IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

STATE OF DELAWARE,	)	
	)	
Plaintiff,	)	
	)	**Case No.: 2502008133**
v.	)	**2510007225**
	)	
DAVID DIFILIPPO,	)	
	)	
Defendants.	)	

Submitted: April 13, 2026
Decided: April 24, 2026

OPINION AND ORDER

On Defendant's Motion to Suppress

DENIED

Amanda Buckworth, Esquire, Deputy Attorney General, Attorney General's Office, 820 N. French Street, 7th floor, Wilmington, Delaware, *Attorney for Plaintiff.*

Brian J. Chapman, Esquire, Law Offices of Brian J. Chapman, 300 Creek View Road, Newark, DE 19711, *Attorney for Defendant.*

Jones, J.

INTRODUCTION

David Difilippo ("Defendant") was arrested and charged with numerous child sex offenses, including, but not limited to, dangerous acts against a child, sexual solicitation of a child, sexual abuse of a child by a person in a position of trust, offensive touching, Rape 4th degree, and dealing in child pornography. The Delaware State Police obtained a search warrant (the "Search Warrant") for Defendant's residence which included cellular devices, computers and other electronic devices in the items to be searched. The defense has filed a corresponding Motion to Suppress arguing the Search Warrant constituted either a general warrant or was overbroad. This is the Court's ruling on the matter.

FACTUAL AND PROCEDURAL OVERVIEW

On August 8, 2024, a 14-year-old female victim disclosed to her therapist that one of her middle school teachers, Defendant David Difilippo, engaged in inappropriate behavior and sexually explicit dialogue with her both in person and over the application Discord.[1] The crimes allegedly occurred between September 23, 2023 – February 18, 2024.[2] On February 20, 2025, Defendant was arrested for the first time in connection with child sex offenses.[3] At that time, Defendant was charged with dangerous acts against a child, sexual solicitation of a child, sexual

[1] Affidavit of Probable Cause ("Affidavit"), at 6-7.
[2] Indictment, Case Id # 2502008133.
[3] Def. Mot. to Suppress, at 1-2.

abuse of a child by a person in a position of trust, obscenity, enticement and offensive touching.[4]

A couple days after the original arrest, a second victim came forward on February 25, 2025.[5] Although the victim was 28 at this point, she alleged that the two engaged in a sexual relationship beginning in September 2014 when the victim was just 17 years old.[6] This relationship continued until she turned 18 in November 2014, and beyond.[7] Defendant videotaped at least one encounter on his cellphone and sent the video to the victim via email a few days later.[8] Defendant received sexually explicit images from the victim and took some articles of her clothing as well.[9] This victim told officers she believed Defendant kept these pictures and articles of clothing to memorialize their experiences.[10] She also recounted that Defendant "wrote stories, poems and fantasies" involving her and drew pictures for her, one of which she saved and turned over to the police.[11] When the two re-engaged in a relationship in 2021, Defendant told the victim "his female students were obsessed with him to thew point where they were sending him nude images of themselves via cellular / mobile device."[12]

---

[4] *Id.* at 1.
[5] Affidavit, p. 7, ¶ 9.
[6] *Id.* at 7-8.
[7] *Id.* at 8, ¶ 10.
[8] *Id.* at 8, ¶ 11.
[9] *Id.* at 8, ¶ 12-13.
[10] *Id.*
[11] *Id.* at 8, ¶ 14.
[12] Affidavit, p. 9, ¶ 15.

On April 2, 2025, Detective Marc Conway of the Delaware State Police secured the Search Warrant for the Defendant's residence at 118 Phyllis Drive, Newark, DE 19711.[13] Among other items, the Search Warrant included a search of any cellular device, personal computers or desktops/laptops, other digital information devices, and the data associated with those devices.[14] Specifically, the warrant provided the police may search and seize "*any* cellular device, personal computer, …," "*any* digital or optical data storage device connected to …," and "*any* digital camera, digital video camera, …."[15] As to the data on those items, the Search Warrant provided the police could search "pictures and images," internet activity, electronic messages, and "documents, writings, publications, [or] notes."[16] The timeframe for the search of these items was September 24th, 2014 to the execution of the Search Warrant.[17] The Search Warrant provided in relevant part:

> 1. Enter and search the residence as completely described for evidence of the aforementioned crime(s), to include evidence of Child Pornography and/or Child Sexual Exploitation.
>
> 2. Search David Difilippo (DOB 10/27/1979) for a cellular device and/or digital mobile device, with cellular and/or WiFi capability, in his possession.

