OFFICE OF THE PROSECUTOR

County of Atlantic

WILLIAM E. REYNOLDS

Atlantic County Prosecutor

4997 Unami Boulevard, Suite 2
P.O. Box 2002
Mays Landing, NJ 08330
609-909-7800 – Fax 609-909-7802

ERIK M. BERGMAN
First Assistant Prosecutor

RICHARD E. McKELVEY
Executive Assistant Prosecutor

JOHN H. FLAMMER
Chief Counsel to the Prosecutor

PATRICK F. SNYDER
Chief of County Detectives

PATRICIA A. HAYEK
Director of Victim Witness

SHAVONNE C. DAVIS
Director of Community Outreach

December 13, 2024

Christopher Santo D'Esposito
Assistant Prosecutor
Of Counsel and on the Letter Brief

Kathleen Robinson
Chief Assistant Prosecutor
Of Counsel and on the Letter Brief

Joseph Remy
Assistant Prosecutor
On the Letter Brief

Bernard E. DeLury, Jr., P.J.Cr. (via eCourts)
Atlantic County Criminal Courts Complex
4997 Unami Boulevard, 2nd Floor
Mays Landing, New Jersey 08330

Re: State of New Jersey v. Constance Days-Chapman
Indictment No. 24-09-02900-T; Case No. 24-1306
Motion to Suppress Evidence Obtained by Search Warrant
Returnable: January 9, 2025

Dear Judge DeLury:

Please accept this letter memorandum in lieu of a more formal brief in response to defendant Constance Days-Chapman's Motion to Suppress Digital Evidence Obtained Pursuant to Search Warrants.

In January 2024, the Division of Child Protection and Permanency ("DCPP") and the Atlantic County Prosecutor's Office ("ACPO") received a referral concerning child abuse allegations made by then [redacted], [redacted] Marty Small, the Mayor of Atlantic City, and his wife, La'Quetta Small, the Superintendent of Atlantic City Schools. [redacted] disclosed that [redacted] (that is, the Smalls) had physically abused her several times in the [redacted]. The abuse reportedly occurred between December 2023 and January 2024. At that time, [redacted] was enrolled as a student at the Atlantic City High School, where the defendant was employed as the school's principal under Mrs. Small.

Following an investigation, detectives determined that on January 22, 2024, the defendant became aware of [redacted]'s disclosure that she had been physically abused by [redacted], but the defendant never reported that disclosure, as required by law or school policy, to either DCPP or law enforcement. Instead, the defendant met with the Smalls and warned them that [redacted] had disclosed being physically abused by them.

While investigating the defendant's failure to report [redacted]'s January 2024 disclosures of child abuse, detectives discovered that the defendant had previously failed to report similar disclosures. More specifically, detectives learned that in December 2023, [redacted] told the defendant that [redacted] physically abused her, but that disclosure was likewise never reported by the defendant to DCPP or law enforcement.

On September 11, 2024, an Atlantic County Grand Jury returned Indictment Number 24-09-02900-T, charging the defendant with second- and third-degree crimes committed between December 2023 and January 2024, to wit: two counts of second-degree official misconduct for failing to report child abuse to the New Jersey State Central Registry, in violation of N.J.S.A. 2C:30-2b (Counts One and Four); two counts of second-degree official misconduct for failing to report child abuse to law enforcement authorities, in violation of N.J.S.A. 2C:30-2b (Counts Two and Five); second-degree endangering the welfare of a child, in violation of N.J.S.A. 2C:24-4a(2) (Count Three); second-degree official misconduct for notifying the Smalls about [redacted] disclosures of abuse despite the fact that the Smalls were alleged by [redacted] to be responsible for committing such abuse, in violation of N.J.S.A. 2C:30-2a (Count Six); third-degree hindering the prosecution of another, in violation of N.J.S.A. 2c:29-3a(3) (Count Seven); and second-degree engaging in a pattern of official misconduct for failing to report [redacted] disclosures, in violation of N.J.S.A. 2C:30-7 (Count Eight).

On November 18, 2024, the defendant, through her counsel, filed a Motion to Suppress Digital Evidence obtained pursuant to Search Warrants which were granted by Your Honor on March 20, 2024. The Search Warrants pertained to three digital devices which belonged to the defendant. True copies of the judicially approved Search Warrants, and the Certification submitted in support thereof, are attached as **Exhibit A**.

STATEMENT OF FACTS

The State opposes the defendant's Motion to Suppress the Digital Evidence obtained by the Search Warrants. In lieu of unnecessary repetition, the State incorporates herein the entirety of Detective Choe's Certification and provides this summary to assist the Court:

Pursuant to law and the Atlantic City Board of Education's District Policy #8462, Atlantic City school officials have a duty to immediately report allegations of child abuse to law enforcement, as well as to DCPP through a phone hotline. Cert. at ¶¶3(w)-(x). Moreover, Atlantic City High School had a policy that any staff who reported an allegation of abuse to DCPP must thereafter complete and email a proscribed form to the Atlantic City Superintendent's Office. Cert. at ¶¶3(aa)(6).

On January 22, 2024, then [redacted], a female student at the Atlantic City High School, attended a school assembly concerning mental health. Cert. at ¶¶3(aa)(1)-(2). At the conclusion of the assembly, [redacted] completed a written "exit ticket." Ibid. On the "exit ticket," [redacted] wrote that she had experienced "abuse," and she asked to speak to a counselor. Ibid. That same day, a counselor at the high school spoke to [redacted] in the hallway. Cert. at ¶¶3(aa)(3). [redacted] disclosed that she had been physically abused and hit with a broom. Ibid. [redacted] also stated that [redacted] is a big guy," and that "she already spoke with Principal Chapman [the defendant] about some choices." Ibid.

