

RECEIVED

Sep 25 2026

SC Court of Appeals

STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM LEXINGTON COUNTY

Court of General Sessions
The Honorable Debra R McCaslin, Circuit Court Judge

Appellate Case No. 2025-002455

THE STATE,

Respondent,

v.

MARK ANTHONY WINCHELL,

Appellant.

INITIAL BRIEF OF RESPONDENT

ALAN WILSON
Attorney General

JOSHUA A. EDWARDS
Assistant Attorney General

Post Office Box 11549
Columbia, SC 29211
(803) 734-3727

S.R. Hubbard III
Solicitor, Eleventh Judicial Circuit

205 E. Main Street
Lexington, SC 29072
(803) 785-8352

ATTORNEYS FOR RESPONDENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii
RESPONDENT'S STATEMENT OF ISSUES ON APPEAL.....	1
STATEMENT OF THE CASE	2
FACTS	5
STANDARD OF REVIEW	8
ARGUMENT.....	9
The trial court correctly refused to suppress evidence seized from Winchell's cell phone because there was probable cause for a thorough search of the phone, any overbroad portions of the warrants were severable, and police acted in good faith reliance on the duly issued search warrants.....	9
CONCLUSION	22

TABLE OF AUTHORITIES

Cases

<u>Andresen v. Maryland</u> , 427 U.S. 463 (1976)	12
<u>Arnold v. State</u> , 309 S.C. 157, 420 S.E.2d 834 (1992)	21
<u>Berger v. State of N.Y.</u> , 388 U.S. 41 (1967)	14
<u>Chatrie v. United States</u> , 146 S. Ct. 2193 (2026)	14
<u>Commonwealth v. Green</u> , 265 A.3d 541 (Pa. 2021)	12, 15
<u>Davis v. United States</u> , 564 U.S. 229 (2011)	20
<u>Illinois v. Gates</u> , 462 U.S. 213 (1983)	19
<u>Maryland v. Garrison</u> , 480 U.S. 79 (1987)	13
<u>Massachusetts v. Sheppard</u> , 468 U.S. 981 (1984)	21
<u>Richardson v. State</u> , 282 A.3d 98 (Md. 2022)	17, 21
<u>Riley v. California</u> , 573 U.S. 373 (2014)	14
<u>State v. Carter</u> , 445 S.C. 157, 912 S.E.2d 264 (2025)	20
<u>State v. Cauthen</u> , 447 S.C. 45, 923 S.E.2d 655 (Ct. App. 2025)	12
<u>State v. Dill</u> , 423 S.C. 534, 816 S.E.2d 557 (2018)	18
<u>State v. Dupree</u> , 354 S.C. 676, 583 S.E.2d 437 (Ct. App. 2003)	9
<u>State v. Frasier</u> , 437 S.C. 625, 879 S.E.2d 762 (2022)	9
<u>State v. Goynes</u> , 303 Neb. 129, 927 N.W.2d 346 (2019)	15
<u>State v. Thompson</u> , 363 S.C. 192, 609 S.E.2d 556 (Ct. App. 2005)	19
<u>State v. Wilson</u> , 884 S.E.2d 298 (Ga. 2023)	19
<u>State v. Workman</u> , 443 S.C. 369, 905 S.E.2d 119 (2024)	21
<u>Steagald v. United States</u> , 451 U.S. 204 (1981)	11

<u>United States v. Blakeney</u> , 949 F.3d 851, 862 (4th Cir. 2020)	16
<u>United States v. Cobb</u> , 970 F.3d 319, 327 (4th Cir. 2020)	13, 16, 19
<u>United States v. Dickerson</u> , 166 F.3d 667, 694 (4th Cir. 1999)	16
<u>United States v. Leon</u> , 468 U.S. 897, 922 (1984)	20
<u>United States v. Phillips</u> , 588 F.3d 218, 225 (4th Cir. 2009)	13
<u>United States v. Ross</u> , 456 U.S. 798, 820-21 (1982)	12
<u>United States v. Williams</u> , 592 F.3d 511, 520 (4th Cir. 2010)	15
<u>United States v. Winn</u> , 79 F. Supp. 3d 904, 919–21 (S.D. Ill. 2015)	18
<u>Wheeler v. State</u> , 135 A.3d 282, 306 (Del. 2016)	18

