kala, a certified nurse practitioner with a doctorate in nursing, failed to return A.B. to the hospital for her follow-up appointment; and that, after making inquiries, the nurses from the hospital discovered that A.B. had not received the antibiotic treatment at home following her release from the hospital. 6 CR-2025-0337 According to Inv. Bowlin, when Kala returned A.B. to the hospital, the child had "several serious physical injuries," which Kala claimed were from "throwing tantrums and running [into] walls." Additionally, A.B. was severely malnourished. The October affidavit, however, indicated that Dr. Peters, a doctor treating A.B., disputed Kala's explanation of the injuries. (C. 467.) Inv. Bowlin further disclosed that a forensic interview was conducted with A.B., during which A.B. disclosed abuse. Nurses at the hospital told detectives that Kala had made statements like "I regret adopting her" and "she's made our life a living hell and I see why her mother abandoned her" and that Kala had refused sedation of A.B., saying that "[A.B. was] going to have to deal with the pain." (C. 468.) Inv. Bowlin also wrote that jail calls between Kala and Bartley disclosed that Bartley advised Kala that he had started deleting her social-media pages and that Bartley stated that he possessed a video of A.B. falling and alluded to the injuries A.B. sustained during the fall. (C. 468.) At the end of his probable-cause statement, Inv. Bowlin included the following conclusion: "For these reasons, I believe probable cause exists to seize, 7 CR-2025-0337 examine, and search all documents and digital storage devices and related accessories at the location described." (C. 469.) But the October affidavit contained a separate section entitled "Removal of Data Storage Devices," in which Inv. Bowlin described the need for "a forensic image or forensic extraction" that is an "exact physical copy of the user data found on the storage media" and why it is "essential" that such an extraction be completed before law-

enforcement officers searched the data for information. (C. 469-70.) The affidavit further explained that searching the digital-storage devices was a "highly technical process that requires specific expertise and specialized equipment," as well as "precise, validated procedures designed to maintain the integrity of the evidence and to recover the latent data not readily apparent to the casual user," and that, because of the volume of data stored on many digital-storage devices, it is "highly impractical" to search the data during the execution of the physical search of the premises because such searches can take a great length of time. (C. 470.) The next section of the October affidavit, entitled "Inventory and Return," explained that a list of the items seized under the authority of the search warrant would be left at the Blakelys' residence and provided 8 CR-2025-0337 to the court. At the end of this section, the following language was included: "An application for a search warrant to forensically search particular items for digital evidence will be forthcoming." (C. 470.) Lastly, Inv. Bowlin's conclusion in the October affidavit read: "Based on the foregoing information, I have probable cause to believe that evidence of the crime(s) of Aggravated Child Abuse (26-15-3.1)/Neglect as set forth herein are currently related to the items listed above and within the digital storage devices described above. I therefore respectfully request that a search warrant be issued authorizing the search for, seizure of and examination of the items set forth herein." (C. 471.) The Blakelys also attached a copy of the October warrant, issued in response to Inv. Bowlin's October affidavit and application, to their motions to suppress. The October warrant provided, in pertinent part: "To Any Police Officer in the State of Alabama Greetings; "You are hereby commanded to search the following in the County of Jefferson State of Alabama for evidence of the crimes of Aggravated Child Abuse. "The location to be searched and the items to be seized are at a private residence located at [the Blakelys' street address,] City of Trussville, County of Jefferson[,] State of Alabama and any vehicles/out buildings on the curtilage. "Evidence to be Searched and Seized: 9 CR-2025-0337 "a. Documents related to the medical care or adoption of any child along with any correspondence associated with the adoption or potential adoption of any child. "Digital Storage Media to be Searched and Seized: "[In paragraphs numbered 1-6, the court listed all the digital- storage and electronic devices, etc., that were subject to the warrant] ... "7. All evidence of user attribution including accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage, or any other evidence that may demonstrate attribution to a particular user or users; "8. All such evidence may be temporarily accessed for the purpose of determining user attribution and to isolate it from the network access or connectivity to prevent user data from being modified, deleted, or accessed; "9. Once such items of digital storage media are seized and rendered isolated, an affiant will apply for a separate search warrant describing specific items to be forensically processed and searched for any live and deleted digital evidence." (C. 472-73 (emphasis added).) In the November affidavit, Inv. Bowlin disclosed that in October 2021 "a forensic data extraction was performed on the suspects' mobile devices" and that the analysis revealed three Google email accounts that were used for various communications. Those email

accounts were the subject of the November warrant. No other information or data obtained 10 CR-2025-0337 from the Blakelys' cellular telephones was disclosed by Inv. Bowlin in the November affidavit. As a result of the November affidavit, the November warrant was issued identifying three Google accounts and authorizing the following evidence to be searched and seized from Google: "1. Account Information -- User name, primary e-mail address, secondary e-mail addresses, connected applications and sites, and account activity from 08/01/2015 to 11/05/2021, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses; "2. Evidence of user attribution -- accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number, or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s); " [In paragraphs numbered 3-12, the court authorized similar searches of calendars, contacts, documents, gmail accounts, photographs, location history data, Play Store data, search histories, voice call records, and Google Home product information pertaining to the three Google accounts.]" (C. 597-98.) The circuit court held a suppression hearing on April 17, 2025. At that hearing, Inv. Bowlin testified that he used a template when he wrote 11 CR-2025-0337 the October affidavit and that the clause stating that a second warrant would be requested to get the data off any digital-storage devices that were seized was "a clause in the template" that he inadvertently failed to remove from the affidavit. (R. 48.) He told the circuit court, that "when [he] did the search warrant, [he was] operating under the belief that[,] based off the last statement [in the conclusion of the affidavit]: 'I, therefore, respectfully request that a search warrant be issued authorizing the search for, seizure of, and examination of the items set forth therein,' " that law-enforcement officers had the authority to search the contents of the devices seized. (R. 49.) Inv. Bowlin testified that, when submitting the affidavit, it was his intent that the October warrant was to "search for the phones, get the phones, and then examine the phones upon getting them." (R. 49.) He indicated that, after the law-enforcement officers reviewed the data on the cellular telephones, officers realized they would need additional warrants for the Google information and that officers sought a second warrant for the Google information. Inv. Bowlin explained that law-enforcement officers sought the October warrant, in part, because officers had obtained phone-call recordings from the jail wherein Bartley advised Kala that he had started 12 CR-2025-0337 deleting Kala's social-media pages and that the officers "wanted to get in there and get the devices before any evidence could be deleted" and, in part, based on information provided by hospital medical staff during interviews. (R. 71.) He maintained that, notwithstanding his error in leaving the language from the template in the October affidavit, he believed that, based on his last statement in the conclusion of the October affidavit, a second search warrant was unnecessary and that, "if [officers] did an additional search warrant," the additional warrant would be for things like the Google information, not the cellular telephones