[13] Def. Mot. to Suppress, at 2.
[14] *Id.* at 2-3.
[15] *Id.*, Ex. A, Search Warrant, at 1 ("The Search Warrant") (emphasis added).
[16] The Search Warrant, at 2.
[17] *Id.*

3. Search the following locations within the residence and on the property described above, to include but not limited to persons, vehicles, sheds, locked or unlocked safety boxes, bags, compartments, storage areas or things in the nature thereof, found in or upon said residence that could be used to contain evidence of Child Pornography.

4. Search for, and seize, any cellular device, personal computer, computer system, other electronic device or component, to include desktop(s), laptop(s), notebook(s), PDA(s), or tower style systems capable of storing, retrieving, and/or processing electronic digital or optical data and, in particular, any such devices capable of connecting to or communicating with the Internet or Internet Service Providers by any means, including dial-up, broadband or wireless services.

5. Search for, and seize, any digital or optical data storage device connected to, capable of being connected to, read by or capable of being read by, any item described in paragraph 3, to include: internal or external hard drives (found within or without any item seized pursuant to paragraph 3), mass storage devices, pen drives, smart cards, compact disks, compact disk-recordable ® or re-writable (RW), floppy diskettes, DVD+/-R or RW, or any other such device that stores digital data optically, electronically or magnetically.

6. Search for, and seize, any digital camera, digital video camera, optical camera, optical video camera, cellular phone or other device capable of capturing and storing to any media, photographs or images and associated media there from.

7. Search the data, to include the forensic examination thereof, stored by whatever means on any items seized pursuant to paragraphs 3, 4, and 5, as

described above, between the timeframe of **September 24, 2014, to the execution date of this search warrant**, for:

a. Pictures and images;

b. Records of or information about the devices' Internet activity, including firewall logs, connection logs, caches, browser history, cookies, "bookmarked" or "favorite" web pages, search terms, records of user-typed web addresses, temporary internet files, and internet history files;

c. Electronic messages, including: chats and chat logs, instant messages and messaging logs, emails and email contacts, and communications of any nature which appear to involve: (1) contact with any minor, particularly pre-pubescent or adolescent children; or (2) images of children.

d. Documents, writings, publications, notes and/or any other electronic materials relating to correspondence or contact with any individuals purporting to be a minor or portraying or implying sexual activity with a child less than 18-years-of-age, or any such document, writing, publication, note, or any other electronic material portraying children who are nude, semi-nude or in other erotic or semi-erotic conditions.

8. Additionally, search this same data, stored by whatever means on any items seized pursuant to paragraphs 3, 4, and 5, as described above, for:

a. evidence of who used, owned, or controlled the data at the time the things described int his warrant were created, accessed, edited, modified, or deleted, such as log entries, user profiles and/or accounts (including cloud-based accounts), saved usernames

and passwords, autofill values, last backup date and time and backup method(s) used;

b. evidence indicating how and when the devices and/or device applications were assessed or used to determine the chronological context of the device access, use, and events relating to the crime(s) under investigation and to the device user, including evidence of the times the devices were used;

c. device information, including IMSI, IMEI, ICCID, and/or device name;

d. passwords, encryption keys, and/or other access devices that may be necessary to access the seized data found stored within the devices.[18]

On October 22, 2025, Defendant was again arrested in connection to new child sex offenses, including two counts of sexual abuse of a child, two counts of Rape 4th degree, one count of dealing in child pornography, one count of sexual solicitation of a child and one count of violation of privacy.[19] These new charges are alleged to have occurred in October 2021, December 2021, and September 1 – November of 2014.[20]

PARTIES' CONTENTIONS

I. Defendant's Contentions

[18] *Id.* at 1-2.
[19] Def. Mot. to Suppress, at 2.
[20] Re-Indictment, Case Id. # 2502008133 & 2510007225.

Defendant's Motion to Suppress focuses heavily on the search of the digital seizures.[21] While the Defendant concedes the search warrant contained sufficient facts to meet the seizure requirements for the Defendant's Android cell phone from September to November of 2014, the defense raises issues with the search and seizure of the other digital data.[22] The defense argues the search warrant did not meet the particularity standard required to be a valid warrant because the warrant used the "any" language before the description of the digital items and corresponding data that were seized, and because the temporal limitation of ten years was too broad in light of the allegations.[23] Thus, Defendant maintains the Search Warrant is either a general or overbroad warrant and the corresponding evidence obtained as a result of the overreach must be excluded.

