THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM LEXINGTON COUNTY
Court of General Sessions

Debra R. McCaslin, Circuit Court Judge

Case No. 2025-002455

The State,

Respondent,

v.

Mark A. Winchell,

Appellant.

INITIAL BRIEF OF APPELLANT

Jack B. Swerling
Curtis J. Copeland
1720 Main Street, Suite 301
Columbia, South Carolina 29201
Telephone: (803) 765-2626
Email: jackswerling@gmail.com

Attorneys for Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

STATEMENT OF ISSUES ON APPEAL 1

STATEMENT OF THE CASE 2

STANDARD OF REVIEW 4

FACTS 7

ARGUMENT 14

I. THE SEARCH WARRANTS WERE UNCONSTITUTIONAL GENERAL WARRANTS THAT LACKED THE PARTICULARITY REQUIRED BY THE FOURTH AMENDMENT 14

II. THE TRIAL COURT ERRED IN RELYING ON POST HOC JUSTIFICATIONS NEVER PRESENTED TO THE MAGISTRATE 20

III. THE GOOD FAITH EXCEPTION DOES NOT APPLY 21

IV. SOUTH CAROLINA'S CONSTITUTION PROVIDES HEIGHTENED PROTECTION AGAINST UNREASONABLE INVASIONS OF PRIVACY 23

CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Aguilar v. Texas, 378 U.S. 108 (1964) 20
Maryland v. Garrison, 480 U.S. 79 (1987) 14
Messerschmidt v. Millender, 565 U.S. 535 (2012) 20
Richardson v. State, 481 Md. 423 (Md. 2022) 5, 15, 16
Riley v. California, 573 U.S. 373 (2014) 14, 15, 16, 18, 22, 25
Stanford v. Texas, 379 U.S. 476 (1965) 14
State v. Brockman, 339 S.C. 57, 528 S.E.2d 661 (2000) 4, 5, 6
State v. Forrester, 343 S.C. 637, 541 S.E.2d 837 (2001) 23
State v. Hall, 293 S.C. 331, 360 S.E.2d 323 (1987) 15
State v. Khingratsaiphon, 352 S.C. 62, 572 S.E.2d 456 (2002) 4, 5, 6
State v. Wilson, 315 Ga. 613 (Ga. 2023) 5, 16
United States v. Burton, 756 F. App'x 295 (4th Cir. 2018) 17, 18, 22
United States v. Leon, 468 U.S. 897 (1984) 21
United States v. Winn, 79 F. Supp. 3d 904 (S.D. Ill. 2015) 17, 19, 22, 23
Wheeler v. State, 135 A.3d 282 (Del. 2016) 5, 16, 17

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. IV 1, 5, 14, 15, 22, 23
S.C. Const. art. I, § 10 ..... 1, 5, 23, 24

STATEMENT OF ISSUES ON APPEAL

I. DID THE TRIAL COURT ERR IN DENYING APPELLANT'S MOTION TO SUPPRESS THE FRUITS OF SEARCH WARRANTS THAT AUTHORIZED LAW ENFORCEMENT TO SEARCH AND SEIZE ALL DATA ON APPELLANT'S CELL PHONE WITHOUT ANY TEMPORAL LIMITATION OR CONTENT-BASED RESTRICTION, THEREBY CONSTITUTING UNCONSTITUTIONAL GENERAL WARRANTS IN VIOLATION OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION AND THE HEIGHTENED PROTECTION OF ARTICLE I, SECTION 10 OF THE SOUTH CAROLINA CONSTITUTION?

II. DID THE TRIAL COURT ERR IN RELYING ON POST HOC JUSTIFICATIONS PROVIDED BY LAW ENFORCEMENT AT THE SUPPRESSION HEARING TO UPHOLD THE VALIDITY OF THE SEARCH WARRANTS, WHERE SUCH INFORMATION WAS NEVER PRESENTED TO THE ISSUING MAGISTRATE?

III. DID THE TRIAL COURT ERR IN ALTERNATIVELY APPLYING THE GOOD FAITH EXCEPTION TO THE EXCLUSIONARY RULE?

STATEMENT OF THE CASE

This is a direct appeal from a criminal conviction in the Lexington County Court of General Sessions. The Appellant, Mark Anthony Winchell, was charged with attempted dissemination of obscene material to a person under the age of eighteen, criminal solicitation of a minor, and attempted sexual exploitation of a minor, first degree. The charges arose from an online undercover operation conducted by law enforcement on August 14, 2021.

Prior to trial, on October 29, 2025, the Appellant filed a Motion to Suppress the fruits of two search warrants executed on his cell phone. The first warrant was issued on September 30, 2021, and the second on June 2, 2023. Both warrants authorized law enforcement to search and seize all data on the Appellant's Samsung Galaxy Note 20 cell phone without any temporal limitation or content-based restriction.

A hearing on the Motion to Suppress was held on November 5, 2025, before the Honorable Debra R. McCaslin. Special Investigator Adam Creech of the Lexington County Sheriff's Department testified for the State. The defense argued that both warrants were unconstitutional general warrants that failed to describe the data to be searched and seized with sufficient particularity, in violation of the Fourth Amendment to the United States Constitution and the heightened protection against unreasonable invasions of privacy afforded by Article I, Section 10 of the South Carolina Constitution.