Constitutions

S.C. Const. Art. I §10	10
U.S. Const. amend. IV	11

Secondary sources

William J. Cuddihy, <u>The Fourth Amendment Origins and Original Meaning, 602-1791</u> (Oxford 2009)	10
--	----

RESPONDENT'S STATEMENT OF ISSUE ON APPEAL

Whether the search of Winchell's cell phone constituted a "general search," and, if so, whether suppression was appropriate.

STATEMENT OF THE CASE

A Lexington County grand jury indicted Appellant Mark Winchell for criminal solicitation of a minor, attempted dissemination of obscene material to a person under 18, and attempted sexual exploitation of a minor in the first degree. He proceeded to jury trial on November 5–7, 2025, before the Honorable Debra R. McCaslin, Circuit Court Judge. Winchell was convicted as charged and sentenced to 10 years' incarceration on each charge, with the attempted exploitation of a minor sentence to be served consecutively to the other two. This direct appeal follows.

FACTS

In August 2021, Officers with the Internet Crimes Against Children Taskforce conducted a sting operation aimed at solicitation of minors via online dating apps. Tr.p.113–14. Posing as “Amy,” a 14-year-old girl living in Lexington County, an officer using an “age-regressed” photo created a profile on the Skout dating app. Tr.p.117–19. A user with the profile name “Dan” from Tybee Island, Georgia, started a chat with the officer. (State’s Exhibit #1). The conversation quickly turned to sexual subject matter after “Dan” asked “Amy” whether she liked to “Netflix and chill.” Tr.p.124. Amy responded, “LOL. Sex?” Dan responded, “Maybe. LOL. If you’re nice to me.” “Amy” then volunteered that she was “younger than [her] profile.” Tr.p.125. Dan asked if Amy was “going to get me in jail,” and Amy responded she was 14 years old. Dan responded, “I won’t tell if you won’t,” and asked if Amy was a cop, which Amy denied. Tr.p.125. The conversation continued to progress to explicit sexual subject matter, and Dan suggested they meet. Tr.p.125–26.

The Skout app automatically deletes profiles which are reported as being used by a minor misrepresenting her age, and “Dan” moved the conversation to the Kik app, which does not police its users as strictly. Tr.p.118–19; 125–26. Dan’s username was “BigBoyTool69,” and his name was listed as “Dan Duncan.” Tr.p.126. “Dan” asked “Amy” about oral and anal sex and requested nude photos. Tr.p.127. He then sent two photos of his erect penis. Tr.p.127. When “Amy” refused to send nude photos back, Dan told her he would not drive to Lexington,

lamenting: “I wanted to have some fun teaching you about sex, but I understand you told your dad you wouldn’t send pics, and I respect you for that.” Tr.p.129.

Police subpoenaed Kik’s subscriber information records. State’s Exhibit #2. The “Dan” username had previously been listed as “Dave.” Tr.p.175. The username was connected to an email address: markmoore007@yahoo.com. Tr.p.175.

Winchell’s ex-wife’s maiden name is Moore. Tr.p.213. The account had been active for more than 800 days. Tr.p.176. Kik does not require email verification, so users can enter a fake address. Tr.p.176. The records showed the account had been set up with a Samsung device, model number SM-N986U. Tr.p.177–78. The records contained login information with IP addresses related to WiFi and cellular internet. Police subpoenaed Yahoo’s records related to the markmoore007 email address. State’s Exhibit #3. The account was linked to a verified telephone number: 912-433-9187. Tr.p.186.