II. State's Response

State's response to Defendant's Motion to Suppress contends that there are sufficient facts alleged to support the finding of probable cause to search the electronic devices. The State maintains that probable cause to search the electronic devices is supported by the reports of Defendant's activity by the two victims, the evidence these two victims produced, officers' observation of Defendant using electronic devise to communicate with minors, and the defense conceding

[21] *See generally* Def. Mot. to Suppress.
[22] Def. Mot. to Suppress, at 6, 12.
[23] *Id.* at 12-13.

probable cause as to an Android mobile device.[24] Taken together the State asserts these facts establish an ongoing course of conduct where Defendant's electronic devices were used as instrumentalities of the alleged crimes.[25] Thus, the State argues that under a common-sense reading of the facts, probable cause cannot be limited to a single device or narrow time frame.[26] The State further claims that the Search Warrant is not general because warrant authorizes a targeted search for evidence of specific criminal conduct.[27] Similarly, it is not overbroad because the manner in which data is stored requires search warrants seeking digital data be drafted with sufficient breadth to capture the data corresponding to the criminal activity.[28]

STANDARD OF REVIEW

"On a motion to suppress contesting the validity of a search warrant, the defendant shoulders the burden of establishing that the challenged search or seizure was unlawful."[29] "The defendant must prove by a preponderance of the evidence that the search and/or seizure violated their rights under the United States

[24] State's Response, at 7-8.
[25] *Id.* at 9-10.
[26] *Id.* at 10.
[27] *Id.* at 12.
[28] *Id.* at 14.
[29] *State v. Spencer*, at *3 (Del. Super. Ct. Apr. 24, 2023), as corrected (Apr. 24, 2023) (citing *State v. Sisson*, 883 A.2d 868, 875 (Del. Super. Ct. 2005), *aff'd*, 903 A.2d 288 (Del. 2006)); *see also State v. Taylor*, 341 A.3d 568, 574 (Del. Super. Ct. 2025) ("On a motion to suppress the proceeds of a search warrant, the movant has the burden of proving, by a preponderance of the evidence, that the warrant was issued unlawfully.") (footnotes omitted).

Constitution, the Delaware Constitution, or Delaware Statutes."[30] "Both constitutions require that a warrant be supported by probable cause and describe the places and things to be searched *with particularity*."[31]

"Great deference" should be given to a magistrate's finding of probable cause,[32] and it should not be invalidated "on the basis of a 'hypertechnical, rather than common sense, interpretation of the warrant affidavit.'"[33] As such, probable cause determinations for warrants and affidavits should be reviewed in their entirety rather than on specific allegations.[34] "It is well settled that any finding of probable cause must be based on the information that appears within the four corners of the application or affidavit."[35] Under this test, "the supporting affidavit must set forth sufficient facts on its face 'for a judicial officer to form a reasonable

[30] *State v. Reese*, 2019 WL 1277390, at *3 (Del. Super. Ct. Mar. 18, 2019) (citing *State v. Westcott*, 2017 WL 283390, at *1 (Del. Super. Ct. 2017)); *see also State v. Oseguera-Avila*, 197 A.3d 1050, 1055 (Del. Super. Ct. 2018) (citing *State v. McElderry*, 2018 WL 4771786, at *2 (Del. Super. Ct. Oct. 1, 2018)).
[31] *Terreros v. State*, 312 A.3d 651, 661 (Del. 2024) (citing *Fink v. State*, 817 A.2d 781, 786 (Del. 2003) (emphasis in original).
[32] *State v. Taylor*, 341 A.3d 568, 574 (Del. Super. Ct. 2025) (citing *State v. Holden*, 60 A.3d 1110, 1114 (Del. 2013)); *see also State v. Chaffier*, 2023 WL 1872284, at *3 (Del. Super. Ct. Jan. 17, 2023), *aff'd*, 328 A.3d 329 (Del. 2024) (citing *Cooper v. State*, 228 A.3d 399, 404 (Del. 2020)).
[33] *State v. Taylor*, 341 A.3d at 574 (quoting *Cooper v. State*, 228 A.3d 399, 404 (Del. 2020)); *see also Spencer*, 2023 WL 3052370, at *4.
[34] *Smith v. State*, 887 A.2d 470, 473 (Del. 2005) (citing *Blount v. State*, 511 A.2d 1030, 1034 (Del. 1986)); *Dorsey v. State*, 761 A.2d 807, 811 (Del. 2000); *see also State v. Anderson*, 2018 WL 6177176, at *2 (Del. Super. Ct. Nov. 5, 2018), *aff'd*, 249 A.3d 785 (Del. 2021) ("The Court must also consider the information in the affidavit under a totality of the circumstances.").
[35] *Willis v. State*, 302 A.3d 417, 427 (Del. 2023) (quoting *Valentine v. State*, 207 A.3d 566, 570 (Del. 2019)) (internal quotations omitted); *see also Sisson*, 883 A.2d 868, 876 (Del. Super. Ct. 2005), *aff'd*, 903 A.2d 288 (Del. 2006) (citing *Pierson v. State*, 338 A.2d 571, 573 (Del. 1975)).