After speaking to [redacted], the counselor learned that [redacted] was [redacted] of the Smalls. Cert. at ¶¶3(ee). The counselor also discussed

[redacted]'s disclosure with a senior member of the high school's staff. Cert. at ¶¶3(dd) - (ee). Together, the counselor and the senior staff member met with the defendant in the latter's school office (the "First Meeting"). Cert. at ¶¶3(ff). During the First Meeting, the counselor advised the defendant of [redacted]'s disclosures that she had been physically abused and hit with a broom. Cert. at ¶¶3(aa)(4). The defendant stated that "[redacted] never mentioned the abuse to her," and that she (i.e., the defendant) would report[redacted]'s disclosure to DCPP, as required. Ibid.

Cellphone records obtained by court order revealed an outgoing call made from the defendant's cellphone to Mrs. Small's cellphone on the day of the First Meeting. Cert. at ¶¶3(tt)(b). The defendant placed this call on January 22, 2024 at 4:07 p.m. Ibid. Additionally, video surveillance shows that the defendant drove her BMW to the Smalls' home in Atlantic City at approximately 5:33 p.m. on January 22, 2024. Cert. at ¶¶3(qq)(i) - (vii). Thereafter, Mrs. Small exited her home and entered the defendant's BMW. Ibid. At approximately 5:41 p.m., Mr. Small arrived home and then entered the BMW. Ibid. At approximately 5:58 p.m., Mr. Small exited the BMW. Ibid. At approximately 6:12 p.m., Mrs. Small exited the BMW and entered the family home as the BMW departed. Ibid.

The next day, during school hours on January 23, 2024, the counselor and the senior staff member again met with the defendant in her office at the high school (the "Second Meeting"). Cert. at ¶¶3(kk). During the Second Meeting, the defendant stated she had went to the Smalls' residence and had notified the Smalls that [redacted] disclosed having

been physically abused by them. Ibid. Just as occurred in the First Meeting, the defendant promised the counselor and the senior staff member that she (i.e., the defendant) would contact DCPP to report [redacted]'s disclosure. Cert. at ¶¶3(ii). The counselor recalled that the defendant "made it seem as if she was going to make the call to DCP&P right then and there as they were leaving her office." Ibid.

That same day, at approximately 3:30 p.m. on January 23rd, [redacted] employed by [redacted] received a referral to speak to [redacted] Cert. at ¶¶3(l). According to the [redacted], the Smalls contacted the [redacted] to arrange a [redacted] for [redacted] Cert. at ¶¶3(aa)(l) – (m). Intake documents from [redacted] showed that Mrs. Small provided [redacted] with a personal email address and a phone number. Cert. at ¶¶3(r). Later in the investigation, the same phone number and email address were found in [redacted] pertaining to a visit by [redacted] to the [redacted] on January 16, 2024. Ibid.

According to [redacted], [redacted] disclosed during the January 23rd [redacted] that she was being physically abused by [redacted] and [redacted]. Cert. at ¶¶3(o) – (p). The abuse occurred inside the family home between December 2023 and January 2024. Cert. at ¶¶3(t).

On January 24, 2024, [redacted] supervisor contacted DCPP to report [redacted]'s disclosure the day prior. Cert. at ¶¶3(r). That same day, DCPP went to the Smalls' [redacted] home. Cert. at ¶¶3(cc)(2). According to DCPP, "La'Quetta Small said she knew DCP&P would be

reporting to her residence to speak with [redacted] because her 'good friend' had told her about DCP&P involvement." Cert. at ¶¶3(f) – (g). However, Mrs. Small did not disclose the identity of her "good friend." Ibid.

Subsequent to the DCPP referral received on January 24, 2024, ACPO initiated an investigation concerning [redacted]'s disclosures of child abuse and whether the defendant committed Official Misconduct by failing to report those disclosures to the authorities, and by notifying the Smalls that [redacted] disclosed having been physically abused by them. That investigation is summarized in the Certification. In relevant part, detectives conducted interviews, including interviews of [redacted], DCPP staff, [redacted], the counselor, and the senior staff member.

On January 31, 2024, ACPO detectives spoke to [redacted] at the high school. Cert. at ¶¶3(s). [redacted] "disclosed being physically abused by [redacted] and [redacted] on multiple occasions during the months of December 2023 to January 2024, while inside their residence." Cert. at ¶¶3(t). [redacted] also advised the detectives that she had already disclosed the physical abuse to a counselor at her school, and [redacted] added that she "believed [the counselor] told [the defendant] because not longer after [the defendant] asked her 'how she was doing.'" Cert. at ¶¶3(u) – (v).

On the same day that ACPO detectives interviewed [redacted] at the high school (i.e., January 31st), the defendant communicated with Mr. Small approximately 23 times according to her cellphone records. Cert. at ¶¶3(tt)(c). Additionally, investigators obtained surveillance footage from the high school at approximately 11:07 a.m. on January 31st. Cert.

at ¶¶3(rr)(i) - (ss). The footage showed a dark SUV drive over the curb and onto a concrete walkway before parking near the high school's front doors. Ibid. Seconds later, Mr. Small is seen talking on a cellphone while walking toward the main entrance of the high school. Ibid.