Police subpoenaed IP address records from Comcast and obtained subscriber information. Tr.p.188; State’s Exhibit #4. Mark Winchell was the listed subscriber, and the associated street address was in Savannah. Tr.p.189–90. The phone number associated with the account was the same number linked to the Yahoo email address. Tr.p.190. Police investigated the street address and found it was associated with Winchell’s Facebook account. Tr.p.191. Police observed photos of the residence which were consistent with the background of the explicit photos sent over Kik. Tr.p.191.

Police obtained Winchell's Facebook records. State's Exhibit #5. The same 912 phone number was associated with the Facebook account. Tr.p.194. One of the same IP addresses was also associated with the Facebook account. Tr.p.194. Based on the foregoing information, police obtained warrants for Winchell's arrest. Police seized Winchell's cell phone and searched it pursuant to a search warrant.

Tr.p.197. The extraction report was admitted as State's Exhibit #6. The phone was a Samsung, the same model documented in the Kik records. Tr.p.199. The phone number was the same one associated with the Facebook profile, Comcast records, and Yahoo email address. Tr.p.200.

Police observed July and August 2021 text messages in which Winchell identified himself as the user of the phone. Tr.p.201. Police discovered the penis pictures Winchell sent via Kik. Tr.p.202, 287. One image was taken on August 5, 2021, 9 days prior to the Kik chat. Tr.p.202. Police discovered a screenshot of a MeetMe interaction from June 2021 with the same "Dan Duncan" persona, and other photos connecting Winchell to the MeetMe and Kik apps from the summer of 2021. Tr.p.203–06. Police also discovered other texts, calls, and photos indicating Winchell was using the phone around the time of the Kik interaction. Tr.p.206–11. David Grubbs, a digital forensic investigator with the Attorney General's Office, analyzed the phone pursuant to a second search warrant and found no evidence it was ever hacked, and no evidence of VPN activity. Tr.p.289.

STANDARD OF REVIEW

On appeal from the denial of a motion to suppress based on the Fourth Amendment, the appellate court reviews the trial court's factual findings for any evidentiary support, but the ultimate legal conclusion is a question of law subject to de novo review. State v. Frasier, 437 S.C. 625, 633–34, 879 S.E.2d 762, 766 (2022). To the extent resolution of the issue depends on the existence of probable cause, the appellate court defers to the magistrate's determination if the magistrate had a "substantial basis" to issue the warrant. State v. Dupree, 354 S.C. 676, 683, 583 S.E.2d 437, 441 (Ct. App. 2003) ("The appellate court should give great deference to a magistrate's determination of probable cause.").

ARGUMENT

- I. **The trial court correctly refused to suppress evidence seized from Winchell's cell phone because there was probable cause for a thorough search of the phone, any overbroad portions of the warrants were severable, and police acted in good faith reliance on the duly issued search warrants.**

The search warrants in this case comported with both the federal and state constitutional requirements that search warrants must “particularly describ[e]” the places to be searched and things to be seized. A broad search was reasonable in this case because there was probable cause to search for all the types of data enumerated in the warrants. To the extent superfluous language rendered the warrants overbroad, these portions of the warrant are severable. And even if the warrants were deficient, suppression was not appropriate because police acted in objectively good-faith reliance on a judicial search warrant. This Court should affirm.

- A. **There was probable cause for a broad search of Winchell's phone, and the warrants were sufficiently particularized.**

The Fourth Amendment was enacted to end the practice of “general searches” that prevailed in colonial America. Colonial officials were typically authorized to conduct searches simply by virtue of their office (“ex officio” searches) or with so-called “warrants” which allowed the officials to determine when, where, and why they searched with no judicial oversight. See William J. Cuddihy, *The Fourth Amendment Origins and Original Meaning*, 602-1791 (2009). For example, a Virginia statute authorized every constable to search in “all suspected places” for

poached deer skins. Id. at 217. Most famously, the writs of assistance “left customs officials completely free to search any place where they believed [uncustomed] goods might be,” providing “no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home.” Steagald v. United States, 451 U.S. 204, 220 (1981). Customs officials in Massachusetts obtained writs of assistance “in much the same, automatic fashion that modern police officers receive uniforms and badges.” Cuddihy, supra at 491.