The trial court denied the Motion to Suppress in an oral ruling, finding that the warrants were sufficiently particularized and that the good faith exception applied in any event. The trial proceeded from November 5 through November 7, 2025. On November 7, 2025, the jury returned guilty verdicts on all charges. The court sentenced the Appellant to twenty years' imprisonment.

On November 17, 2025, the Appellant filed a Motion for Reconsideration and for a New Trial, again challenging the denial of the Motion to Suppress. The defense further argued that, in denying the motion, the trial court improperly considered factual justifications for the breadth of the warrants that were never presented to the issuing magistrate. On December 2, 2025, the trial court summarily rejected these arguments in a written order. This appeal timely followed.

The ultimate issue on appeal is whether the trial court erred in denying the Appellant's Motion to Suppress evidence obtained pursuant to overbroad, unparticularized search warrants that Appellant contends amounted to general warrants.

The defense submits the trial court's finding of particularity is unsupported by the evidence, *i.e.*, the warrant and its supporting affidavit. The denial of the motion to suppress was independently tainted by a clear error of law insofar as the trial court considered factual justification for the warrants that were never provided to the issuing magistrate. Finally, Appellant contends that the good faith exception to the exclusionary rule should not apply.

STANDARD OF REVIEW

In *State v. Khingratsaiphon*, 352 S.C. 62, 572 S.E.2d 456 (2002), the South Carolina Supreme Court adopted the standard of review articulated in *State v. Brockman*, 339 S.C. 57, 66, 528 S.E.2d 661, 666 (2000), for appellate review of a trial court's ruling on a motion to suppress based on Fourth Amendment grounds. Under *Brockman*, the appellate court applies a deferential standard: "We will review the trial court's ruling like any other factual finding and reverse if there is clear error. We will affirm if there is any evidence to support the ruling." *Khingratsaiphon*, 352 S.C. at 70, 572 S.E.2d at 460 (quoting *Brockman*, 339 S.C. at 66, 528 S.E.2d at 666).

This Court should exercise caution, however, in mechanically applying that deferential standard to the issue presented in this appeal. Both *Khingratsaiphon* and *Brockman* involved straightforward factual disputes about the reasonableness of a particular officer's conduct during a warrantless encounter—whether specific and articulable facts supported a *Terry* frisk in *Khingratsaiphon* and whether the totality of the circumstances justified a traffic stop in *Brockman*. In each case, the trial court's ruling turned on its assessment of testimonial evidence adduced at the suppression hearing: the credibility of witnesses, the weight of the facts, and the reasonable inferences to be drawn therefrom. The deferential standard makes sense in that context because the trial court, having observed the witnesses and weighed the evidence firsthand, occupies a superior vantage point.

The issue in this appeal is fundamentally different. This case does not ask this Court to second-guess the trial court's resolution of a factual dispute. No material facts are in contest. The warrants themselves are in the record, their language is undisputed, and the testimony of Special Investigator Creech regarding the scope of the search and seizure is uncontroverted—indeed, it is the State's own witness who confirmed that the warrants authorized seizure of all data on the phone

without temporal or categorical limitation. The questions presented are purely legal: whether search warrants that authorize law enforcement to search and seize the entirety of a citizen's cell phone data—without reference to a specific crime, without temporal boundaries, and with expressly non-exhaustive catch-all language—satisfy the Fourth Amendment's particularity requirement and the heightened privacy protections of Article I, Section 10 of the South Carolina Constitution.

No South Carolina appellate court appears to have addressed the question of how the particularity requirement applies to modern digital searches. The motion to suppress filed below acknowledged as much. The trial court was thus writing on a blank slate in this jurisdiction, and its resolution of the issue carries no special institutional competence warranting deference. As the Supreme Court of Maryland recognized in addressing the identical legal question in *Richardson v. State*, 481 Md. 423 (2022), the constitutional validity of a search warrant is a mixed question of law and fact in which the appellate court accepts the trial court's factual findings unless clearly erroneous, but "[t]he ultimate determination of whether there was a constitutional violation . . . is an independent constitutional evaluation that is made by the appellate court alone." *Id.* (quoting *State v. Carter*, 472 Md. 36, 55 (2021)). Critically, the *Richardson* court emphasized that it reviews "any questions of law de novo, without any special deference to the views of the lower courts." *Id.* Every sister jurisdiction to consider this precise issue—whether overbroad, unparticularized cell phone search warrants satisfy the Fourth Amendment—has applied de novo review to the legal question. *See Wheeler v. State*, 135 A.3d 282, 298 (Del. 2016) (applying de novo review to legal conclusions regarding denial of suppression motion); *State v. Wilson*, 315 Ga. 613 (2023) (applying de novo review to trial court's application of law to undisputed facts regarding cell phone warrant particularity).