themselves. (R. 72.) On cross-examination, defense counsel asked Inv. Bowlin how he failed to notice the places in his affidavit where it said that he would seek an additional warrant to search the cellular telephones. Inv. Bowlin responded: "When typing a search warrant, there's particular parts of it that are highlighted. So my thought process at the time was what specifically do I need to add to the search warrant that establishes my probable cause. The notion of what do I need to delete from it was --- was not in the forefront of my mind." (R. 56.) Inv. Bowlin admitted that the information relating to the Blakelys' Google accounts was derived from the search and forensic 13 CR-2025-0337 analysis performed on the Blakelys' cellular telephones; however, he "felt like [he] was acting in good faith" by searching the phones even if the October warrant did not actually authorize him to do so. (R. 68.) At the hearing's conclusion, the circuit court granted the Blakelys' motions to suppress, finding that the information found during the forensic analysis of the two cellular telephones was due to be suppressed. In so ruling, the circuit judge noted that she "did not believe that Investigator Bowlin acted in bad faith" or that he "intentionally or deliberately tried to circumvent the Blakelys' Fourth Amendment rights"; however, she stated, the October warrant was what gave him the authority to search and that she "ha[d] to go by the four corners of the search warrant." (R. 90.) The circuit court found that the October warrant required Inv. Bowlin to obtain an additional warrant to search the seized digital-storage devices' contents. (R. 90.) The circuit court then granted the motions to suppress as it related to information obtained during the execution of the November warrant because it was fruit of the poisonous tree. 1 1The record on appeal does not identify or contain any description of the evidence produced by Google as a result of the November warrant. 14 CR-2025-0337 On April 21, 2025, the circuit court issued a written order granting the Blakelys' motions to suppress. The circuit court concluded: "Here, the Court finds from the four corners of the first search warrant that a second search warrant was needed to do a forensic examination of the electronic devices seized from the home to get any live or deleted data. The first search warrant only allowed for a seizure of electronic devices and rendering them safe until a subsequent search warrant was obtained for the data on the phones. That subsequent search warrant was not obtained. The Court finds that there was no intention on the part of Inv. Bowlin to violate the rights of the [Blakelys]; however the error in not obtaining a subsequent search warrant cannot be remedied by looking only to the favorable portions of the affidavit. "Therefore, this Court finds that the forensic examination of the [Blakelys'] phones was an unlawful search. Moreover, the evidence obtained from Google is also inadmissible as fruit of the poisonous tree. The MOTION TO SUPPRESS

UNLAWFULLY OBTAINED DIGITAL FORENSIC

EVIDENCE is hereby GRANTED." (C. 106-07; 159-60 (capitalization in original).) On April 24, 2025, the State moved the circuit court to reconsider its ruling. In support of its motion, the State submitted multiple attachments, including an application for a search warrant and subsequent search warrant authorizing the search of the Blakelys' cellular telephones, both of which were dated April 17, 2025. The State also filed its notice of pretrial appeal. 15 CR-2025-0337

Discussion On appeal, the State contends that the circuit court erred in granting the Blakelys' motions to suppress because, the State says, "it improperly concluded that the forensic examinations of the cellphones constituted an unlawful search and the subsequent Google search warrant return was fruit of the poisonous tree." (State's brief at 23.) Specifically, the State argues that the circuit court failed to apply the proper legal analysis in these cases because it concluded that the search of the cellular telephones was warrantless, relying on *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009), and because the circuit court relied on an improper "four corners" analysis. The State also contends that a second warrant was not required because, it says, the October affidavit established probable cause for the examination of the cellular telephones and the contradictory language in the October warrant did not merit suppression of the evidence. The Blakelys maintain that, although "the initial seizure of the devices was authorized, without obtaining a second warrant" to search those devices, the law-enforcement officers "blatantly violated the scope of the warrant" by conducting an unauthorized search of the contents of 16 CR-2025-0337 the cellular telephones in violation of the Fourth Amendment. (Blakelys' brief at 20.) "In reviewing a decision of a trial court on a motion to suppress evidence, in a case in which the facts are not in dispute, we apply a de novo standard of review." *State v. Otwell*, 733 So. 2d 950, 952 (Ala. Crim. App. 1999); *State v. Cheatwood*, 267 So. 3d 882, 884-85 (Ala. Crim. App. 2018). Because the relevant facts here -- namely, the language of the October affidavit and the October warrant and Inv. Bowlin's testimony - - are undisputed, this Court reviews the circuit court's decision granting the Blakelys' motions to suppress de novo. The Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides further that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." " 'A search is unreasonable and violates the protections of the Fourth Amendment if it exceeds the scope of the authorizing warrant. U.S. Const. Amend. IV; see *Long v. State*, 532 S.W.2d 591, 596 (Tex. Crim. App. 1975). While the scope of the search warrant is governed by its terms, the 17 CR-2025-0337 search may be as extensive as is reasonably required to locate items described in the warrant. U.S. Const. Amend. IV; *Haynes v. State*, 475 S.W.2d 739, 741-42 (Tex. Crim. App. 1971). If the scope of the search is challenged because of the location where the items were found, the officer must show that he was properly in the place where the item was found, either on basis of the search warrant or under the authority of an exception to the warrant requirement. *Snider v. State*, 681 S.W.2d 60, 62-62 (Tex. Crim. App. 1984); *Swink v. State*, 747 S.W.2d 53, 54 (Tex. App.--Texarkana 1988, no writ).' " *DeMoss v. State*, 12 S.W.3d 553, 558 (Tex. App. 1999). See also *United States v. Wuagneux*, 683 F.2d 1343 (11th Cir. 1982), cert. denied, 464 U.S. 814, 104 S.Ct. 69, 78 L.Ed.2d 83 (1983) and *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978) ("The question is whether or not the search that was conducted was confined to the