To end this practice, the framers of the Fourth Amendment provided that search warrants must be supported by probable cause and particularly describe the “place to be searched” and the “persons or things to be seized.” U.S. Const. amend. IV. These complimentary requirements ensure the decision whether to search a particular place is made by a neutral and detached magistrate based on sufficient cause, rather than at the unchecked discretion of an executive officer. South Carolina’s particularity requirement largely mirrors the Fourth Amendment, except that it also requires particularization of the “information to be obtained.” S.C. Const. Art. I, §10.

The warrants at issue in this case are distinguishable from “general warrants” in two basic respects. First, the warrants were issued by judges based on a case-specific showing of probable cause. Second, the warrants authorized the search of a particular piece of property—a cell phone—and specified the type of evidence police were looking for.

That the warrants authorized a thorough search of the phone does not make them “general warrants.” General warrants are impermissible because they allow police, not judges, to determine the scope of a search. A judge may, consistent with the Fourth Amendment, authorize police to search the entire contents of a cell phone.

The Fourth Amendment does not require exacting specificity in the description of each potential “place” where evidence may be found. For example, when police execute a search warrant for physical place, they may lawfully search “the entire area in which the object of the search may be found” State v. Cauthen, 447 S.C. 45, 50, 923 S.E.2d 655, 658 (Ct. App. 2025) (citing United States v. Ross, 456 U.S. 798, 820-21 (1982) (“When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand.”)); Andresen v. Maryland, 427 U.S. 463, 466 (1976) (upholding a warrant authorizing the search of an entire law office for documents relevant to a fraud investigation). This principle applies “equally to the search of a digital space” Commonwealth v. Green, 265 A.3d 541, 553 (Pa. 2021).

Likewise, the test for particularity in the description of the “things to be seized” is pragmatic. “The degree of specificity required when describing the goods to be seized may necessarily vary according to the circumstances and type of items

involved. There is a practical margin of flexibility permitted by the constitutional requirement for particularity in the description of items to be seized.” United States v. Cobb, 970 F.3d 319, 327 (4th Cir. 2020). A warrant “need not—and in most cases, cannot—scrupulously list and delineate each and every item to be seized. Frequently, it is simply impossible for law enforcement officers to know in advance exactly what records the defendant maintains or how the case against him will unfold.” Id. at 327–28 (citing United States v. Phillips, 588 F.3d 218, 225 (4th Cir. 2009)).

The proper scope of a search is tied to the probable cause supporting the search. Maryland v. Garrison, 480 U.S. 79, 84 (1987) (“By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.”). The sufficiency of a warrant’s particularity cannot be assessed without considering the facts of the case, e.g. the complexity of the investigation, the types of evidence sought, and issues of proof. Especially when a defendant engages in subterfuge, or where police must use circumstantial evidence to prove a suspect’s identity, magistrates may authorize a more thorough search than would be justified where police are looking for a single, discrete piece of evidence which they know will be found in a certain place. See Phillips, 588 F.3d at 225–26 (explaining in case where suspect engaged in “misrepresentations of his own identity,” broad search warrant was justified

because in “complex cases . . . courts have routinely upheld the seizure of items described under a warrant’s broad and inclusive language Standing alone, a particular document may appear innocuous or entirely innocent, and yet be an important piece of the jigsaw puzzle that investigators must assemble.”).

Winchell argues the warrants in this cases were “general warrants” because they authorized the seizure of “essentially all data on the phone” IBOA at 15. He argues this was impermissible given the “unique Fourth Amendment concerns” implicated by cell phone searches. As explained by the United States Supreme Court in Riley v. California, 573 U.S. 373 (2014), and Chatrie v. United States, 146 S. Ct. 2193 (2026), cell phones do present unique privacy concerns. But the Court has never held that a magistrate cannot authorize police to search the full contents of a cell phone. Rather, the Riley court held only that officers must “get a warrant” before searching a cell phone rather than relying on the search incident to arrest exception to the warrant requirement. Riley, 573 U.S. at 403.