Moreover, the *Khingratsaiphon* court itself cautioned that its deferential standard does not strip the appellate court of its independent review function: "Contrary to petitioner's claim, *Brockman* does not hold the appellate court may not conduct its own review of the record to determine whether the trial judge's decision is supported by the evidence." 352 S.C. at 70, 572 S.E.2d at 460. That independent review is particularly vital here, where the trial court's treatment of a complex constitutional question of first impression was remarkably cursory. The trial court denied the pretrial motion to suppress from the bench without written findings, without citation to any authority, and without analysis of extensive authority presented by the defense. When the defendant sought reconsideration in a detailed post-trial motion, the trial court's written order disposed of the suppression issue in a single paragraph, stating only that "[t]he pretrial suppression hearing fully addressed and resolved the warrant challenges, with the warrants upheld as valid under the Fourth Amendment and South Carolina law." The order contained no legal analysis, cited no authority, and did not address any of the specific arguments raised in the motion—including the defendant's argument that the court had improperly relied on *post hoc* testimony never presented to the issuing magistrate, and the defendant's argument under Article I, Section 10 of the South Carolina Constitution, which the court simply ignored.

Where, as here, a trial court resolves a novel and weighty constitutional question without engaging the legal arguments and without citing any authority, there is no legal analysis to which this Court could defer even if deference were otherwise warranted. The question of what level of particularity the Fourth Amendment and the South Carolina Constitution demand of cell phone search warrants is a question of law that this Court is in an equally—if not better—position to resolve. This Court should therefore conduct its own independent analysis of whether the warrants at issue satisfied constitutional requirements, giving no particular deference to the trial court.

FACTS

A. The Underlying Investigation

Between August 11 and August 15, 2021, law enforcement officers from the South Carolina Internet Crimes Against Children (ICAC) Task Force conducted an undercover chat operation at the Lexington County Sheriff's Department. During this operation, an undercover officer posed as a fourteen-year-old female online using two particular applications: (1) "Skout" a/k/a "MeetMe" and (2) "Kik." These messaging applications allow users to create a profile and transmit media and messages. These two applications were the only medium through which the undercover officer communicated in this case.

On August 14, 2021, a user with profile name "Dan Duncan" contacted the undercover persona. According to the warrant affidavit, the online conversation lasted several hours that day. The user sent inappropriate messages and two images of a nude adult male to the undercover officer. Law enforcement traced the "Dan Duncan" account to an IP address that resolved to Appellant's home address. Law enforcement did not have any reason to believe the Appellant committed any other crime apart from the suspected conduct on Skout/MeetMe and Kik on August 14, 2021. Tr. at 64:14-17. Law enforcement declined to send search warrants to Skout/MeetMe

On September 29, 2021, the Appellant was arrested by the U.S. Marshals Service in Savannah, Georgia. His cell phone, a Samsung Galaxy Note 20, was seized during the arrest.

B. The Search Warrants

On September 30, 2021, Special Investigator Adam Creech obtained a search warrant for the Appellant's cell phone. In his probable cause affidavit, he informed the magistrate that "data sought" was needed to (1) potentially associate the Appellant to the suspect Kik account, and (2) find "artifacts," or evidence, to corroborate the occurrence of the chats on August 14, 2021. *See*

Tr. at 61:16-20 (Q: [Y]ou describe just two essentially specific categories of things, what is going to tie your suspect to the account, and then data that may corroborate the occurrence of that chat on August 14th. Correct? A: Correct."). The evidence actually sought by law enforcement—according to the affidavit—was well-defined and tailored to the facts of the crime under investigation. The warrant itself, however, authorized the search and seizure of every conceivable piece of data on the phone:

> *By way of example and not limitation*, call detail records, to include incoming/outgoing phone calls and SMS/MMS text messages, including the content thereof, data events date, time, and duration of same. Also sought are *all third party applications and associated application data*. Digital media is also sought, which may include, but not be limited to, explicit digital videos, digital images, digital photographs, and digital documents. Electronic correspondences and other electronic data are also sought, which may include emails, instant messages, other electronic messages, screen names, passwords, chat logs, Internet searches, stored Internet history, and stored third party application data. Any of the above are sought on the phone's internal memory, as well as on any associated Micro SD card or other external storage media. Also sought are the contents of any recoverable deleted data, which may contain any of the above items.

(emphasis added). Critically, the warrant stated that the listed categories of data were "not" a "limitation" on the scope of the search. Tr. at 65:7-10. Special Investigator Creech testified at the suppression hearing that the breadth of this search warrant "covered" categories of data even though "we're not asking for it." Tr. at 67:14-15; *see also* Tr. at 67:19-21 (Q: "This covers you looking at anything in the phone. Does it not?" A: "Well, of course . . . .").

On June 2, 2023, due to the timing of the defense expert's examination, Special Investigator David Grubbs obtained a second search warrant for the same cell phone. This warrant was similarly unbounded, authorizing the seizure of "all data" on the phone "including but not limited to" specified types, again with no temporal restrictions whatsoever:

> A search for *any and all* saved, archived, encrypted, and/or deleted data *including but not limited to* email, ledgers, lists, records, documents, digital artifacts from programs used, digital photographs, and digital videos contain [sic] data depicting

> minors engaged in sexual activity, and/or posed in lewd or lascivious manners taken from, derived from or contained in the electronic components, cell phones, computer systems, and/or storage media described in the below listed systems and/or devices seized pertaining to this investigation of Sexual Exploitation of a Minor under our South Carolina Code of Laws.