authorization given by the magistrate. In determining whether or not a search is confined to its lawful scope, it is proper to consider both the purpose disclosed in the application for a warrant's issuance and the manner of its execution.')."

Smith v. State, 908 So. 2d 273, 289 (Ala. Crim. App. 2000). Initially, we note that the Blakelys do not challenge the validity of the October warrant to seize the digital-storage devices, and they do not argue that law-enforcement officers lacked sufficient probable cause to support the issuance of the October warrant. In fact, the Blakelys concede that the seizure of the devices was valid pursuant to the October warrant. (Blakelys' brief at 20, 38.) Instead, the issues presented to this Court 18 CR-2025-0337 center on whether law-enforcement officers' subsequent search of the contents of the cellular telephones and other electronic devices violated the Blakelys' Fourth Amendment rights and whether the circuit court's suppression of the evidence resulting from that search was proper. To that end, the State contends that the search of the contents of the Blakelys' cellular telephones was proper and that a second warrant was not needed to examine those devices. The Blakelys, on the other hand, maintain that law-enforcement officers knew, or reasonably should have known, a second warrant was needed to search the contents of the cellular telephones once they were seized. Contrary to the Blakelys' contention, however, Alabama law does not generally dictate a requirement to obtain a second warrant to search seized electronic devices. Ultimately, because the circuit court made two critical errors in granting the Blakelys' motions to suppress, we agree with the State. First, the circuit court's reading of the "four corners" of the October warrant was clearly erroneous. The circuit court characterized the October warrant as allowing no search at all of the listed electronic devices, including cellular telephones, only "seizure ... and rendering them safe until a subsequent search warrant was obtained for the data 19 CR-2025-0337 on the phones." (C. 107.) Unfortunately, that conclusion is simply not accurate. The October warrant authorized law-enforcement officers to search the Blakelys' home for documents related to the medical care or adoption of any child along with any correspondence associated with the adoption or potential adoption of a child. The October warrant then identified specific types of digital-storage devices that could be seized and searched for evidence related to the crime of aggravated child abuse. Because there was a search warrant for those items, the Blakelys' reliance on *Riley v. California*, 573 U.S. 373 (2014), is misplaced. Moreover, this is not a case in which it could be argued that the "warrant authorized only the search for ... electronic devices and did not authorize the search of those devices." *State v. Hunt*, 316 So. 3d 271, 283 (Ala. Crim. App. 2020) (emphasis in original). After setting out the specific types of digital-storage devices that were authorized to be seized and searched, additional authority was granted to temporarily access those devices to determine "user attribution" information for "accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data 20 CR-2025-0337 storage, or any other evidence that may demonstrate attribution to a particular user or users." (C. 541.) Thus, the October warrant envisioned far more than the simple seizure and storage suggested by the circuit court's order. Further, we note that, although the October warrant clearly contemplated that broad categories of

digital-storage devices that were to be "seized and searched," the language that appears in the final two paragraphs of the warrant did not contemplate an additional warrant for "all digital storage media seized" or "all electronic evidence seized." Instead, it contemplated that an additional application would be forthcoming for "specific items to be forensically processed and searched for any live and deleted digital evidence." (C. 473.) Thus, the October warrant both explicitly authorized the seizure and search of six broad categories of digital-storage devices and, arguably, implicitly limited the scope of any search by contemplating that law-enforcement officers would seek an additional warrant for specific items. Second, the circuit court erred by finding that a second warrant was required before the State could search the seized devices for evidence. As discussed above, the October warrant authorized at least some search of 21 CR-2025-0337 the seized devices. Had the language discussing a second warrant not been -- inadvertently -- included in the October warrant, there would be no question that the October warrant was sufficient to authorize the searches that the State conducted in this case. This Court recently addressed a similar situation in *Hunt*, where this Court explained: "[T]he dispositive question in this case is whether a warrant that authorizes the search for electronic devices believed to contain child pornography also authorizes a search of those devices. The holding of *Riley*[v. California, 573 U.S. 373, 384