On March 15, 2024 the defendant's cellphone records were received. Cert. at ¶¶3(tt)(a) - (c). Prior to obtaining a court order requiring disclosure of those records from Verizon Wireless, the defendant's cellphone number was "confirmed from reports of her assistance in other child abuse investigation[s] when she worked as the Vice-Principal for the Pleasantville High School, Pleasantville, NJ." Cert. at ¶¶3(oo). A review of the records showed that between December 1, 2023 and February 13, 2024, over 100 outgoing and incoming telephone calls and text messages were exchanged between the defendant's cellphone number and cellphone numbers belonging to the Smalls, including the cellphone number of Mrs. Small which was found by detectives in the intake documents and [redacted]. Cert. at ¶¶3(r), (tt)(a) - (c).

Ultimately, ACPO (and DCPP) determined that a referral was never made to DCPP by the defendant, or anyone from the Atlantic City Board of Education, concerning [redacted]'s disclosures on January 22, 2024 that she was physically abused by the Smalls. Cert. at ¶¶3(nn). Rather, the only referral concerning such alleged abuse committed by the Smalls was made on January 24th by [redacted]'s supervisor. Cert. at ¶¶3(r).

In March 2024, investigators were granted warrants to search Chapman, her office at the Atlantic City High School, and her BMW and

to seize any electronic devices found in those locations. Cert. at ¶¶3(uu) – (vv). Upon executing the warrants at the high school, detectives seized the defendant's iPhone, her Samsung cellphone, and her iWatch (collectively, the "Devices"). Cert. at ¶¶3(ww) – (xx).

On March 20, 2024, ACPO Detective Daniel Choe of the Professional Standards and Accountability Unit authored the Certification, which details his extensive training and experience investigating child abuse incidents and official misconduct, and he further summarized the facts and circumstances giving rise to probable cause to believe that the Devices contained digital evidence relating to ACPO's investigation.

On March 20, 2024, Your Honor found probable cause and granted the Search Warrants, thereby authorizing a search of each device for:

> stored electronic information with regards to the above investigation [described in the Certification and] in relation to N.J.S.A. 2C:30-2a, Official Misconduct; N.J.S. 2C:5-2a(1), Conspiracy to Commit Official Misconduct; N.J.S.A. 2C:12-1(B)1, Aggravated Assault, a Crime of the Second Degree; N.J.S. 2C:24-4A2, Endanger the Welfare of a Child, a Crime of the Second Degree and N.J.S. 9:6-1, Child Abuse, a Crime of the Fourth Degree, more specifically, stored electronic information on the device – including, but not limited to: emails, all stored contact numbers, stored incoming and outgoing calls, stored incoming and outgoing text/image messages, stored chats, stored images/videos, internet website visitation/search history, and any additional stored digital evidence pertaining to passwords and/or encryption relating to the computer system, computer software, and/or any related device.

The Search Warrants commanded detectives to search the Devices for the "digital evidence herein above named" and for "the property specified."

LEGAL ARGUMENT

POINT I[1]

THIS COURT SHOULD DENY THE DEFENDANT'S MOTION TO SUPPRESS THE DIGITAL EVIDENCE BECAUSE THE PRESUMPTIVELY VALID WARRANTS WERE SUPPORTED BY AMPLE PROBABLE CAUSE TO SEARCH ALL THE DATA ON THE DEVICES

Our Supreme Court has long "announced a preference for law enforcement to secure warrants from detached judges prior to a search." E.g., State v. Boone, 232 N.J. 417, 426 (2017). In this case, such guidance was heeded precisely when Detective Choe applied for the Search Warrants from Your Honor, a detached Superior Court Judge, rather than engaging in presumptively invalid warrantless searches. Upon Your Honor granting the Search Warrants, all data on the Devices was searched and law enforcement uncovered digital evidence of official misconduct and the defendant's failure to report [redacted]'s child abuse disclosures.

Nonetheless, the defendant moves this Court to "quash the search warrants" which were granted by Your Honor based on the Certification because the Search Warrants were allegedly "overly broad in violation of State v. Missak." Db4-8. Ultimately, the defendant's proposed order seeks the extraordinary remedy of suppression of the entirety of the digital evidence which was obtained from searching the Devices.

The defendant's Motion lacks merit and must be denied. For starters, there is no basis in law to "quash" the Search Warrants

[1] Point I is responsive to Subpoint A of the defendant's brief.

because same were already executed after Your Honor's finding of probable cause. Second, contrary to the defendant's claims, Missak did not establish a per se ban on search warrants seeking "all data" on a cellphone. Rather, Missak merely held that a search warrant seeking all data on a device must be accompanied by probable cause to search all such data. As explained below, the State satisfied that holding by presenting probable cause to search all data, including all data before, during, after December 2023 to January 2024. Accordingly, this Court should deny the defendant's Motion, but for the sake of thoroughness, the State notes that the defendant's proposed order seeking total suppression of the digital evidence is contrary to longstanding precedent, which recognizes the remedy for an overbroad search warrant is merely to redact any items allegedly unsupported by probable cause.

A. Fundamental Search Warrant Principles and Overbreadth

"[S]earch warrants are strongly favored under the Federal and State constitutions." State v. Sheehan, 217 N.J. Super. 20, 26 (App. Div. 1987). Indeed, our Supreme Court has held time and again that a search executed pursuant to a warrant is "presumptively valid." E.g., Boone, 232 N.J. at 427; State v. Keyes, 184 N.J. 541, 554 (2005); State v. Jones, 179 N.J. 377 (2004); State v. Sullivan, 169 N.J. 204, 211 (2001). Thus, a defendant challenging a search warrant has the burden of proving "there was no probable cause supporting the issuance of the warrant or that search was otherwise unreasonable." Jones, 179 N.J. at 388.