(emphasis added). Notably, while this description of property referenced an investigation into actual "sexual exploitation of a minor" and a search for child sexual abuse material, Grubbs' probable cause affidavit confirmed that the facts only established probable cause to believe the Appellant engaged in criminal solicitation.[1]

Neither warrant contained any date range limitation. Neither warrant restricted the search to data related to the specific messaging applications at issue (Skout/MeetMe and Kik) identified in the investigation. Neither warrant limited the search to a reasonable timeframe surrounding August 14, 2021, when the alleged offense occurred. Both warrants, by their own terms, allowed law enforcement to search through and seize anything on Appellant's cell phone whether it constituted evidence of the crime under investigation or not. To be sure, the first warrant did not identify any crime under investigation, and the second warrant referenced a crime contradicted by its own supporting affidavit.

C. Special Investigator Creech's Testimony

At the suppression hearing, Special Investigator Creech testified about the warrants and the forensic extraction of the Appellant's phone. His testimony revealed both the capabilities of modern forensic software to tailor searches—by timeframe and content type—and law enforcement's deliberate choice not to do so in this case (or any other case).

---

[1] No child sexual abuse material was transmitted during the conversation on August 14, 2021, and no child sexual abuse material or inappropriate conversations with a minor were found among approximately 1.6 million artifacts within the Appellant's cell phone. *See* Tr. at 294:4-13.

Special Investigator Creech acknowledged that the forensic software he used, Cellebrite, has the capability to filter data by timeframe before it is viewed:

Q: You have the ability to filter data from an extraction by time frame within [the] Cellebrite application?

A: You can run a timeline report within Cellebrite . . . .

Tr. at 62:15-17.

Q: [O]nce you process [the data] through Cellebrite you can filter it by time. Can you not?

A: You can . . . [but] we're going to be missing critical data . . . .

Tr. at 62:24-63:1.

When pressed further, Special Investigator Creech conceded the point directly:

Q: [T]he answer to the question "can you filter the data by timeframe" is yes. Correct?

A: It is possible, but it would not be a standard investigative practice.

Tr. at 63:15-18.

When defense counsel noted that all of the electronic service provider (ESP) warrants in this case contained reasonable temporal limitations on the data sought, Special Investigator Creech attempted to distinguish ESP warrants from cell phone search warrants, but the distinction underscored the point: law enforcement knew how to draft particularized warrants—focused on a relevant timeframe—but chose not to do so. *See* Tr. at 62:10-14.

Special Investigator Creech further acknowledged that searches through a digital forensic extraction can be narrowed by the type of data:

Q: [Y]ou can filter data [to] search just for things related to Kik. Can't you? Now we're talking about types of data.

A: You can but if you're—

Q: Okay. Can you look at the description of property here?

A: Certainly.

Q: [Y]ou requested permission to seize not just Kik, not just Skout[/]MeetMe, [but] all third-party applications and associated application data. There are all kinds of applications on a phone—

A: Certainly.

Tr. at 65:10-20.

Moreover, counsel for the State confirmed that current methodologies allow for targeted searches for particularized types or categories of data. Tr. at 38:23-25. ("So, for example, if you're looking—this case involves Kik, which is a chat application, so they type in 'Kik,' and then when they get hits back for 'Kik,' that may be relevant.").

The State's primary argument during the suppression hearing was that the warrants "did not say those magic words of 'I want anything and everything that's on this device." Tr. at 44:12-13; *see also* Tr. at 39:15-16 ("Neither one of these warrants say they want to rummage through the entire cell phone."); Tr. at 54:10-12 ("They don't have that magic language of trying to seize the entirety of the contents of the cell phone . . . ."). This proposition is refuted by the warrants themselves and law enforcement's uncontradicted testimony:

Q: This [warrant] covers you looking at anything in the phone. Does it not?

A: Well, of course . . . .

Tr. at 67:19-21.

The resulting Cellebrite report was over 13,000 pages in length. Tr. at 75:17-18; Tr. at 224:10-11. As Special Investigator Creech confirmed again during the trial, "in this search, absolutely nothing in the phone was off-limits for you to go through." Tr. at 224:18-19. Special Investigator Creech agreed: "We wouldn't have been doing a full acquisition of the data if we wouldn't have been looking at that data in its totality." Tr. at 224:20-22; *see also* Tr. at 224:23-225:1. ("Q: You had the ability to search through every single piece of data stored on that cell phone. Correct? A: Every piece of data that Cellebrite was able to interpret at that time, yes.").