(2014),] does not, in our opinion, provide guidance on this

issue. However, cases from the federal circuit courts have directly addressed this specific issue, and we find the analysis in those cases to be persuasive. "In *United States v. Grimm*, 439 F.3d 1263 (10th Cir. 2006), the United States Court of Appeals for the Tenth Circuit addressed the same argument *Hunt* makes here. In that case, a law-enforcement officer sought a warrant authorizing him to search Stephen Grimm's home for Grimm's computer, among other electronic devices, which the officer had probable cause to believe contained child pornography. *Id.* at 1266. The officer's affidavit submitted in support of the search warrant also sought permission to search the contents of any computers he seized during the search. *Id.* The search warrant issued to the officer authorized the officer to search Grimm's home for computer hardware, and after the officer seized a hard disk drive from a computer in Grimm's home, a subsequent forensic examination of the hard drive unearthed 1,642 images and videos of child pornography. *Id.* On appeal from Grimm's multiple convictions for child-pornography offenses, the Tenth Circuit addressed Grimm's argument that the evidence discovered during the search of the hard drive was due to be suppressed: 22 CR-2025-0337 " 'Mr. Grimm argues that the warrant authorized only the seizure, but not the subsequent search, of his computer and computer storage devices (collectively, "the computer"). Although not couched in "particularity" terms, Mr. Grimm appears to argue that the warrant was not sufficiently particular to authorize a search of the computer. " 'Mr. Grimm relies on *United States v. Carey*, 172 F.3d 1268, 1270 (10th Cir. 1999) for his argument that a second warrant is required to search a properly seized computer. In *Carey*, the original warrant authorized a search of the computer for evidence related to illegal drug sales. But, when

the officers found evidence of another crime -- possession of child pornography -- another warrant was needed to search for this evidence, which was beyond the scope of the original warrant. Id. at 1271, 1273-74 ("[I]t is plainly evident each time [the officer] opened a subsequent JPG file, he expected to find child pornography and not material related to drugs Under these circumstances, we cannot say the contents of each of those files were inadvertently discovered.").

" 'Carey does not support Mr. Grimmatt's argument, but simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification. In this case, unlike the search in Carey, where the probable cause that permitted the search related to drugs, the original justification for the search and seizure of the computer was the probable cause to believe the defendant possessed child pornography. We hold that the evidence obtained 23 CR-2025-0337 in the search of the defendant's computer was consistent with the probable cause originally articulated by the state court judge; hence, the search was permissible under Carey. " 'Moreover, the affidavit underlying the application for a search warrant clearly states that Detective Askew sought the authority to search both the premises and the computers: " ' "This affidavit is made in support of an application for a warrant to search the entire premises located at 920 SE 33rd Street, Topeka, Shawnee County, Kansas. Additionally, this application is to search any computer media found therein." " 'The affidavit also made clear that the search of the computer would be off-site in a laboratory setting: "It is only with careful laboratory examination of electronic storage devices that it is possible to recreate the evidence trail." In turn, the warrant expressly refers to the "evidence under oath before me," which is, of course, a direct and explicit reference to the affidavit. Accordingly, we hold that the warrant authorized both the seizure and search of the computer.' "Id. at 1268-69 (internal citations to appellant's brief omitted). "The United States Court of Appeals for the Sixth Circuit also addressed the same argument in *United States v. Evers*, 669 F.3d 645 (6th Cir. 2012). In *Evers*, law- enforcement officers who believed *Ovell Evers, Sr.*, was in possession of child pornography obtained a search warrant authorizing them to search *Evers's* home for computers and 24 CR-2025-0337 other electronic devices. Id. at 650. Upon executing the search, officers found a black computer, which they seized, and a subsequent search of the computer revealed sexually explicit images of a 13-year-old female. On appeal from his multiple convictions of child-pornography offenses, *Evers* argued that the images seized from the black computer were due to be suppressed because, he argued, 'although the search warrant authorized the seizure of his computers, ... it did not authorize a search of the black computer's hard drive, and the police therefore unlawfully exceeded the scope of the warrant when they searched the contents of the computer without obtaining a second warrant.' Id. at 652. In rejecting that argument, the Sixth Circuit, citing *Grimmett, supra*, held that 'a second warrant to search a properly seized computer is not necessary "where the evidence obtained in the search did not exceed the probable cause articulated in the original warrant." ' Id. (quoting *United States v. Richards*, 659 F.3d 527, 539 n.10 (6th Cir. 2011)). Thus, after noting that *Evers* did not argue that there was not probable cause to believe there would be evidence of child pornography on his

computer, the Sixth Circuit concluded: " 'The warrant was, as the district court properly concluded, "specifically designed not simply to permit the officers to seize the computer ..., but to view the computer and ... to have access to [it].'" We agree with the district court that the search for, and extraction of, illegal images from the black computer's hard drive fell within the lawful parameters of the warrant.' "Evers, 669 F.3d at 653. "We hold, as the Tenth Circuit and Sixth Circuit held under similar circumstances in *Grimmett* and *Evers*, respectively, that in cases involving the seizure and search of electronic devices containing data, such as cellular telephones and computers, a second search warrant is not required to 25 CR-2025-0337 search the contents of such devices when the initial search warrant is based on an affidavit that demonstrates probable cause to believe that the evidence sought is contained within those devices. This determination will of necessity depend on the specific facts of each case, but ' "where the evidence [sought to be] obtained in the search [does] not exceed the probable cause articulated in the original warrant," ' *Evers*, 669 F.3d at 652 (quoting *Richards*, 659 F.3d at 539 n.10), then the original search warrant is sufficient to permit a law- enforcement officer not only to seize the electronic device, but also to view the contents of the device and to extract data consistent with that search warrant. *Evers*, supra. "Accordingly, in this case, we hold that a second search warrant was not required to search the contents of Hunt's electronic devices because, as we have already concluded, there was probable cause to believe Hunt's electronic devices contained child pornography, which, of course, could be discovered only by searching the contents of the devices. Thus, the Colbert warrant clearly contemplated 'the search for, and extraction of, illegal images' contained within Hunt's electronic devices, and, as a result, the search for such images 'fell within the lawful parameters of the warrant.' *Evers*, 669 F.3d at 653. See also *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) ('As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images.'). In addition, we note that Det. Harless's affidavit clearly sought authority to search the contents of Hunt's electronic devices. Specifically, Det. Harless's affidavit states: 'I request that if electronic storage devices such as computers are seized as a result of this search warrant, that the court authorize the seizure and removal of the devices to a laboratory environment for the forensic examination of the same by persons qualified to conduct said examination.' (Emphasis added.) Although the Colbert warrant does not expressly authorize the search of the contents of Hunt's electronic 26 CR-2025-0337 devices, the warrant does expressly refer to the '[a]ffidavit in support of application for a search warrant' (C. 72), which, as noted, sought such authority. As was the case in *Grimmett*, such facts further strengthen the conclusion that the Colbert warrant 'authorized both the seizure and search of the computer.' *Grimmett*, 439 F.3d at 1269 (emphasis added). "We emphasize that our holding that a second search warrant was not required in this case does not mean that a second search warrant is never required before law-enforcement officers may search the contents of electronic devices seized pursuant to a search warrant that does not expressly authorize such a search. However, under the specific facts of this