belief that an offense has been committed and that seizable property would be found in a particular place to support a finding of probable cause.'"[36]

With that comes the second warrant requirement: particularity.[37] "In addition to being supported by probable cause, a search warrant must 'be as particular as possible.'"[38] To satisfy this requirement, "[t]he warrant must describe the things to be searched with sufficient particularity and be no broader than the probable cause on which it is based."[39] Due to the sheer amount of private information contained within digital devices, "[w]arrants directed to digital information present unique challenges in satisfying the particularity requirement."[40] In addition to the types of files and information you would typically find in the home, cellphones "also contain[] a broad array of private information never found in a home in any form."[41] The Delaware Supreme Court has warned the judiciary "that the risk that warrants for digital and electronic devices take on the character of 'general warrants' is substantial" and "necessitates heightened vigilance."[42] Thus, when dealing with electronic warrants, "in order

[36] *Sisson*, 883 A.2d at 876 (quoting *State v. Manley*, 706 A.2d 535, 540 (Del. Super. Ct. 1996); *see also Spencer*, 2023 WL 3052370, at *4.
[37] *Wheeler v. State*, 135 A.3d 282, 298-99 (Del. 2016).
[38] *Spencer*, 2023 WL 3052370, at *4 (quoting *Taylor v. State*, 260 A.3d 602, 613 (Del. 2021)); *see also Buckham v. State*, 185 A.3d 1, 16 (Del. 2018) (quoting 11 *Del. C.* § 2306).
[39] *Wheeler*, 135 A.3d at 298-99 (citing *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)).
[40] *Id.* at 299 (citing *Riley v. California*, 573 U.S. 373, 403 (2014); *see also Taylor v. State*, 260 A.3d 602, 613-14 (Del. 2021).
[41] *Id.* (citing *Riley v. California*, 573 U.S. 373, 396-97 (2014)); *see also Taylor v. State*, 260 A.3d 602, 613-14 (Del. 2021).
[42] *Wheeler*, 135 A.3d at 307.

to satisfy the particularity requirement, [the warrant] must describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances."[43]

When a warrant does not meet the particularity requirement, it is categorized as either a general warrant or an overbroad warrant.[44] A general warrant is one "that allows law enforcement to conduct an indiscriminate search."[45] Similarly, "[a]n overbroad warrant explicitly allows investigators to search places and things when no probable cause exists to search them."[46] The difference between the two is that a general warrant is one that "allows investigators to conduct an 'exploratory rummaging," while an overbroad warrant "allows police to search in specified places or for specified items more broadly than the articulated probable cause."[47] Each also carries its own distinct remedy: "[a]ll fruits of a general warrant must be suppressed in their entirety, whereas an overbroad warrant … can be redacted as to the portions of the search for which no probable cause exists."[48]

The Delaware Supreme Court has had the opportunity over the last few years to address warrants involving digital data.[49] The Court's most recent

---

[43] *Id.* at 304.
[44] *Terreros v. State*, 312 A.3d 651, 662-63 (Del. 2024)
[45] *Id*. (citing *Wheeler v. State*, 135 A.3d 282, 292 (Del. 2016)); *see also Thomas v. State*, 305 A.3d 683, 701 (Del. 2023) (citing *United States v. Yusuf*, 461 F.3d 374, 393, n. 19 (3d Cir. 2006)).
[46] *Terreros*, 312 A.3d at 663.
[47] *Id.*
[48] *Id.*
[49] *Terreros v. State*, 312 A.3d 651 (Del. 2024); *Taylor v. State*, 260 A.3d 602 (Del. 2021); *Buckham v. State*, 185 A.3d 1 (Del. 2018); *Wheeler v. State*, 135 A.3d 282 (Del. 2016).

decision is in *Terreros v. State*. In *Terreros*, the Court found a warrant for the search of a cell phone's data to be a general warrant.[50] In reaching this conclusion, the Court held that even where there is limiting language, when the search essentially allows law enforcement to look at the entire phone, the warrant can still be a general warrant.[51] There, the warrant at issue did not contain the "any and all data" language that had been found to be an issue in previous general warrants.[52] However, because the warrant was still broad and general enough to grant "police the authority to conduct an indiscriminate search through Terreros's cell phone," the Court ruled the *Terreros* warrant was a general warrant.[53] Like *Wheeler v. State*, *Buckham v. State*, and *Taylor v. State*, the *Terreros* warrant also lacked a temporal limitation.[54]

ANALYSIS

First, a determination must be made as to probable cause. As noted above, Defendant has already conceded that there is probable cause for a search of his cell phone from September to November of 2014.[55] Thus, the Court must determine whether there was probable cause to search the cell phone beyond that time frame,