Then, instead of suggesting that the warrants were not unlimited authorizations to search and seize everything in the phone, the State had Special Investigator Creech attempt to justify why he wanted to seize each enumerated category of data listed in the initial warrant. *See generally* Tr. at 68-71. Setting aside that the enumerated categories of data were not an exhaustive list of what the warrant authorized, Creech went far beyond what he originally claimed to be searching for in his affidavit. Only during the hearing did Creech claim a need to learn things like Appellant's "speech patterns" and amorphously-defined "pattern of life behavior." *See* Tr. at 68:16-20. Defense counsel ultimately objected to this line of questioning on the basis of relevance, as there had been no foundation that any of these *post-hoc*, line item justifications had been presented to the magistrate who issued the warrants. Tr. at 70:19-25. The trial court overruled the objection and considered Special Investigator Creech's after-the-fact justifications. *See* Tr. at 70:24-25.

At bottom, Special Investigator Creech explained that he was to be the final arbiter on the breadth of his discretion to search—with a general warrant in hand: "We have to *look at it all* to make the appropriate investigative decisions." Tr. at 63:13-14 (emphasis added).

D. The Trial Court's Ruling

In the trial court's oral ruling denying the Motion to Suppress, the court stated:

> [T]he motion to suppress is still denied. I think the warrant is sufficiently particularized, specifying targeted data despite lacking a precise timeframe. The cell phone's data is unique, it's ongoing in nature, and it's crucial here. Probable cause gave the ability to look through the phone for child pornography and apps that can be deleted, and data can be hidden. I was going to tell you, it would be very unusual to look into a phone and there be a file there that says hey, look at me, this is all the child pornography. It is normally hidden, deleted, somewhere in other apps. Accordingly, older data pointing to when an app was downloaded or used may still be relevant and is not overly broad. There is no specific amount of time required to see if there is a prior message evidencing when the app in question was installed or a later message evidencing when the app was deleted.
>
> Regardless, here, the good faith exception applies. Special Investigator Creech, with over a decade of experience in such warrants, reasonably relied on the approved warrant that had undisputed probable cause. Moreover, special investigator Creech's reliance on the warrant was objectively reasonable, so that's my ruling on that.

Tr. at 78:1-79:21. The trial court's ruling did not address extensive case law from multiple jurisdictions holding that warrants with nearly identical search authorizations are unconstitutional general warrants. The court did not grapple with the fact that the warrants authorized search and seizure of all data on the phone regardless of its relevance to the investigation—which never involved actual or suspected possession, receipt, or distribution of child pornography. And the court relied heavily on Special Investigator Creech's *post hoc* explanations for why an unlimited search was necessary—testimony that was never presented to the issuing magistrate.

ARGUMENT

I. THE SEARCH WARRANTS WERE UNCONSTITUTIONAL GENERAL WARRANTS THAT LACKED THE PARTICULARITY REQUIRED BY THE FOURTH AMENDMENT.

A. The Constitutional Framework

The Fourth Amendment provides 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*." U.S. Const. amend. IV (emphasis added). This particularity 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." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *State v. Thompson*, 363 S.C. 192, 200, 609 S.E.2d 556, 560 (Ct. App. 2005).

The Framers' concern was not abstract. The Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). General warrants are "constitutionally intolerable," *Stanford v. Texas*, 379 U.S. 476, 486 (1965), and "in fact one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403; *see also State v. Austin*, 306 S.C. 9, 11, 409 S.E.2d 811, 813 (Ct. App. 1991) ("The King's ministers issued general warrants . . . which eventually led to the 'shot heard round the world.'").

The Supreme Court's landmark decision in *Riley* recognized that cell phones present unique Fourth Amendment concerns. Modern cell phones hold for many Americans "the privacies of life"—information well "worthy of the protection for which the Founders fought." 573 U.S. at 403. A cell phone "not only contains in digital form many sensitive records previously found in

the home; it also contains a broad array of private information never found in a home in any form." *Id.* at 396-97. Indeed, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." *Id.* at 396.

B. The Warrants in This Case Were General Warrants

The warrants in this case epitomize the general warrants that the Fourth Amendment was designed to prohibit. The 2021 warrant authorized seizure of essentially all data on the phone, including, but not limited to, call records, text messages, emails, chat logs, digital images, videos, documents, passwords, internet history, application data, and "any recoverable deleted data." The warrant expressly stated that the listed categories were "not" a "limitation" on its scope. The unlimited nature of the warrant was fully endorsed by testimony of the officer who obtained and executed it. Knowing that an exhaustive search would reveal the Appellant's "whole pattern of life behavior" through an indefinite period, Special Investigator Creech nevertheless claimed in conclusory fashion that an unlimited search was necessary to make "appropriate investigative decisions." Tr. at 68:19-20; 63:13-14 ("We have to look at it all . . . .").

The South Carolina Supreme Court has long recognized that warrants can become so "impermissibly broad and so nondescriptive as to render the resulting warrant a general warrant, in violation of the Fourth Amendment to the United States Constitution." *State v. Hall*, 293 S.C. 331, 333, 360 S.E.2d 323, 324 (1987) (citation omitted). And courts across the country have held that warrants with virtually identical, all-encompassing language are unconstitutional in the particular context of digital forensic extractions like those conducted here.