case, neither the lack of language in the Colbert warrant expressly authorizing a search of Hunt's electronic devices nor the lack of a second warrant authorizing such a search provides a basis for suppressing the evidence resulting from the Colbert County search. *Grimmett*, supra; *Evers*, supra."

316 So. 3d at 283-86 (footnote omitted).

At first blush, the holding in *Hunt* appears to be controlling in the present cases. The October affidavit demonstrated probable cause to believe that evidence of aggravated child abuse was contained within the digital-storage devices that it listed. Additionally, the October affidavit further included a clear statement that Inv. Bowlin sought the authority to search, seize, and examine those devices. The October warrant accordingly authorized the seizure of the digital-storage devices taken from the Blakelys' residence. See *Hunt*, 316 So. 3d at 285; see also *United States v. Upham*, 186 F.3d 532, 535 (1st Cir. 1999) (holding that, when the warrant explicitly authorized the seizure of the computer plus diskettes and unlawful images, because the unlawful images were inside the computer or diskettes, "the extraction of unlawful images from within the computer and diskettes was therefore contemplated by the warrant"). However, these cases involve a complicating factor that was not present in *Hunt* in the form of language that could be read as narrowing the broad search authority granted by the initial paragraphs of the October warrant. While the October warrant authorized law-enforcement officers to "search[] and seize[]" multiple types of digital-storage devices,² it also, confusingly -- and apparently inadvertently -- contained language that contemplated "temporary access" to the seized electronic devices to search for information "for the purpose of determining user attribution and to isolate [them] from network access ... to prevent user data from being modified, deleted, or accessed." (C. 541.) But even that language authorized searches for "accounts, e-mail accounts, passwords, PIN 2The October warrant also permitted a search throughout the Blakelys' residence for any "[d]ocuments related to the medical care or adoption of any child along with any correspondence associated with the adoption or potential adoption of any child." (C. 540.) 28 CR-2025-0337 codes, patterns, account names, user names, screen names, remote data storage, or any other evidence that may demonstrate attribution to a particular user or users," as well as for "any other items or information that may be necessary for access, allow for proper identification, operation and analysis of the items seized." (Id.) To further complicate matters, as Inv. Bowlin explained, the section of the October affidavit listing digital-storage devices inadvertently concluded with a statement that once such devices "are seized and rendered isolated, an affiant will apply for a separate search warrant describing specific items to be forensically processed and searched" for "live and deleted digital evidence." (C. 541.) Thus, unlike the affidavits in *Hunt* and *Grimmett*, the October affidavit contemplated, albeit inadvertently, that Inv. Bowlin would seek a second warrant for the search of "specific" digital-storage devices. In response to that statement, the magistrate included language in the October warrant that "an affiant will apply for a separate search warrant." (C. 541.) To sustain the circuit court's ruling, this Court would have to conclude

that this additional language -- which at most contemplated a second search warrant for specific items -- acted to negate the October 29 CR-2025-0337 warrant's prior authorization to seize and search all listed digital-storage devices. But the result of construing the warrant in this way would lead to a conclusion that the warrant authorized the State to seize the digital-storage devices "based on an affidavit that demonstrates probable cause to believe that the evidence sought is contained within those devices." Hunt, 316 So. 3d at 285. And, as we held in Hunt, in those circumstances a second warrant would not be required. Under the particular facts before us, we see no reason not to read the October warrant as being the authorization to "seize[] and search[]" the digital-storage devices that Inv. Bowlin believed it to be. " 'A search is unreasonable and violates the protections of the Fourth Amendment if it exceeds the scope of the authorizing warrant. U.S. Const. Amend. IV; see Long v. State, 532 S.W.2d 591, 596 (Tex. Crim. App. 1975).' " Smith,

908 So. 2d at 289 (quoting DeMoss v. State, 12 S.W.3d 553, 558 (Tex. App. 1999)). As we have explained, the October warrant authorized the State to seize and search the digital-storage devices. The fact that other language in the warrant, some of which was inadvertently included, permitted law-enforcement officers to search all the seized devices for "user attribution" evidence, which "include[ed] accounts, e-mail accounts, 30 CR-2025-0337 passwords ... or any other evidence that may demonstrate attribution to a particular user or users", did not change the fact that the warrant -- which, again, was based on probable cause to believe that the devices contained evidence of a crime -- specifically contemplated the seizure and search of those devices. (C. 541 (emphasis added)); cf. Hunt, 316 So. 3d at 285. When discussing the standards by which a reviewing court should approach the interpretation of affidavits supporting warrants that have been duly issued by examining magistrates, the United States Supreme Court has explained: "[T]he Fourth Amendment's commands, like all constitutional requirements, are practical and not abstract. If the teachings of this Court's cases are to be followed and the constitutional policy served, affidavits for search warrants, such as the one involved here, must be tested and interpreted by magistrates and courts in a commonsense and realistic fashion. They are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area. A grudging or negative attitude by reviewing courts toward warrants will tend to discourage police officers from submitting their evidence to a judicial officer before acting." United States v. Ventresca, 380 U.S. 102, 108 (1965). 31 CR-2025-0337 Applying that standard to the October affidavit, Inv. Bowlin plainly sought authority to specifically "seize, examine, and search all documents and digital storage devices and related accessories" at the Blakelys' residence (C. 469) and to "search for," seize, and examine the items identified in his affidavit. (C. 471.) He also sought permission to remove digital-storage devices from the Blakelys' residence because, he averred, "it is essential that a forensic image or forensic extraction be obtained prior to conducting any search of data for information" pursuant to a warrant and because such imaging required