[50] *Terreros*, 312 A.3d at 666.
[51] *Id.* at 667 ("Although the warrant for Terreros's phone did not go so far as to authorize a search of 'any and all data,' that was, in effect, what the warrant permitted law enforcement to extract and search. In other words, this warrant gave police the authority to conduct an indiscriminate search through Terreros's cell phone.")
[52] *Id.*; *see also Buckham v. State*, 185 A.3d 1 (Del. 2018); *see also Wheeler v. State*, 135 A.3d 282 (Del. 2016).
[53] *Terreros*, 312 A.3d at 667.
[54] *Id.* at 668.
[55] Def. Mot. to Suppress, at 6.

and whether there was sufficient probable cause for the search of the other digital items and their corresponding data for the 10 year period.

I. Probable Cause as to Electronic Devices and Their Data

Taking the affidavit in its totality, there is probable cause to search for child pornography on Defendant's digital devices and corresponding data. The affidavit includes accusations from two women about improper relationships / communications with minors. The accusations are specific as to Defendant's actions in the alleged incidents and dates when they occurred. Both victims also recounted a similar method Defendant employed to groom the students, such as allowing them to skip class and hide in his classroom.[56] Further still, the victims provided investigators with both electronic photo evidence of the alleged wrongdoings, including sexually explicit photos and messages that were sent over the Discord application,[57] and physical evidence in the form of a drawing Defendant made for one of the victims.[58]

The communications between Defendant and the two victims occurred via text messages, email, Discord, and Facebook. During a conversation with one of the victims, Defendant reportedly received a picture from the victim and responded, "I just saw that pic," "saved."[59] Additionally, one victim recounted

[56] Affidavit of Probable Cause, p.6, ¶ 5, p. 8, ¶ 10.
[57] *Id.* at 6, ¶ 3, 4, p. 7, ¶ 6, 7, 8.
[58] *Id.* at 8, ¶ 14.
[59] *Id.* at 7, ¶ 7.

that Defendant recorded a sexual encounter between the two of them and emailed her the recording a few days later.[60] These two experiences indicate Defendant was storing the photos he took / received of the victims. The affiant also explained that based on their own training, experience, and knowledge, and the training, experience, and knowledge of other officers, when an individual possesses these types of images on one device, they typically store similar images on other devices.[61] Finally, one of the victims also expressed her belief that Defendant still possessed these explicit images / videos of her to memorialize the experiences.[62]

Based on the totality of the allegations contained in the affidavit, and giving great deference to the magistrate's determination, the Court finds there was probable cause to search the Defendant's cell phone, other electronic devices, and the corresponding data. The information provided in the affidavit would lead a judicial officer to a reasonable belief that evidence of the accused crimes would be found on these devices. Additionally, the most natural reading of the affidavit is that Defendant's electronic devices were used as instrumentalities of the offenses and contain material of evidentiary value. Any deficiencies in this warrant / affidavit arise not from the lack of probable cause, but from a lack of specificity.

[60] *Id.* at 8, ¶ 12.
[61] *Id.* at 10-11, ¶ 21-25.
[62] *Id.* at 8, ¶ 14.

II. The Particularity Requirement

The Particularity requirement is both a constitutional and statutory requirement in Delaware.[63] Delaware caselaw has shown that "in order to satisfy the particularity requirement, [warrants] must describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances."[64] Common deficiencies in warrants for electronic items are the lack of a temporal limitation,[65] not specifying the categories of data to be searched,[66] or including all-inclusive language in the warrant.[67]

i. Temporal Limitation

In *Wheeler v. State*, the Delaware Supreme Court dealt with an issue of first impression: "a challenge to warrants seeking to seize and search computer-based and digital items on the grounds that they are in the nature of a general warrant, unconstitutionally overbroad, and lack sufficient particularity."[68] There, a magistrate issued a warrant to search the defendant's electronics for evidence of witness tampering. Importantly, the *Wheeler* warrant had no temporal limitation. To begin the analysis, the Court examined the rulings of other jurisdiction on this

[63] DE CONST, Art. 1, § 6 ("no warrant to search any place, or to seize any person or thing, shall issue without describing them as particularly as may be."); *see also* 11 *Del. C.* § 2307 ("The warrant shall designate the house, place, conveyance or person to be searched, and shall describe the things or persons sought as particularly as possible.").
[64] *Wheeler*, 135 A.3d at 304.
[65] *Terreros*, 312 A.3d 651; *Taylor v. State*, 260 A.3d 602; *Buckham*, 185 A.3d 1; *Wheeler*, 135 A.3d 282.
[66] *Terreros*, 312 A.3d 651; *Taylor v. State*, 260 A.3d 602; *Buckham*, 185 A.3d 1; *Wheeler*, 135 A.3d 282.
[67] *Thomas*, 305 A.3d at 702; *Buckham*, 185 A.3d 1; *Wheeler*, 135 A.3d 282.
[68] *Wheeler*, 135 A.3d at 302.