In *Richardson v. State*, 481 Md. 423 (2022), the Supreme Court of Maryland confronted a cell phone search warrant that "allowed police to search everything on the device." *Id.* at 439. Citing *Riley* in the first line of the decision, the court ultimately held: "The warrant that authorized

the search . . . did not satisfy the particularity requirement of the Fourth Amendment, *as it allowed police to search everything on the device*." *Id.* at 443 (emphasis added).

The *Richardson* court explained that "[t]he particularity requirement is arguably of even greater importance in the context of computers and smartphones than it is in the physical world, given the ability of smartphones to store 'millions of pages of text, thousands of pictures, or hundreds of videos.'" *Id.* at 432 (quoting *Riley*, 573 U.S. at 394). To be sure, law enforcement in this case seized over 1.6 *million* data artifacts. Tr. at 294:11-13. But the *Richardson* court emphasized: "Without understating the problem posed by a general warrant to search someone's home prior to the digital age, a general warrant to search a computer or a smartphone today magnifies that problem exponentially." 481 Md. at 432.

Similarly, in the murder case of *State v. Wilson*, 315 Ga. 613 (2023), the Supreme Court of Georgia affirmed the suppression of evidence from a warrant that authorized seizure of "any and all stored electronic information, including but not limited to" various specific categories of data on the defendant's cell phones. The court rejected the State's argument that the warrant's language could possibly be read as limiting:

> [T]hat language clearly states that "[t]he foregoing described property"—that is, "any and all stored electronic information" on the phones—"constitutes evidence connected with the crimes." This language cannot plausibly be read, as the State suggests, to limit the otherwise limitless authorization to search for and seize any and all data that can be found on Wilson's cell phones.

Id. at 619. The Delaware Supreme Court reached the same conclusion—that a search warrant failed to satisfy the particularity requirement—in *Wheeler v. State*, 135 A.3d 282 (Del. 2016). In that case, the State conceded that the challenged warrants authorizing seizure of "any and all data" were copied-and-pasted templates. *Id.* at 298. The court conducted an extensive historical analysis of general warrants, observing that "[o]ur nation's constitutional history and jurisprudence reflects

a long-standing hostility towards general warrants. General warrants, when employed by the government, afford officials 'blanket authority' to indiscriminately search persons, houses, papers, and effects." *Id.* at 292. The *Wheeler* court held that the challenged warrants were "in the nature of 'general warrants' in violation of the United States and Delaware Constitutions" and reversed the lower court's contrary holding. *See id.* at 287.

Finally, in *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015), the court confronted a cell phone warrant with language strikingly similar to the warrants here. The warrant sought:

> *any or all* files contained on said cell phone and its SIM Card or SD Card to *include but not limited to* the calendar, phonebook, contacts, SMS messages, MMS messages, emails, pictures, videos, images, ringtones, audio files, all call logs, installed application data, GPS information, WIFI information, internet history and usage, any system files on phone, SIM Card, or SD Card, or any data contained in the cell phone, SIM Card or SD Card to include deleted space.

Id. at 910-11 (emphasis added). The *Winn* court found this language "invited the police to conduct an illegal general search." *Id.* at 918-19. While this language authorized search and seizure of everything on the phone, the court emphasized that "the police did not have probable cause to believe that *everything* on the phone was evidence of the crime." *Id.* at 919 (emphasis in original). The court ordered suppression of all evidence obtained from the cell phone, explaining: "This case goes to the very heart of what the Fourth Amendment was designed to prohibit—general warrants and general searches." *Id.* at 926.

The Fourth Circuit's decision in *United States v. Burton*, 756 F. App'x 295 (4th Cir. 2018), while ultimately applying the good faith exception to save the evidence in that case, provides powerful support for suppression in the instant case because of the temporal distinction between the two matters. In *Burton*, the district court expressly found that the search warrant authorizing search and seizure of "[t]he entire contents of the cellphones" was "constitutionally overbroad," relying extensively on *Winn* for the proposition that warrants must be "limited by the facts of the

underlying offense, particularly where that offense is limited to a particular time frame and location." *Burton*, No. 4:16-cr-00071-AWA, at *11-12 (E.D. Va. Apr. 7, 2017).

On appeal, the Fourth Circuit assumed the warrants in *Burton* were unconstitutional and declined to suppress solely because the warrant was executed in 2011—three years before *Riley v. California* and seven years before *Carpenter v. United States*—when "the legal authority governing the scope of permissible searches of electronic devices was less developed than it is today." *Id.* at *16. Critically, the Fourth Circuit explained that "[a]t that time, neither our precedent nor that of the Supreme Court had developed the robust privacy protections for cell phone users that are applicable today," and that "[g]iven the *state of the law in 2011* . . . we conclude that application of the exclusionary rule in this case would not deter officers from committing violations of the Fourth Amendment." *Burton*, 756 F. App'x at 302 (emphasis added). The necessary implication of *Burton* is that officers executing warrants *after* the Supreme Court's decisions in *Riley* and *Carpenter* can no longer claim the benefit of legal uncertainty. The "robust privacy protections" the Fourth Circuit referenced are now firmly established, and an officer who seeks a warrant authorizing seizure of all data on a cell phone without temporal limitations or other constraints tethering the search to its probable cause bases does so in the face of clearly developed law.