"specific expertise and specialized equipment." (C. 469-70.) Moreover, Inv. Bowlin was aware that the "volume of data stored on many digital devices is typically so large that it will be highly impractical to search for data during the execution of the physical search of the premises." (C. 470.) Accordingly, a fair reading of the October affidavit shows that Inv. Bowlin sought a search warrant authorizing the seizure of the digital-storage devices and their removal from the Blakelys' residence to quickly obtain a forensic image or forensic extraction before conducting any search of data for information. 32 CR-2025-0337 At most, the subsequent language regarding searches for specific information and contemplating a second search warrant for particular items introduced some ambiguity into the October warrant. But employing the "commonsense and realistic" approach to interpreting the warrant's language, *Ventresca*, 380 U.S. At 108, we find that this ambiguity was the product of the "haste" that often affects criminal investigations. We do not condone sloppiness or inattention to detail by agents of the State, and we strongly encourage investigating officers to exercise due care in drafting search-warrant affidavits and warrants to avoid the ambiguity and confusion that has affected these cases. However, under the facts presented to us, law-enforcement officers were permitted to search the contents of the Blakelys' cellular telephones to determine whether those devices included accounts, email accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage, or any other evidence that could demonstrate attribution to a particular user or users. Clearly, as evidenced by the Blakelys' standing to bring this Fourth Amendment challenge, law-enforcement officers found text message accounts on those devices that included evidence attributing those accounts to the Blakelys. 33 CR-2025-0337 Consequently, law-enforcement officers were permitted to access the Blakelys' cellular telephones for the purpose of determining, among other things, whether they contained evidence of "accounts" and "user attribution" under the terms of the October warrant. Accordingly, the circuit court also erred by employing the exclusionary rule with respect to the November warrant, which was issued based on Google user data obtained through execution of the October warrant. The November warrant was issued in response to an affidavit identifying three Google user accounts associated with the Blakelys, which were discovered as a result of the execution of the October warrant. (C. 596.) Although the circuit court suppressed the evidence produced in response to the November warrant under the fruit-of-the-poisonous-tree doctrine, that ruling fails to recognize that the October warrant's language explicitly permitted law-enforcement officers to conduct -- at the very least -- limited searches of the seized digital-storage devices to determine user accounts, passwords, email addresses, and the like. In short, there was nothing poisonous about the tree that produced the fruit used to obtain the November warrant, and the circuit court clearly erred when it suppressed the responsive evidence produced by Google. 34 CR-2025-0337 Additionally, a Fourth Amendment violation does not automatically render evidence inadmissible. See *Herring v. United States*, 555 U.S. 135, 140 (2009) ("The fact that a Fourth Amendment violation occurred ... does not necessarily mean that the exclusionary rule applies."); *Illinois v. Gates*, 462 U.S. 213, 223 (1983) ("The question

whether the exclusionary rule's remedy is appropriate in a particular context has long been regarded as an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct."). In these cases, we conclude that the circuit court erred in its rigid application of the exclusionary rule under the facts of these cases. Specifically, because law-enforcement officers sought and obtained a warrant that envisioned and permitted searches of the seized digital- storage devices, and because the circuit court found "that there was no intention on the part of Inv. Bowlin to violate the rights of the Defendants," suppression of the text-message evidence was unwarranted. (C. 107.) This Court has explained: "The exclusionary rule was adopted to effectuate the Fourth Amendment right of all citizens "to be secure in their persons, houses, papers, and effects, against unreasonable searches and 35 CR-2025-0337 seizures. ..." Under this rule, evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure. *Weeks v. United States*, 232 U.S. 383 [34 S.Ct. 341, 58 L.Ed. 652] (1914); *Mapp v. Ohio*, 367 U.S. 643 [81 S.Ct. 1684, 6 L.Ed.2d 1081] (1961). This prohibition applies as well to the fruits of the illegally seized evidence. *Wong Sun v. United States*, 371 U.S. 471 [83 S.Ct. 407, 9 L.Ed.2d 441] (1963); *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 [40 S.Ct. 182, 64 L.Ed. 319] (1920). "The purpose of the exclusionary rule is not to redress the injury to the privacy of the search victim: " "(T)he ruptured privacy of the victims' homes and effects cannot be restored. Reparation comes too late." *Linkletter v. Walker*, 381 U.S. 618, 637 [85 S.Ct. 1731, 14 L.Ed.2d 601] (1965). " 'Instead, the rule's prime purpose is to deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures: " ' "The rule is calculated to prevent, not to repair. Its purpose is to deter -- to compel respect for the constitutional guaranty in the only effectively available way -- by removing the incentive to disregard it." *Elkins v. United States*, 364 U.S. 206, 217 [80 S.Ct. 1437, 4 L.Ed.2d 1669] (1960).' 36 CR-2025-0337 " 'Accord, *Mapp v. Ohio*, supra, 367 U.S. at 656 [81 S.Ct. 1684]; *Tehan v. United States ex rel. Shott*, 382 U.S. 406, 416 [86 S.Ct. 459, 15 L.Ed.2d 453] (1966); *Terry v. Ohio*, 392 U.S. 1, 29, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968). In sum, the rule is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *United States v. Calandra*, 414 U.S. 338, 347-48, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974) (footnote omitted). " 'Suppression of evidence, however, has always been our last resort, not our first impulse. The exclusionary rule generates "substantial social costs," *United States v. Leon*, 468 U.S. 897, 907, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984), which sometimes include setting the guilty free and the dangerous at large. We have therefore been "cautio[us] against expanding" it, *Colorado v. Connelly*, 479 U.S. 157, 166, 107 S.Ct. 515, 93 L.Ed.2d 473 (1986), and "have repeatedly emphasized that the rule's 'costly toll' upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application," *Pennsylvania Bd. of Probation and Parole v. Scott*, 524 U.S. 357, 364-365, 118 S.Ct.