"Probable cause for the issuance of a search warrant requires a fair probability that contraband or evidence of a crime will be found in a particular place." State v. Chippero, 201 N.J. 14, 28 (2009). In examining probable cause, the judge must consider "all relevant circumstances." Id. at 27. That is because "probable cause often arises out of the 'total atmosphere of the case," including "the suspect's occupation, reputation, [and] associates." State v. Tanzola, 83 N.J. Super. 40, 46-47 (App. Div. 1964). Furthermore, the judge must consider 'what is commonly known to be the usual procedures and operations of offenders in perpetrating the type of crime alleged." Id. at 44-45.

There is a marked contrast between a "general warrant" and a "warrant that is simply overly broad." United States v. $92,422.57, 307 F.3d 137, 149 (3d Cir. 2002). A general warrant authorizes an "exploratory search in a person's belongings." Ibid. Conversely, an overbroad warrant describes items in specific terms, but authorizes the seizure of items as to which probable cause is unestablished. E.g., State v. Sheehan, 217 N.J. Super 20, 28 (App. Div. 1987); Simmons v. Loose, 418 N.J. Super. 206, 225 (App. Div. 2011).

B. The Judicially Approved Search Warrants Were Adequately Supported by Probable Cause and Were Not Overbroad

Here, Detective Choe requested, and the Search Warrants authorized, a search for all "stored electronic information" on the Devices, including "emails, all stored contact numbers, stored incoming and outgoing calls, stored incoming and outgoing text/image messages,

stored chats, stored images/videos, internet website visitation/search history, and any additional stored digital evidence pertaining to passwords and/or encryption[.]" In the paragraphs below, the State explains why the Certification established probable cause to search all this data before, during, after December 2023 to January 2024 and, thus, the presumptively valid Search Warrants are not overbroad.

To understand why defendant's overbreadth argument is erroneous, a brief discussion of State v. Missak is warranted. There, the defendant allegedly used online chatting applications to exchange sexual messages with a detective posing as a juvenile; the messages were exchanged over a period of two days. 476 N.J. Super 302, 309-310 (App. Div. 2023). On the evening of the second day, the defendant was arrested after he attempted to meet up with the "juvenile" with whom he was chatting. Ibid. The defendant's cellphone was seized and a judge granted a warrant to search "all the phone's contents, information, and data" pertaining to the crimes of "luring and attempted sexual assault allegedly committed by the defendant on December 8 and 9, 2021." Id. at 310-311.

The Missak panel found that the search warrant satisfied the particularity requirement, but nonetheless the panel quashed the unexecuted warrant because it was overbroad insomuch as the detective's certification did not establish probable cause to search "all the data and information on the seized cellular phone." Id. at 322-23. The Missak panel reasoned that "the [certification] lacks facts establishing [that] the phone's text messages, calls communications, GPS data, or

other data created or existing prior to defendant's alleged initial communication with [the detective] posing as the juvenile on December 8, 2021, contain evidence of the two crimes for which [police] expressly sought the search warrant." Id. at 320. Thus, although the panel found that the unexecuted warrant was particularized, the warrant was quashed as overbroad because it sought data which "predate[d]" the criminal events and for which probable cause was lacking. Id. at 321-23.

Despite the defendant's attempts to analogize the Search Warrants to Missak, this matter is factually distinguishable and the State complied with Missak[2] by presenting probable cause to search all data on the Devices, including data before, during, and subsequent to December 2023 to January 2024. Factually, Missak involved an investigation of attempted child luring which spanned a mere two days, and the purpose of the search warrant was to prove one fact: identity. Put differently, the detectives in Missak applied for the warrant to essentially prove that the man who was arrested at the meeting location was the same man who had sent the sexual messages (over a two-day period) to the detective posing as a child. Ultimately, because of the narrow timeframe of the investigation in Missak and the narrow purpose

[2] The Appellate Division reached its holding in Missak after admitting it lacked an adequate record on how digital forensics work, and conspicuously absent from that decision is any discussion of the voluminous caselaw from jurisdictions across the nation which have disagreed with the logic of the lone Connecticut Supreme Court case upon which Missak relied in passing. Since Missak was decided in May 2023, it has never been cited in a published decision of the Appellate Division, nor has the Supreme Court ever passed on its validity.

of the warrant in that case, the Appellate Division found a lack of probable cause to search all the phone's data, including data prior to the sexually explicit chats. The detective in Missak simply did not articulate facts in her certification to support a request for data prior to and subsequent to the sexual messages and attempted meet up.

In contrast to Missak, the Search Warrants here concerned a broad investigation, and Detective Choe's Certification established probable cause that the defendant's devices contained data existing prior, during, and subsequent to December 2023 to January 2024, and further, such data "contain[ed] evidence of the [] crimes for which [Detective Choe] expressly sought the search warrant." Id. at 320.

Whereas Missak involved a narrow investigation of a single suspect spanning a mere two days, Detective Choe applied for the Search Warrants in this matter as part of an investigation involving multiple crimes, including child abuse, official misconduct, and conspiracy, and his investigation involved multiple individuals and events spanning multiple months. Moreover, unlike where identity was at issue in Missak, the detectives here were tasked with proving several legal elements comprising the crime of official misconduct, namely that (1) the defendant knew of her legal obligation to report child abuse; (2) the defendant knew how to report child abuse through the prescribed telephone hotline; and (3) and that the defendant failed to report [redacted]'s disclosures. See Model Jury Charge (Criminal) Official Misconduct (9/11/06). Regarding the latter, the investigators were also

tasked - even more specifically - with proving that no report was made in any medium by the defendant to either DCPP, or to law enforcement. And lastly, Detective Choe was investigating the "benefit" element of the crime of official misconduct, which is closely related to "motive."