issue and made several important takeaways to guide their analysis. One takeaway, which came from reviewing a Sixth circuit Court of appeals decision, was that "the proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation."[69] Additionally, in reviewing a case from the Supreme Court of Ohio, the Court recognized that "officers must describe what they believe will be found on a [device] with as much specificity as possible under the circumstances."[70]

The *Wheeler* court initially "hesitate[d] to prescribe rigid rules and instead reiterate[d] that warrants must designate the things to be searched and seized as particularly as possible."[71] With this in mind, the court zeroed in on this temporal limitation issue and "the failure to limit the search to the relevant time frame."[72] Specifically, "[t]he Affidavits contain[ed] no facts suggesting that any tampering might have occurred prior to July 2013. Yet, the Witness Tampering Warrants were boundless as to time."[73] Furthermore, it had been determined that one iMac belonging to the defendant was searched despite the Sergeant's determination that the computer had not been powered on since September of 2012.[74] The court

[69] *Id.* (citing *United States v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982)).
[70] *Id.* at 304 (quoting *State v. Castagnola*, 46 N.E.3d 638, 659 (Ohio 2015)) (internal quotations omitted).
[71] *Wheeler*, 135 A.3d at 305.
[72] *Id.* at 304.
[73] *Id.* at 305.
[74] *Id.*

seemed particularly troubled that "the State unsystematically sifted through Wheeler's digital universe, even though the iMac logically could not have contained material created or recorded during the relevant time period."[75] As a result, the court in *Wheeler* held "[b]ecause the State was able to more precisely describe the items to be searched and seized, the Witness Tampering Warrants violated the particularity requirement" and constituted a general warrant.[76]

This decision aligns with further Delaware cases on this topic. In *Thomas v. State*, the Delaware Supreme Court highlighted the following trend:

> We invalidated the warrants in *Wheeler*, *Buckham*, and *Taylor* because investigators had a more precise description of the places to be searched than was provided in the warrant, and there was nothing in those cases to support an inference that evidence would have been found in the less precise locations which the warrants authorized law enforcement to search. Therefore, the warrants in those cases authorized unconstitutional exploratory rummaging.[77]

Yet just because a warrant contains a temporal limitation for a search of digital items does not mean it is specific enough. In *Thomas*, the police secured a warrant against the defendant for stalking and other related charges.[78] The *Thomas* warrant sought to search the defendant's iPhone for call and text message logs, social media data, and other communication data for February 22, 2019 - January 18,

[75] *Id.*
[76] *Id.* at 305-06.
[77] *Thomas*, 305 A.3d at 702.
[78] *Id.* at 686-87.

2020.[79] The warrant also allowed for a search of the photos and videos on the iPhone which did not have a temporal limitation.[80]

The *Thomas* court ultimately found that the warrant was overbroad because it could have been more specific in the communications it sought to search:

> [T]he trial court did not err in finding that the Search Warrant was overbroad, and not general. Because the Search Warrant was overbroad, the proper remedy was for the trial court to limit the Search Warrant only to that which was supported by probable cause. Here, the trial court limited the time frame considerably — to January 1, 2020, through January 18, 2020 — and limited the calls and messages to those involving the victims. The affidavit prepared by Detective Herrera-Cortes articulated facts supporting probable cause that information regarding the crime of Stalking would be found in such data. After a de novo review of the record here, we are satisfied that the trial court acted properly and with such heightened vigilance and with this Court's guidance in mind. We AFFIRM.[81]

Perhaps the most important takeaway from *Thomas* is the court's determination that "the lack of a temporal limitation on photos and videos does not invalidate the Search Warrant."[82]

Turning to the case at hand, the Court is satisfied that the Warrant meets the specificity requirements as to the temporal limitations. The Search Warrant here

---

[79] *Id.* at 689.
[80] *Id.*
[81] *Id.* at 703.
[82] *Thomas*, 305 A.3d at 703. This dealt solely with pictures and videos on an iPhone. No time restriction was implemented because the photos could have been taken at any time. *Id.* at 703, n. 40.

differs from previous insufficient warrants in a couple ways. First, unlike *Wheeler*, *Buckham*, *Taylor* and *Terreros*, this warrant contained a temporal limitation. Second, as opposed to *Wheeler* and *Thomas* where the warrants dealt with charges of witness tampering and stalking, respectively, the Search Warrant in this case dealt with child sex crimes, including rape, sexual exploitation of a child, and possession and distribution of child pornography.