2014, 141 L.Ed.2d 344 (1998). We have rejected "[i]ndiscriminate application" of the rule, *Leon*, supra, at 908, 104 S.Ct. 3405, and have held it to be applicable only "where its remedial objectives are thought most efficaciously served," *United States v. Calandra*, 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561

(1974) -- that is, "where its deterrence benefits

outweigh its 'substantial social costs,' " *Scott*, supra, at 363, 118 S.Ct. 2014 (quoting *Leon*, supra, at 907, 104 S.Ct. 3405).'³⁷ CR-2025-0337 "*Hudson v. Michigan*, 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006). "Indeed, the United States Supreme Court has recognized several exceptions to the Fourth Amendment exclusionary rule, including the attenuation-of-taint exception, see *Utah v. Strieff*, 579 U.S. 232, 237-43, 136 S.Ct. 2056, 195 L.Ed.2d 400 (2016), the independent-source exception, see *Murray v. United States*, 487 U.S. 533, 536-41, 108 S.Ct. 2529, 101 L.Ed.2d 472 (1988), the inevitable- discovery exception, see *Nix v. Williams*, 467 U.S. 431, 441- 48, 104 S.Ct. 2501, 81 L.Ed.2d 377 (1984), and the good-faith exception, see *United States v. Leon*, 468 U.S. 897, 905-25, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)." *Picogna v. State*, 360 So. 3d 1105, 1107-08 (Ala. Crim. App. 2022). Additionally, in *Davis v. United States*, 564 U.S. 229 (2011), the United States Supreme Court explained the following regarding the exclusionary rule: "Real deterrent value is a 'necessary condition for exclusion,' but it is not 'a sufficient' one. *Hudson v. Michigan*, 547 U.S. 586, 596 (2006). The analysis must also account for the 'substantial social costs' generated by the rule. [*United States v.*] *Leon*, [468 U.S. 897,] 907 [(1984)]. Exclusion exacts a heavy toll on both the judicial system and society at large. *Stone[v. Powell]*, 428 U.S. [465], at 490-491 [(1976)]. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. *Ibid.* And its bottom- line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. See *Herring[v. United States]*, 555 U.S. 135,] 141 [(2009)]. Our cases hold that society must swallow this bitter pill when necessary, but only as a 'last resort.' *Hudson*, supra, at 591. 38 CR-2025-0337 For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs. See *Herring*, supra, at 141; *Leon*, supra, at 910. "Admittedly, there was a time when our exclusionary- rule cases were not nearly so discriminating in their approach to the doctrine. 'Expansive dicta' in several decisions, see *Hudson*, supra, at 591, suggested that the rule was a self- executing mandate implicit in the Fourth Amendment itself. See *Olmstead v. United States*, 277 U.S. 438, 462 (1928) (remarking on the 'striking outcome of [*Weeks v. United States*, 232 U.S. 383 (1914)]' that 'the Fourth Amendment, although not referring to or limiting the use of evidence in courts, really forbade its introduction'); *Mapp [v. Ohio]*, 367 U.S. 643,] at 655, [(1961)] ('[A]ll evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in a state court'). As late as our 1971 decision in *Whiteley v. Warden*, *Wyo. State Penitentiary*, 401 U.S. 560, 568-569 [(1971)], the Court 'treated identification of a Fourth Amendment violation as synonymous with application of the exclusionary rule.' *Arizona v. Evans*, 514 U.S. 1, 13 (1995). In time, however, we came to acknowledge the exclusionary rule for what

it undoubtedly is--a 'judicially created remedy' of this Court's own making. [United States v.] Calandra, [414 U.S. 338,] 348 [(1974)]. We abandoned the old, 'reflexive' application of the doctrine, and imposed a more rigorous weighing of its costs and deterrence benefits. [Arizona v.] Evans, [514 U.S. 1,] 13 [(1995)]; see, e.g., Calandra, supra; [United States v. Janis, [428 U.S. 433, 454, n.29 (1976)]]; Stone, supra; INS v. Lopez-Mendoza, 468 U.S. 1032 (1984); United States v. Havens, 446 U.S. 620 (1980). In a line of cases beginning with Leon, 468 U.S. 897, we also recalibrated our cost-benefit analysis in exclusion cases to focus the inquiry on the 'flagrancy of the police misconduct' at issue. Id., at 909, 911. "The basic insight of the Leon line of cases is that the deterrence benefits of exclusion 'var[y] with the culpability of 39 CR-2025-0337 the law enforcement conduct' at issue. Herring, 555 U.S., at 143. When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs. Id., at 144. But when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, Leon, supra, at 909 (internal quotation marks omitted), or when their conduct involves only simple, 'isolated' negligence, Herring, supra, at 137, the ' "deterrence rationale loses much of its force," ' and exclusion cannot 'pay its way,' Leon, supra, at 919, 908, n. 6 (quoting United States v. Peltier, 422 U.S. 531, 539 (1975)). "The Court has over time applied this 'good-faith' exception across a range of cases. Leon itself, for example, held that the exclusionary rule does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid. 468 U.S., at 922. The error in such a case rests with the issuing magistrate, not the police officer, and 'punish[ing] the errors of judges' is not the office of the exclusionary rule. Id., at 916; see also Massachusetts v. Sheppard, 468 U.S. 981, 990 (1984) (companion case declining to apply exclusionary rule where warrant held invalid as a result of judge's clerical error). "Other good-faith cases have sounded a similar theme. Illinois v. Krull, 480 U.S. 340 (1987), extended the good-faith exception to searches conducted in reasonable reliance on subsequently invalidated statutes. Id., at 349-350 ('legislators, like judicial officers, are not the focus of the rule'). In Arizona v. Evans, supra, the Court applied the good-faith exception in a case where the police reasonably relied on erroneous information concerning an arrest warrant in a database maintained by judicial employees. Id., at 14. Most recently, in Herring, supra, we extended Evans in a case where police employees erred in maintaining records in a warrant database. '[I]solated,' 'nonrecurring' police 40 CR-2025-0337 negligence, we determined, lacks the culpability required to justify the harsh sanction of exclusion. 555 U.S., at 137." 564 U.S. at 237-39. In determining whether the exclusionary rule should have been applied in these cases, we consider the flagrancy of the law-enforcement officers' conduct at issue here. In these present cases, Inv. Bowlin testified at the suppression hearing that he believed that he had the authority to search the contents of the digital-storage devices once he obtained the October warrant, especially considering his statement of probable cause in the October affidavit and his clear statement of his intent to seize, search, and examine the evidence. When making its ruling on admissibility, the circuit court stated that it did