Against the factual backdrop of the Certification, and in recognition of these legal elements, the State presented probable cause to search all data on the Devices, as explained in more detail below.

i. The Certification Established Probable Cause to Search All Data for Evidence of the Defendant's Knowing Failure to Report [redacted]'s Disclosures to DCPP or Law Enforcement

Here, Detective Choe had probable cause to search all call, message, and chat data on the Devices from December 2023 to January 2024 to prove that the defendant never complied with her obligations to report [redacted]'s disclosures. Unlike in Missak, the Search Warrants in this case were sought to prove a negative: the defendant never reported [redacted]'s disclosures. And to prove that negative and to show the defendant never complied with her mandatory reporting obligations for child abuse, it was necessary to examine all call, message, and chat data on the Devices, including from December 2023 to January 2024. Indeed, only by reviewing all such data could Detective Choe prove the negative, and it bears emphasizing DCPP required disclosure by a telephone hotline.

There was also probable cause to search all call, message, and chat data, because not only did Detective Choe seek the Search Warrants to disprove that the defendant reported [redacted]'s disclosures, he had to prove yet another negative: that the defendant never reported [redacted]'s

disclosures in any medium or form, including by phone, text message, or any cellphone-based chat applications. Of course, the very purpose of a cellphone is to communicate through such capabilities. E.g., State v. Earls, 214 N.J. 564, 587 (2013) (recognizing, in 2013, that "cell phone use has become an indispensable part of modern life and "[p]eople buy cellphones to communicate with others, to use the internet, and for a growing number of other reason") (emphasis added). Thus, Detective Choe reasonably applied for authorization to search all communication data because had the defendant complied with her duty to report, which she did not, the communication data would have exculpated her. Conversely, the absence of any such report in the data is probative of her guilt and evidence of the crimes for which the Search Warrants were sought.

Probable cause to search all call, message, and chat data before and after December 2023 to January 2024 was also satisfied because, in addition to being tasked with proving the aforesaid "negatives," the investigators were tasked with proving – affirmatively - that the defendant knew about her obligation to disclose child abuse and that she knew how to do so through the DCPP hotline and to law enforcement. Hence, the Certification established probable cause to examine all call, message, and chat data on the Devices, including before and after December 2023 and January 2024, in order to search for all discussions of, and incidents where, the defendant actually complied with her reporting obligations. Such evidence is extremely relevant; it proves the defendant knew about her legal obligation to report abuse and that

she knew how to fulfill it by calling DCPP and the police, which are all elements the State must prove beyond a reasonable doubt at trial.

In other words, there was a fair probability that all the Devices' call, message, and chat data from prior and subsequent to December 2023 to January 2024 included occasions where the defendant complied with her obligations to disclose to DCPP or law enforcement. Those occasions would be highly probative evidence that the defendant knowingly failed to comply with her reporting duties with respect to [redacted]'s disclosures. See Model Jury Charge (Criminal) Official Misconduct (9/11/06) (requiring the State to prove that the defendant "knowingly" refrained from performing an official act, or that she committed such an act in an unauthorized manner "knowing" that the manner was unauthorized).

By arguing the Certification fails to establish any facts satisfying probable cause to search call, message, and chat data before December 2023, the defendant disregards salient facts in the Certification. Detective Choe certified that the defendant's cellphone number was "confirmed" (prior to court-ordered disclosure of her cellphone records) "from reports of her assistance in other child abuse investigation[s] when she worked as the Vice-Principal for the Pleasantville High School." Cert. at ¶¶3(oo). Thus, Detective Choe presented facts that the defendant used the same cellphone number as when she was an educator subject to mandatory reporting of child incidents before the 2023 – 2024 school year. Thus, there was a "fair probability" that the Devices contained data prior to December 2023

which showed the defendant had reported child matters, thereby further proving that she "knowingly" failed to report [redacted]'s disclosures.

For reasons similar to those already articulated, Detective Choe had probable cause to search all email data on the Devices. The Certification establishes that Atlantic City High School had a policy specifying that any staff member who contacted DCPP to report an allegation of abuse must thereafter complete and email a proscribed form to the Superintendent's Office. Cert. at ¶¶3(aa)(6). Accordingly, Detective Choe had probable cause to search all emails from December 2023 to January 2024 to disprove that the defendant completed and sent the requisite form with respect to [redacted]'s disclosures. So too, Detective Choe had probable cause to search emails before and after December 2023 to January 2024, because all emails where the defendant complied with school policy by completing and emailing the form would prove that she "knowingly" violated the policy with respect to [redacted]'s disclosures.

Relatedly, the Certification established probable cause to search all stored contact data on the Devices. Like the data described above, there was a "fair probability" that the contact data contained evidence pertaining to the crimes under investigation, namely whether the defendant saved in her contacts either the DCPP hotline, or telephone numbers of the school resource officer or the Atlantic City Police Department. The lack of any such saved contacts is of course probative evidence that the defendant never reported [redacted]'s disclosures.

Detective Choe likewise had probable cause to search all internet visitation and search history, including before, during, after December 2023 to January 2024. There was a "fair probability" that such data would reveal searches proving the defendant knew about her mandatory reporting duties and how to comply with them, such as any instances where the defendant searched for or visited websites with the DCPP hotline, whether she searched for or visited websites concerning the legal duties to report child abuse, and whether she searched for or visited websites concerning school policies for reporting child abuse.