Winchell argues the warrants for his phone were general warrants because they did not contain “temporal or categorical limitation” on the data sought. IBOA at 5. Assuming for argument’s sake that warrants for cell phones must particularly describe certain types of digital data, the warrants in this case did just that. The warrants did not generically authorize a search for “all evidence” or “evidence of any crime.” Cf. Berger v. State of N.Y., 388 U.S. 41, 58–59 (1967) (finding statute authorizing months-long wiretap without particularization of suspected crime or evidence sought allowed general searches). Rather, the warrants were extremely

detailed—i.e. particularized—in listing the types of data which were subject to search, such as “electronic correspondence,” “digital media,” and “other electronic messages, screen names, passwords, chat logs, internet searches, stored internet history, and stored third party application data.”¹ Thus the warrants did contain “categorical restrictions.”

Each type of data listed in the warrants carried a “fair probability” of identifying Winchell as a participant in the Kik chats, which was borne out by the evidence police found on the phone, e.g. text messages identifying Winchell as the phone’s user. Thus the warrants satisfied both the particularity and probable cause requirements of the Fourth Amendment. See United States v. Williams, 592 F.3d 511, 520 (4th Cir. 2010) (approving warrant authorizing search of “[a]ny and all computer systems and digital storage media . . . documents, photographs, and instrumentalities” indicative of suspected crime of harassment by computer); State v. Goynes, 143, 927 N.W.2d 346, 356 (Neb. 2019) (approving broad warrant for cell phone data because “the court had a substantial basis to find probable cause that evidence relevant to the shooting was accessible data in the areas listed”); Commonwealth v. Green, 265 A.3d 541, 554 (Pa. 2021) (holding search warrant for

¹ Some courts have distinguished general warrants from those which are “overbroad” or overinclusive in that they authorize a search both for things for which there is probable cause and things for which there is no probable cause. See United States v. Yusuf, 461 F.3d 374, 393 n.19 (3d Cir. 2006). The warrants in this case identified specific types of data, rather than a generic description of “evidence of a crime,” and thus were not general warrants. Overbreadth is discussed further infra.

all suspect's electronic devices to find child pornography need not be limited to specific time frame and was supported by probable cause).

The investigators in this case were not on a “fishing expedition” looking for evidence of unknown crimes. They were looking for evidence to prove Winchell's involvement in this specific crime, as explained in the attached affidavits. As the Cobb court explained, courts may reference the description of the suspected offense as a limitation on the scope of a search. Cobb, 970 F.3d at 328; see also United States v. Blakeney, 949 F.3d 851, 862 (4th Cir. 2020) (explaining warrant, when read with affidavit, sufficiently limited search to evidence of a specific crime where “the warrant applications in this case in fact did describe, to a reasonable degree of specificity, the crimes for which evidence was sought” and thus officers knew to limit their search for evidence of that crime); United States v. Dickerson, 166 F.3d 667, 694 (4th Cir. 1999), rev'd on other grounds, 530 U.S. 428 (2000) (holding warrant was sufficiently particular where it authorized search for “evidence of a bank robbery”).

In cases where police are looking for a single, discrete piece of evidence that can only be found in a specific part of a phone's memory, such as a single photograph or text message, a full search of the phone's contents may not be reasonable. But in this case a full search of the phone's contents was reasonable in order to discover unknown digital evidence which would “attribute” the Kik messages to Winchell. As Investigator Creech explained, police were looking for evidence of “an online persona that may predate or postdate the specific days' worth

of activity and also go toward a concept we call user attribution,” which he explained was “a pattern of who has access to that device at the time, who’s using that device with those things leading up to the event, before and after the event.” Tr.p.63, 66. Because Winchell took steps to conceal his identity, such as a fake name and profile picture, and because identity was the sole issue in this case, a thorough search was necessary to prove, through context, that Winchell was the person using the phone to send the Kik chats.² A too-restrictive search warrant would not be practical or reasonable, and reasonableness is, of course, the touchstone of the Fourth Amendment.