And third, there is evidence to suggest that wrongdoing occurred during the entirety of the sought-after time period. Defendant made an explicit video with the first minor victim in 2014 and later sent her that video via email. This means that he possessed, stored and circulated the video starting in 2014. The present circumstances are different from *Wheeler* where it was impossible that one searched iMac could have contained evidence of the witness tampering charges. Here, a search warrant for the entire ten years would be necessary to see if Defendant circulated the explicit video or photos to any other parties, if he transferred any of this explicit material from one device to another and if he possessed anymore material in a different digital location.

Furthermore, when Defendant and the first victim re-engaged in a relationship in 2021, Defendant told the victim that his female students were obsessed with him and were sending nude images of themselves to his cellphone.[83]

[83] Affidavit of Probable Cause, p. 9, ¶ 15.

This, coupled with the Defendant's actions against the second victim in 2023-2024, demonstrates Defendant was likely engaged in child sex crimes during the entire span of the Search Warrant. Essentially, the affidavit alleges Defendant had an inappropriate relationship with a child in 2014, admitted to continuing inappropriate conversations with children in 2021, and was then reported by a second victim in 2024. These facts indicate evidence of these crimes could be found from September of 2014 to the execution of the Search Warrant.

As highlighted in *Wheeler*, the time span need only be as specific as possible in light of the circumstances.[84] Given Defendant's own admission to continuing crimes from 2014-2021 without providing further information, the Court is satisfied that the State was as specific as it could be given the information it had and, therefore, met the particularity requirements as to the temporal limitation. While the Court is not going so far as to say that no temporal limitation is required here for the search of photos and videos, the Delaware Supreme Court's language in *Thomas* plays a role in this decision as well. Accordingly, the Motion to Suppress is **DENIED** as to any temporal limitation violation.

[84] *Wheeler*, 135 A.3d at 305 (citing *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980)) ("the search and seizure should be appropriately narrowed to the relevant time period so as to mitigate the potential for unconstitutional exploratory rummaging.").

ii. All Inclusive Language & Specific Categories of Data

Another area where warrants fail to meet the particularity requirement when dealing with digital assets is the categories of data to be searched.[85] Specifically, the use of all-encompassing language, such as "any and all data," indicates a warrant may not be specific enough to meet the particularity standard.[86]

In *Taylor v. State*, the warrant at issue "authorized a search of 'any and all data' on the smartphones."[87] In case there was any doubt, the Delaware Supreme Court first clarified "the fact that the investigator identified the smartphones as the object of the search and the data on the smartphones as the things to be searched does not satisfy the particularity requirement."[88] The Court then went on to state unequivocally "a warrant that allows investigators to search for 'any and all data' 'pertinent to the criminal investigation' is unlimited in scope," and held the warrant was a general warrant.[89] Similarly, when a warrant that sought GPS location data from the Defendant's phone "authorized [the police] to search '[a]ny and all store[d] data contained within the internal memory' of the phone for

[85] *See e.g*. *Taylor v. State*, 260 A.3d at 616-17; *Buckham*, 185 A.3d at 19; *see also Terreros*, 312 A.3d at 667-68 (Del. 2024).
[86] *Taylor v. State*, 260 A.3d at 616 ("a warrant that allows investigators to search for 'any and all data' 'pertinent to the criminal investigation' is unlimited in scope.").
[87] *Id.*
[88] *Id.*
[89] *Id.* at 616-17.

evidence of the shooting," the Court in *Buckham v. State* found the warrant to be a general warrant.[90]

Even where the warrant identifies specific categories of data to be searched, the all-encompassing language can still render a warrant general. In *Terreros*, the police wanted to search the Defendant's phone to view his internet search history. Accordingly, the police obtained a warrant to search "'[a]ny and all messages, any and all messaging apps, all search history, all photographs, videos, GPS coordinates, incoming and outgoing calls used or intended to be used for Rape 2nd by person of Authority.'"[91] The warrant also lacked a temporal limit.[92] Ultimately, the warrant was held to be a general warrant.[93] The court reasoned "even though the warrant identified specific categories of data, rather than referring to 'any and all data,' each category was preceded by 'any and all' language with no temporal limitation."[94] The court further explained "there was no probable cause to believe that any type of data on Terreros's phone would yield seizable evidence other than his internet search history" and, thus, "the warrant authorized the very type of unbounded fishing expedition that the particularity requirement is intended to prevent."[95] However, in *State v. Riley* this court

[90] *Buckham*, 185 A.3d 1, 18-19.
[91] *Terreros*, 312 A.3d at 655.
[92] *Id.*
[93] *Id.* at 666.
[94] *Id.* at 668.
[95] *Id.*

previously found that "the *verboten* language 'any', 'all', and 'any and all,'" used to modify specific categories of data to be searched did "not render the warrant 'general' or 'overbroad'" when there was a temporal limitation and the warrant was backed by probable cause.[96]