The warrants in the instant case were executed in September 2021 and June 2023, a full decade after *Burton*'s 2011 warrants and years after *Riley*, *Carpenter*, and *Burton* itself clarified the constitutional landscape. Under *Burton*'s own reasoning, the good faith exception cannot shield the fruits of these searches because any deterrent value that suppression lacked in 2011 is now fully present: officers are on notice that cell phones fall squarely within the heartland of the Fourth

Amendment, and excluding evidence obtained through such warrants serves the exclusionary rule's core purpose of discouraging unconstitutional police practices.

C. The Warrants Lacked Any Temporal Limitation

A critical deficiency of the warrants in this case was the complete absence of any temporal limitation. The affidavit supporting the 2021 warrant described conduct that allegedly occurred on a single day: August 14, 2021. Yet the warrant authorized seizure of all data on the phone, regardless of when it was created.

The *Winn* court addressed this precise issue:

> [T]he warrant should have specified the relevant time frame. The alleged criminal activity took place on one day only—June 18, 2014—and the police were looking for photos or videos taken that same day. There was nothing in the complaint indicating that any data created prior to that date was connected to the suspected public indecency.

79 F. Supp. 3d at 921. The same essential analysis applies here. The alleged criminal activity took place on August 14, 2021. The warrant affidavit described conversations on particular messaging applications during a particular timeframe. Courts—and reasonably informed law enforcement officers—have long understood that "probable cause, with time, dissipates." *State v. Winborne*, 273 S.C. 62, 64, 254 S.E.2d 297, 298 (1979). Yet the warrants in this case authorized search and seizure of all data from the phone's entire existence, including data predating the alleged offense by years. To be sure, law enforcement was authorized to review private conversations dating back to 2011 during this investigation. *See* Tr. at 49:13-21.

Special Investigator Creech's own testimony underscores the constitutional problem. He acknowledged that he had the capability to filter his search to a reasonable timeframe—as he did with every other ESP warrant—but deliberately chose not to do so for the cell phone. *See* Tr. at 62:15-17; 63:15-18. This was not a case where temporal limitations were impractical—it was a

case where law enforcement chose to seek unlimited access despite having the facts and the tools to narrow the search. Moreover, the 2021 warrant affidavit itself makes apparent that law enforcement knew exactly how to describe, with particularity, the evidence they actually sought: (1) evidence associating Appellant to the user account, and (2) evidence substantiating that the August 14 conversation occurred on that particular device.

II. THE TRIAL COURT ERRED IN RELYING ON *POST HOC* JUSTIFICATIONS NEVER PRESENTED TO THE ISSUING MAGISTRATE.

"It is elementary that in passing on the validity of a warrant, the reviewing Court may consider *only* information brought to the magistrate's attention." *Aguilar v. Texas*, 378 U.S. 108, 109 n.1 (1964) (emphasis in original) (citation omitted). The State "cannot rationalize a search *post hoc* on the basis of information they failed to set forth in their warrant application." *Messerschmidt v. Millender*, 565 U.S. 535, 568 n.8 (2012).

In violation of this principle and over a defense objection at the suppression hearing, Tr. at 70:19-25, Special Investigator Creech was permitted to provide extensive testimony explaining the factual bases he contended should justify a search he understood to be limitless. Setting aside whether his explanations were credible in the context of an investigation into a discrete criminal conversation, none of this testimony was permissible: it was never presented to a magistrate. Indeed, it was wholly inconsistent with the affidavit presented to the magistrate.

The warrant application consisted solely of the written affidavit, and there is no evidence that the written affidavit was buttressed by oral testimony to the magistrate.

The trial court's oral ruling, however, was based substantially on Special Investigator Creech's *post hoc* explanations at the hearing and not on the probable cause affidavit. The court echoed that "data can be hidden" and that investigators needed "the ability to look through the phone for child pornography and apps that can be deleted." Tr. at 79:5-6. These rationales came

solely from Special Investigator Creech's testimony, not from the warrant application, which did not even seek or mention evidence of child pornography. Although the 2023 warrant did seek such evidence, its supporting affidavit made clear that the crime under investigation was criminal solicitation alone, *i.e.*, a conversation that law enforcement knew did not involve transmission of any child pornography.

This reliance on *post hoc* justifications was legal error. Under decades-old precedent, the relevant question was whether the issuing magistrate had a substantial basis to issue an unlimited warrant based on the information presented. If the magistrate was not told why unlimited access to the phone was necessary despite two limited categories of data sought in the affidavit, the warrant cannot be upheld on the basis of reasons later articulated at a suppression hearing. Moreover, if such explanations could ever justify searches as broad as those authorized in this case, the rule must be that general warrants are always acceptable for cell phones.

Hedging against its position that the warrants were not in fact unlimited, all the State accomplished below was improper *post hoc* rationalization for the unlimited breadth of the warrants. whether the affidavit alone justified the admittedly all-encompassing search through the defendant's phone.