In sum, the presumptively valid Search Warrants did not suffer from the fatal flaw articulated in Missak where the detective in that case did not establish probable cause that data existing prior to the sexual messages contained evidence relevant to the crimes being investigated. Rather, Detective Choe's certification established probable cause to search all data before, during, and after December 2023 to January 2024 as such data contained evidence of the defendant's knowing failure to report [redacted]'s disclosures of child abuse.

ii. The Certification Established Probable Cause to Search All Data for Evidence the Defendant Committed Official Misconduct by Notifying the Smalls of [redacted]'s Disclosures

In granting the Search Warrants, this Court properly found there was probable cause to search all data on the Devices for evidence of official misconduct. That is because there was a "fair probability" that all data would contain evidence of the defendant's knowing failure to comply with her mandatory duty to report [redacted]'s child abuse

disclosures to DCPP and law enforcement. See Subpoint i. But there is another reason why there was probable cause to search such data: there was a fair probability, that the data contained evidence that the defendant committed official misconduct by notifying the Smalls of [redacted]'s disclosures, even though the Smalls were accused of abusing [redacted]

In relevant part, the Certification established: (a) the defendant did not report [redacted]'s disclosures as required; (b) the defendant called Mrs. Small on January 22, 2024 which was the date of the First Meeting and [redacted] disclosure's to the counselor; (c) later on January 22nd, the defendant met with the Smalls, inside her BMW, at their home; (d) the defendant communicated with the Smalls more than 100 times, including on January 31st (i.e., the day that detectives interviewed [redacted] at the high school, and the day that Mr. Small drove to the high school and was video recorded talking on his cellphone); and (e) on January 24, 2024, after DCPP finally learned about [redacted]'s disclosures from [redacted] supervisor, DCPP went to the Smalls' home where Mrs. Small stated her "good friend," whom she refused to identify, had told Mrs. Smalls in advance about a potential investigation by DCPP.

Viewing those facts collectively, it was reasonable to infer the defendant illegally[3] notified the Smalls of [redacted]'s disclosures and that the data on the Devices would contain such evidence. It was also

[3] See N.J.A.C. 6A:16-3.2 (discussing mandatory policies for child interviews and specifying that "[s]chool officials shall not notify the student's parent(s) in instances of suspected child abuse or neglect.").

reasonable to infer that Mrs. Small was the "good friend" who had illegally warned Mrs. Small of [redacted]'s disclosures – a clear benefit under the official misconduct statute, as the Smalls had advance notice and time to prepare for any investigations by DCPP and law enforcement.

Accordingly, there was probable cause to search all data, before, during, after December 2023 to January 2024, to locate evidence pertaining to the defendant's relationship with the Smalls. Only by searching all data, including searching for any photos and videos of the defendant with the Smalls, could the detectives fully determine the extent, nature and scope of the defendant's ties to, and relationships with, the Smalls – which would be highly relevant to whether the defendant sought to benefit the Smalls by not reporting [redacted]'s disclosures which, if reported, would negatively impact the Smalls.

iii. Search Warrant Jurisprudence and Principles of Forensic Science Bely the Defendant's Claims that the Search Warrants Should Have Been Limited by Data Types or Dates.

A search warrant for an area generally authorizes the search of all subareas therein, even if the subareas are not explicitly mentioned in the warrant. E.g., United States v. Ross, 456 U.S. 798, 820-21 (1982); State v. Watts, 223 N.J. 503, 515 (2015). A warrant to search a specific area also permits a search of containers "found therein that might reasonably contain any evidence sought by the warrant." E.g., See State v. Jackson, 268 N.J. Super. 194, 208 (Law. Div. 1993).

Here, the Devices searched pursuant to the Search Warrants are containers which "contain" numerous interconnected folders, files, and

databases, which enable the Devices to function. Although the Devices are electronic data storing devices, the Devices should not be viewed "differently from [tangible] storage mediums such as filing cabinets and briefcases[.]" United States v. Giberson, 527 F.3d 882, 887-89 (9th Cir. 2008); United States v. Highbarger, 380 Fed.Appx. 127, 130 (3d Cir. 2010); State v. Melia, 2014 WL 10186793 at *8 (App. Div. 2015) (citing Giberson with approval). And just like a search of a filing cabinet, the evidence sought on the Devices by the Search Warrants was reasonably likely to be located in any file or folder therein. E.g., United States v. Bishop, 910 F.3d 335, 337 (7th Cir. 2018); United States v. Murphy, 2024 WL 3440149 at *13 (D.N.J. 2024); United States v. Graham, 2022 WL 4132488 at *4 (D.N.J. 2022).

The authorization by the Search Warrants to search "all" data also comported with traditional case law governing search warrants. "When a search requires review of a large collection of items, such as papers, 'it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" United States v. Williams, 592 F.3d 511, 519-20 (4th Cir. 2010) (quoting Andersen v. Maryland, 427 U.S. 463, 482 n.11 (1976)). Relatedly, given the nature and volume of information contained within, law enforcement are afforded discretion in executing search warrants on electronic devices. E.g., United States v. Ulbricht, 858 F.3d 71, 101-02 (2d Cir. 2017) (approving agent's "cursory" review of numerous files on laptop during warrant execution

to ascertain their relevance); United States v. Bass, 785 F.3d 1043, 1050 (6th Cir. 2015) (approving broad scope of search warrant as "the officers could not have known where [the] information was located in the cell phone or in what format"); United States v. Stabile, 633 F.3d 219, 238-239 (3d Cir. 2011)("'the search warrant itself need not 'contain a particularized computer search strategy,'" but may consist of "a focused search of the hard drives" based on specified crimes).

Unlike in some jurisdictions, our Rules of Courts do not require search warrant applications to explain the methodology (that is, the forensic processes) by which a cellphone is to be searched pursuant to a warrant.[4] Nonetheless, a brief discussion of digital forensics helps explain why all data on a device must reviewed, and that limiting data by data type or dates – which our caselaw has never required - would be infeasible and generate highly skewed and misleading results.