Winchell emphasizes that the warrants did not contain a “temporal restriction.” But even cases Winchell relies on in his brief acknowledge that a temporal limitation is not always required, depending on the facts of the case. Richardson v. State, 282 A.3d 98, 120 (Md. 2022) (recognizing that in certain cases, including “child pornography and financial crimes,” a search warrant authorizing “a broad forensic analysis of a cell phone can be appropriate”); Wheeler v. State, 135

² Winchell argues the circuit court engaged in “post hoc” rationalizations for the search, specifically citing the court’s rationale that “data can be hidden.” IBOA at 20. But Creech’s affidavit specifically explained that Winchell “had a history of using false online identities to meet women on various dating apps” and that “the data sought will show associations with the account of ‘Dan Duncan’” Creech thus explained—in the necessarily limited context of a warrant affidavit—that identity was the primary issue in the case and that a thorough search was necessary to pierce Winchell’s fake online persona. That Creech was allowed to elaborate on this explanation during the suppression hearing does not make it a “post hoc” rationalization. It is completely proper for courts to take officer testimony to better understand and explicate the constitutional interests at stake in any particular case. The court’s comment that “data can be hidden” is a consideration reasonably indicated by the affidavits and warrants.

A.3d 282, 306 (Del. 2016) (explaining warrant affidavits which were “copied and pasted from a search warrant for child pornography” were not sufficiently particularized to witness tampering incident which occurred on specific dates); United States v. Winn, 79 F. Supp. 3d 904, 919–21 (S.D. Ill. 2015) (explaining “in the case of a misdemeanor crime, it is difficult to fathom why the police would ever need, or have probable cause” to search entire contents of a phone, and finding temporal restriction should have been included for crime “which took place on one day only”).

In this case, where the purpose of the search was to “attribute” the Kik messages to Winchell through historical context, the magistrate appropriately declined to place a temporal restriction on the search. As Creech explained, had police limited the inquiry into Winchell’s 800-day-old Kik account to the immediate timeframe when the messages were sent, they would have risked missing crucial evidence, including potential exculpatory evidence.

A magistrate’s decision whether to place temporal restrictions on a warrant is intertwined with its probable cause determination. Reasonable minds could differ on how far back the phone’s contents will have a fair probability of containing evidence of the suspected crime. Reviewing courts show “great deference” to a magistrate’s probable cause determination because probable cause is not an exact science. State v. Dill, 423 S.C. 534, 542, 816 S.E.2d 557, 562 (2018). Reflecting the “preference for the warrant process, the traditional standard for review of an issuing magistrate’s probable cause determination has been that so long as the

magistrate had a ‘substantial basis for ... conclud[ing]’ that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more.” Illinois v. Gates, 462 U.S. 213, 236 (1983) (citation omitted). A broad search of Winchell’s phone’s contents was reasonable and does not violate the spirit of the Fourth Amendment.

B. Any overbroad portions of the warrants are severable.

Both warrants contained a residual clause. The first warrant provided the description of the “things to be seized” were enumerated “by way of example and not limitation.” The second warrant authorized a search for data “including but not limited to” the enumerated items. To the extent these clauses rendered the warrants overbroad, they are severable from the remainder. See State v. Thompson, 363 S.C. 192, 202, 609 S.E.2d 556, 561 (Ct. App. 2005) (Kittredge, J.) (collecting cases and explaining “overbroad portions of a search warrant may be ‘severed’ from the portions for which probable cause is found to exist, thus permitting the admission of evidence properly obtained”); Cobb, 970 F.3d at 331 (holding overbroad phrase granting permission to search for “[a]ny and all evidence of any other crimes” was severable from otherwise particularized warrant); State v. Wilson, 884 S.E.2d 298, 302 (Ga. 2023) (Peterson, J., concurring) (explaining “a general, catch-all phrase (a ‘residual clause’) in the description of places to be searched or things to be seized does not necessarily invalidate an otherwise proper warrant” where phrase can be reasonably read as relating to evidence of the crime under investigation).