The motion for reconsideration was denied without addressing the prohibition against reliance on material not presented to the magistrate; rather, the trial court specified that it again considered this witness' testimony in reaching its decision.

III. THE GOOD FAITH EXCEPTION DOES NOT APPLY.

The good faith exception to the exclusionary rule, established in *United States v. Leon*, 468 U.S. 897 (1984), does not apply where "the warrant is so facially deficient—*i.e.*, *in failing to*

particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* at 923 (emphasis added).

The warrants in this case are facially deficient because they are facially general warrants. There is nothing *not* subject to search and seizure under them. They authorize the search and seizure of all data on the phone, expressly without limitation. No reasonable officer could presume such a warrant to be valid in light of what was known about the suspected activity at the time the warrants were obtained.

The state of the law regarding the privacy interests of cell phones has been clear since *Riley* in 2014. Cell phones deserve heightened Fourth Amendment protection. Warrants for cell phone searches must be particularized. General warrants are constitutionally intolerable. These principles are not new or uncertain.

The Fourth Circuit's decision in *United States v. Burton*, 756 F. App'x 295 (4th Cir. 2018), illustrates this point. In *Burton*, the court applied the good faith exception to a cell phone warrant executed in 2011—three years *before Riley*. The court, giving officers the benefit of uncertainty in the law after executing a general warrant on a phone, emphasized that, at the time of the search, "neither our precedent nor that of the Supreme Court had developed the robust privacy protections for cell phone users that are applicable today." *Id.* at 302.

Here, the warrants were executed in 2021 and 2023—seven and nine years after *Riley*. The law could not have been clearer. Special Investigator Creech himself acknowledged having written "hundreds" of cell phone search warrants. Tr. at 62:6-9. An officer with that level of experience cannot claim ignorance of the particularity requirement.

Moreover, as the court recognized in *Winn*: "[I]t is manifest that [the magistrate] abandoned his judicial role" by approving facially overbroad warrants. 79 F. Supp. 3d at 923. And

as in *Winn*, "[i]t is simply impossible to conclude that [the magistrate] adequately reviewed the complaint when he signed off on a warrant despite the facially overbroad nature of the list of items to be seized and its utter disconnect from the type of crime at issue and the facts alleged in the complaint." *Id.* at 924. When a magistrate approves a warrant that is nothing more than an unmodified template authorizing seizure of all data, the magistrate has not performed the neutral evaluation that the Fourth Amendment requires.

IV. SOUTH CAROLINA'S CONSTITUTION PROVIDES HEIGHTENED PROTECTION AGAINST UNREASONABLE INVASIONS OF PRIVACY.

Article I, Section 10 of the South Carolina Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures *and unreasonable invasions of privacy* shall not be violated." S.C. Const. art. I, § 10 (emphasis added).

This explicit guarantee against "unreasonable invasions of privacy" goes beyond the Fourth Amendment's text. The South Carolina Supreme Court has recognized that this language "can afford citizens a higher level of privacy protection than the Fourth Amendment." *State v. Forrester*, 343 S.C. 637, 642-43, 541 S.E.2d 837, 840 (2001).

In the context of modern cell phones, South Carolina's constitutional commitment to privacy weighs strongly in favor of requiring particularity in digital warrants—where the United States Supreme Court has made clear that such searches are potentially *more* intrusive than the most thorough search of a home. And if multiple courts in other jurisdictions have invalidated warrants with language identical to those at issue here under the Fourth Amendment alone, then South Carolina courts, armed with an even more protective constitutional provision, should do the same.

The trial court declined to address the implications of Article I, Section 10 in this case. On appeal, this Court should hold that South Carolina's constitution—in addition to the Fourth Amendment—requires suppression of evidence obtained under the general warrants executed here.

CONCLUSION

For the foregoing reasons, the Appellant respectfully requests that this Court reverse the trial court's denial of the Motion to Suppress, vacate the Appellant's convictions, and remand for a new trial at which the fruits of the unconstitutional search warrants are suppressed.

The warrants in this case were general warrants that facially authorized law enforcement to search and seize all data on the Appellant's cell phone without any temporal limitation or content-based restriction. Multiple courts across the country have held that warrants with virtually identical language violate the Fourth Amendment. The trial court erred in upholding these warrants. The factual conclusion that the warrants were sufficiently particular is unsupported by any evidence, and the trial court made a fundamental error of law in relying on *post hoc* justifications never presented to the issuing magistrate. The good faith exception does not apply to facially deficient general warrants, particularly given that the Fourth Amendment's strict applicability to cell phones has been clear since *Riley v. California* in 2014.

The only appropriate remedy for execution of general warrant is to suppress all evidence obtained thereby. The Appellant respectfully requests that this Court apply that remedy here.

Respectfully submitted,

Jack B. Swerling
Curtis J. Copeland
1720 Main Street, Suite 301
Columbia, South Carolina 29201
Telephone: (803) 765-2626
South Carolina Bar No. 5457
Attorneys for Appellant