The National Institutes for Standards and Technology ("NIST") is a federal agency charged with the examination and development of standards for technology, both public and private. NIST recognizes that mobile devices have dependencies between different data elements. For

[4] It bears noting that the Certification did prove an overview of the methodology by which the Search Warrants would be executed. See Cert. at ¶¶7(a) – (b). That was not required by law and it far exceeded what is typically included in traditional search warrants, which are to be viewed on equal footing as that of digital devices. E.g., United States v. Giberson, 527 F.3d 882, 887-89 (9th Cir. 2008). For example, a residential search warrant need not specify which rooms the police will enter first, which containers the police will review and seize, how quickly the police will go through certain areas, and related matters.

example, extracting call logs may require accessing the device's call history database, which may be interconnected with other databases such as contacts or messaging applications. As explained more below, removing specific items without considering these dependencies can result in incomplete or inaccurate information and otherwise provide a review of said evidence which lacks a contextual understanding of the evidence.

Only by examining the relationships between files, directories, logs, databases, and applications, can investigators accurately reconstruct the user's actions, interactions, and patterns of behavior. This contextual information is invaluable in understanding the purpose and significance of specific data and is essential to building a coherent narrative during the investigation. See Digital Investigation Techniques: A NIST Scientific Foundation Review, NISTIR 8354 (2022). NIST further emphasizes that anti-forensic techniques can be used to hide data. Consequently, a forensic examination requires the extraction of "all" data on a mobile device; the data is then rendered for commonly used applications onto a digital report, along with file systems which contain the data, in order to render applications not otherwise supported by the software. Ibid. This digital report is then reduced to a readable .pdf report.

Understanding a digital device's dependency on its files, directories, logs, databases, and applications, is most easily understood when a person receives a telephone call. While the person merely hears their phone ringing and vibrating in response to a call,

the device itself is interacting with the cellular telephone network, verifying that the person receiving the call or text is a valid user. The phone itself then ensures that the settings set by the person are followed, plays the person's ringtone or vibration pattern, identifies the number of the person calling, displays the calling number listed in the person's contacts, displays the avatar or photo assigned to the contact, registers the call in a call log, and connects the call.

If a call is not answered, the device then accesses its voicemail system and registers a missed call within a set database within the phone. The phone then stores the information. See Rohit Tamma, et al., Practical Mobile Forensics. 4th Ed. (Packt Publishing 2020). If the call received is through a rich communication services ("RCS"), which is available on both Google and Apple (iMessage), the device does not use the traditional cellular telephone network, nor may a communication be recorded on traditional phone records kept by a cellular provider. Modern mobile devices often receive and send both RCS and traditional telephony communications. See "Best Practices for Mobile Device Analysis," Scientific Working Group on Digital Evidence Version 1.0 (September 17, 2020). If a third-party application (e.g., Whatsapp, Telegram, or Kik Messenger) is used to receive a telephone call, the user believes the same process is used, but, in actuality, numerous other databases and logs, set forth by the third-party application's package, or apk for Android or ipa for iPhone, interact with the device and its files and folders to receive the phone call.

Similar interconnected processes occur when an individual receives a text message. Moreover, a peripheral device, such as an iWatch, captures communications, in part, in a similar manner as explained above. However, due to data storage limitations, peripheral devices do not retain the communications for as lengthy of a period as a smart phone that received the initial call or text message. Thus, a forensic examiner may need to individually review all files, directories, logs, and databases depending on the device's make, model, and file structure.

In sum, due to the interconnected nature of a device's databases, folders, and files, a digital forensic examiner cannot merely extract one particular portion of the data, such as phone logs or text messages, without extracting the entirety of the data. Moreover, the notion that a search of a digital device can be cabined to a certain set of data defies principles of digital forensic science, as such cabining leads to the data being skewed or rendered unreadable. See "Considerations for Required Minimization of Digital Forensics Seizure," Scientific Working Group on Digital Evidence Version 2.1 (August 5, 2024). Moreover, this is the case even if the entirety of the data is filtered post-extraction through digital forensic software. Ibid.

To illustrate, the Scientific Working Group on Digital Evidence ("SWGDE") has published reports discussing how limiting data searches by date or time ranges creates inaccurate and skewed results. See Considerations for Required Minimization of Digital Evidence Seizure 16-F-002-2.1 Version: 2.1 (8/5/2024); SWGDE Best Practices for Mobile

Device Forensic Analysis Version: 1.0 (September 17, 2020). For example, SWGDE imposed a "date range" limitation of one date (the alleged offense date) on multiple conversations exchanged between two individuals which were extracted from a device's text message data. SWGDE concluded that the "device user's act of deleting relevant messages that occurred on that date had removed the timestamps on these now deleted, but still recoverable messages," and consequently, "imposition of a 'date range' limitation on the data that could be analyzed excluded this probative evidence from the investigation." SWGDE reached similar conclusions with respect to data type and date limitations and other types of extracted data, such as internet history. Thus, the SWGDE findings demonstrate that data type and date limitations improperly exclude relevant evidence encompassed within a search warrant's authorization.

Here, the defendant's Verizon cellphone records (referenced in the Certification) demonstrated that the defendant communicated with the Smalls repeatedly. But those call detail records captured only voice calls and text messages; the records provided none of the additional information generated through the processes described above in detail, which were contained solely in the Device's data. Therefore, there was probable cause to search "all" the data on the Devices in order for Detective Choe to obtain this relevant and additional information, and all the data had to be searched because of the interconnectedness of the data and how electronic devices operate, again as described above.