not "believe that Investigator Bowlin acted in bad faith" or "that Investigator Bowlin intentionally or deliberately tried to circumvent the Blakelys' Fourth Amendment rights." (R. 90.) It bears repeating, too, that the October warrant unquestionably did envision and authorize at least limited searches of the contents of the seized digital-storage devices to determine the existence of evidence of any user accounts, as well as to obtain user- attribution evidence. 41 CR-2025-0337 Thus, it is clear from the record that the law-enforcement officers' conduct here was not an intentional disregard for the rights of the Blakelys, or of the October warrant itself. Instead, these cases involve, at most, a negligent and isolated act by law-enforcement officers in misreading portions of the October warrant and in failing to clarify the somewhat conflicting and ambiguous language used by the issuing magistrate. We recognize the importance of ensuring that law-enforcement officers act within the confines of their authority so as to not violate the rights of citizens when executing their investigative duties. And, there is no doubt that the best practice here would have involved removing the imprecise or unintended language from the October affidavit and warrant application or to have obtained a second warrant or a clarification from the issuing magistrate. Under the facts of these particular cases, however, in which law- enforcement officers possessed the authority to search the contents of the digital-storage for user accounts and user-attribution evidence, the lack of malicious intent by the law-enforcement officers lends itself to a determination that the harsh sanction of exclusion was not justified. The social costs here are not insignificant -- it harms the public's interest in 42 CR-2025-0337 criminal adjudications when evidence is suppressed not because its seizure violated settled legal principles under the Fourth Amendment, but because it may have violated an additional legal requirement imposed by the issuing magistrate but unrelated to the existence of probable cause. Finally, we think it is clear that law-enforcement officers would have inevitably discovered the evidence at issue here. In *Nix v. Williams*, 467 U.S. 431 (1984), the United States Supreme Court recognized that evidence illegally discovered by law-enforcement officers may still be admissible if "the information ultimately or inevitably would have been discovered by lawful means." 467 U.S. at 444. "Under the inevitable-discovery exception, the prosecutor has the burden of demonstrating (1) that there is a reasonable probability that the evidence in question would have been discovered by lawful means but for the police misconduct; (2) that the leads making the discovery inevitable were possessed by the police at the time of the misconduct; and (3) that the police, before the misconduct, were actively pursuing the alternative line of investigation. *United States v. Cherry*, 759 F.2d 1196 (5th Cir. 1985); *United States v. Brookins*, 614 F.2d 1037, 1043 (5th Cir. 1980)." *Kabat v. State*, 867 So. 2d 1153, 1156 (Ala. Crim. App. 2003). The evaluation of whether law-enforcement officers would have inevitably discovered the evidence at issue in these cases is complicated 43 CR-2025-0337 by the unique circumstances presented here. These were not cases where law-enforcement officers exceeded their authority by seizing items without a warrant, by seizing items not specified in a warrant, or by going outside a specific location identified in a warrant, which are situations most often contemplated when discussing the exclusionary rule.

Rather, in these cases, the digital-storage devices were lawfully seized and secured pursuant to established probable cause to believe that the devices contained evidence of aggravated child abuse. At a minimum, the October warrant permitted law-enforcement officers to temporarily access the devices to search for user-attribution evidence and to prevent remote deletion of the data they contained. Thus, while the search may have violated the additional conditions imposed within the warrant, it did not necessarily violate of the Fourth Amendment. Further, the October affidavit contained sufficient probable cause to permit the search of the Blakelys' cellular telephones. In other words, law-enforcement officers took all the necessary steps to obtain the authority to seize the digital-storage devices and to search their contents by submitting the application and affidavit to a magistrate, failing only to take the additional, technical step of requesting a second, unnecessary 44 CR-2025-0337 warrant to search the same digital-storage devices based on the same probable cause. Had Inv. Bowlin properly understood the extralegal requirement imposed by the magistrate in the October warrant, the circumstances of these cases indicate that the contents of the digital- storage devices would have inevitably been discovered during the law- enforcement officers' investigation of the charged offenses. Based on the foregoing, we find that the circuit court erred when it granted the Blakelys' motions to suppress the evidence recovered from the search of the Blakelys' cellular telephones and other digital-storage devices, as well as when it suppressed of the results of the search conducted pursuant to the November warrant. Accordingly, the circuit court's order is reversed, and the cause is remanded for further proceedings consistent with this opinion. REVERSED AND REMANDED. Minor, J., concurs. Windom, P.J., and Kellum and Cole, JJ., concur in the result. 45