The warrants specifically authorized police to search for particular types of digital data, and there was a “fair probability” each type of data could contain relevant evidence. All the data which was in fact seized fit within the enumerated categories. This renders the residual clauses superfluous and severable from the remainder of the warrants. As the Thompson court explained:

If there was probable cause to issue a search warrant describing particular items to be seized, and such items are found and those items alone constitute the basis of the criminal charge, there is no reason why some additional unsupported language in the search warrant, while to be avoided, should not be severable, particularly where no items seized thereunder are included as a basis for the criminal charge.

Id. at 202, 609 S.E.2d. at 562 (quoting People v. Mangialino, 75 Misc. 2d 698, 706–07 (N.Y. Co. Ct. 1973)).

C. Suppression was not appropriate because police acted in good faith.

Even if the warrants were not sufficiently particularized, the extreme remedy of suppression was not appropriate because police acted in good faith reliance on a duly issued warrant. “[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” United States v. Leon, 468 U.S. 897, 922 (1984) (internal citation omitted). The sole purpose of the exclusionary rule is to deter misconduct by law enforcement, i.e. “deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights.” Davis v. United States, 564 U.S. 229, 238, 246 (2011). Courts should suppress evidence only when that purpose is “clearly” served. State v. Carter, 445 S.C. 157, 163, 912 S.E.2d 264, 267 (2025). When police reasonably rely on a

judicially approved search warrant, “there is no police illegality and thus nothing to deter.” Leon, 468 U.S. at 921. “When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.” Id. at 924.

The warrants in this case were not so facially deficient that no reasonable officer would rely on them. Neither warrant authorized a limitless search for all evidence of any crime, the type of generic description which the Supreme Court has found to constitute a “general” warrant. The law in this area is far from clear, particularly in South Carolina. Both Creech and Grubbs had drafted hundreds of warrant affidavits for cell phones. Creech testified he had never included a temporal limitation. Even if this Court finds the warrants were not sufficiently particularized, the record strongly demonstrates that the officers acted in good faith reliance on the warrants. See Massachusetts v. Sheppard, 468 U.S. 981, 987 (1984) (holding officer acted in good faith despite fact that warrant failed to particularly list the things to be seized as relayed in the affidavit); Richardson, 282 A.3d at 126.

D. Harmless error.

Even if the trial court erred by admitting the extracted data, Winchell was not prejudiced because his guilt was conclusively proven by other evidence. See State v. Workman, 443 S.C. 369, 377–78, 905 S.E.2d 119, 123 (2024) (discussing harmless error standard); Arnold v. State, 309 S.C. 157, 165, 420 S.E.2d 834, 838 (1992) (discussing “harmless beyond a reasonable doubt” standard for constitutional errors). Police proved Winchell sent the chats by connecting the Kik account to his

IP address and verified phone number, and by corroborating this information through Facebook. The Kik chats were sent from the same model Samsung phone as Winchell's, from his home IP address. Further, the background of the explicit photos he sent were consistent with photos on his Facebook page. There is not a "reasonable possibility" that the additional information from the phone extraction affected the verdict. Id. This Court should affirm.

CONCLUSION

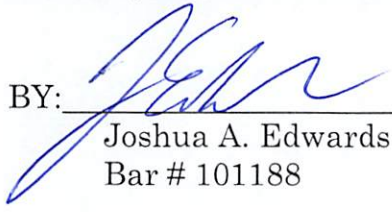
For all the foregoing reasons, it is respectfully submitted that the judgment and conviction of the lower court be affirmed.

Respectfully submitted,

ALAN WILSON
Attorney General

JOSH EDWARDS
Assistant Deputy Attorney General

S.R. HUBBARD III
Solicitor, Eleventh Judicial Circuit

BY: 

Joshua A. Edwards
Bar # 101188

Office of the Attorney General
Post Office Box 11549
Columbia, SC 29211
(803) 734-3727

ATTORNEYS FOR RESPONDENT

September 25, 2026