Conversely, *Thomas* illustrates an instance where the warrant did not include this all-encompassing or open-ended language. The *Thomas* court specifically noted "[t]he Search Warrant here does not authorize law enforcement to search 'any and all data on the smartphone,' or certain data 'including but not limited to.'"[97] Instead, the warrant named the specific categories of data to be searched and provided a temporal limitation.[98] In the end, the *Thomas* court viewed the temporal limitation to be too long and held the warrant to be overbroad, not general.[99]

When dealing with warrants for electronic data, it is the nature of the beast that extensive records will be examined.[100] Many courts have highlighted the danger posed in relation to the search of electronic assets because of the vast amount of information they can hold.[101] However, the *Wheeler* court also

[96] *State v. Riley*, 2024 WL 2375164, at *8 (Del. Super. Ct. May 22, 2024) (emphasis in original).
[97] *Thomas*, 305 A.3d at 702.
[98] *Id.* at 702-03.
[99] *Id.* at 703.
[100] *See Taylor v. State*, 260 A.3d at 613-14; *see also Wheeler*, 135 A.3d at 299 ("Warrants directed to digital information present unique challenges in satisfying the particularity requirement, given the unprecedented volume of private information stored on devices containing such data.").
[101] *Riley v. California*, 573 U.S. 373 (2014); *United States v. Perez*, 712 F. App'x 136, 139 (3d Cir. 2017); *United States v. Purcell*, 967 F.3d 159, 183 (2d Cir. 2020); *Wheeler v. State*, 135 A.3d 282, 299-300 (Del. 2016); *State v.*

recognized "[s]ome irrelevant files may have to be at least cursorily perused to determine whether they are within the authorized search ambit. Accordingly, the proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation."[102] The court also reminded us "[w]arrants 'must be tested by courts in a commonsense and realistic fashion,' and reviewing courts should avoid a 'hypertechnical approach.'"[103]

Applying these principles to Mr. Difilippo's present case, the Court believes the State has met its particularity requirements. To begin, the Search Warrant lays out exactly what categories of data are to be searched: 1) "pictures and images;" 2) records of internet activity; 3) electronic messages that "appear to involve" minors or "images of children;" 4) notes, publications or "other electronic materials relating to correspondence or contact with any individuals purporting to be a minor or portraying … sexual activity with a child less than 18-years-of-age;" and 5) the corresponding data to determine when these aforementioned categories of data were accessed, by who, and who had control over them. While this may

McDonnell, 297 A.3d 1114, 1130-31 (Md. 2023); *see also Commonwealth v. Green*, 265 A.3d 541, 553-54 (Pa. 2021).

[102] *Wheeler*, 135 A.3d at 301 (citing *Christine*, 687 F.2d at 760). The Court also noted "'[N]o tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision.'" *Id.* (quoting *Christine*, 687 F.2d at 760).

[103] *Id.* at 300 (quoting *Christine*, 687 F.2d at 760).

sound expansive upon a first glance, there is probable cause for all of this information.

As to the first category, Defendant has been producing, collecting and storing explicit images and videos of minor children since at least September 2014. Defendant admitted in 2021 he was still receiving explicit images of children, and in 2024 he told a child that he "saved" an image they had sent of themselves. To the second category, we know Defendant has been communicating with minors over the internet and sharing / receiving these explicit materials through internet connection. To the third, the messages to be searched and seized are limited to those involving children as opposed to all messages during the time of the warrant. The fourth category is also limited to writings or other materials involving minors, which is pertinent given that Defendant "wrote stories, poems and fantasies" for and about the first victim.[104] Finally, the fifth category of data would be necessary to ensure that Defendant was actually the one using these materials.

Thus, the Court is satisfied the State limited the warrant to the relevant categories of data with enough specificity as the circumstances allowed at that juncture of the investigation. The warrant does not fail for a lack of specificity as to language or the categories of data to be searched, and the Motion to Suppress is **DENIED** as to that issue.

[104] Affidavit of Probable Cause, p. 8, ¶14.

Even if the Warrant did have any deficiencies, this Court is of the view that the Warrant would be overbroad, not general, because the Warrant was backed by probable cause and contained a temporal limitation.[105]

CONCLUSION

For the aforementioned reasons, the Motion to Suppress is **DENIED**.

IT IS SO ORDERED.

/s/ Francis J. Jones, Jr.
Francis J. Jones, Jr., Judge

cc: Original to Prothonotary

[105] *See Thomas v. State*, 305 A.3d 683 (Del. 2023).