The defendant, however, argues that the Search Warrants impermissibly authorized a search of "all" data, and that only restricted searches should have been completed. However, this argument completely overlooks the fact that if only a limited search of the data was undertaken, then detectives would have failed to locate all relevant evidence authorized by the Search Warrants[5], as exemplified in the aforementioned reports published by SWGDE. And a limited review of the data, as advocated by the defendant, would have run the risk of detectives unknowingly "missing" exculpatory evidence, such as any communications between her and DCPP. Accordingly, a review of all data was necessary under principles of forensic science and to ensure the State fully disproved that the defendant ever reported [redacted]'s disclosures to DCPP or law enforcement, as required by law and policy.

To conclude, the defendant's claim that the Search Warrants should have been limited to a search by data type or by date-limitation is belied not only by well-established principles of traditional search warrant jurisprudence, but also forensic science. Indeed, such limitations are infeasible and lead to misleading and skewed results.

[5] Should the Court desire it, the State will produce an expert witness, with notice to the defense, to further explain these digital processes.

C. The Remedy for an Overbroad Search Warrant is Redaction

Even if the Search Warrants were overbroad, which is not the case, the proper remedy is not wholesale suppression of all digital evidence, as advocated by the defendant in her proposed order. Rather, under well-settled law, the remedy for an overbroad warrant is simply to redact the timeframe of any records for which probable cause was lacking.

Evidence seized pursuant to an overbroad warrant is not subject to total exclusion. State v. Burnett, 232 N.J. Super. 211, 217 (App. Div. 1989). Rather, "where articles of personal property are seized pursuant to a valid warrant, and the seizure of some of them is illegal as beyond the scope of the warrant, those illegally taken may be suppressed, or excluded at trial, but those within the warrant do not become so tainted as to bar their receipt." State v. Dye, 60 N.J. 518, 537 (1972); State v. Masco, 103 N.J. Super. 277, 282 (App. Div. 1968) (holding that erroneous inclusion in search warrant of command to search the person as well as the premises "did not vitiate the warrants – that since the warrants were valid as to one command and not as to the other, the part which was not essential or invalid may be treated as surplusage").

The Appellate Division's decision in Burnett, 232 N.J. Super. 211 (App. Div. 1989) is illustrative. There, the Appellate Division found there was probable to issue a search warrant for records in the defendant's office relating to an illegal kickback scheme, but the authorization to search records "covering a period of approximately ten years" was "overly broad." Id. at 213, 215-16. Under such circumstances

the Appellate Division held that the remedy was to "redact" the records which were not supported by probable cause in the affidavit, observing:

> [O]therwise admissible evidence should not be excluded because a portion of the warrant authorizes the seizure of [evidence] . . . in excess of that justified by the supporting affidavit. The proper remedy is redaction, the striking of those portions of the warrant which are invalid for want of probable, and preserving those several portions that satisfy the Fourth Amendment, and our state constitutional counterpart.
>
> [Id. at 217 (internal quotations and citations omitted).].

Thus, after "[c]onsidering the facts set forth in the affidavit issued in support of the search warrant," the Appellate Division ordered that the "seizure of defendant's records should be limited to a period inclusive of one year," which was the "longest period which could reasonably have been granted by the issuing judge upon the initial application for the search warrant." Id. at 218.

The same exact logic applies here. Accordingly, should the Court grant the defendant's Motion, which the State strongly opposes, the sole and proper remedy in law is merely redaction of the records.

D. The Search Warrants Satisfied the Particularly Requirement

The defendant also raises a particularity argument, alleging that the Search Warrants granted by Your Honor did not "provide any guidance to the executing officers for them to know what they could seize and what was off limits." Db7. This claim, however, is belied by Missak which observed: "[T]he fatal flaw in the warrant is not that it does not define with particularity where the search may be conducted. The warrant is very particular – it allows a search of all the phone's contents, information, and data." 476 N.J. Super at 323.

Here too, the Search Warrants were sufficiently particularized to a search of all "stored electronic information," including "emails," "stored contact numbers," "stored incoming and outgoing calls," "stored incoming and outgoing text/image messages," "stored chats," and "internet website visitation/search history." Furthermore, the Search Warrants were particularized to a search of such evidence with "regards to the [] investigation" in the Certification and the specified crimes listed by Detective Choe. E.g., United States v. Bishop, 910 F.3d 335, 337 (7th Cir. 2018) (recognizing a warrant authorizing the search of a cellphone is sufficiently particularized "if the warrant cabins the things being looked for by stating what crime is under investigation").

Based on the foregoing, the Search Warrants were not invalid general warrants authorizing an exploratory search for illegality, but rather the Search Warrants were sufficiently particularized and limited to specified data being searched in relation to specified crimes.

POINT II[6]

THIS COURT SHOULD DENY THE DEFENDANT'S MOTION TO SUPPRESS THE SEARCH WARRANTS BECAUSE THE CERTIFICATION ESTABLISHED PROBABLE CAUSE TO SEARCH ALL THE DEVICES AND THE DEFENDANT HAS NOT OVERCOME THE STRONG PRESUMPTION OF VALIDITY OF THE JUDICIALLY APPROVED SEARCH WARRANTS

The defendant alleges this Court abandoned its neutral and detached role by granting the Search Warrants despite there being no probable cause to search the Devices. More specifically, the defendant argues that Detective Choe was required to state with absolute precision the evidence sought by the Search Warrants and, furthermore, that probable cause was non-existent to grant Search Warrants for all Devices because there was no "nexus" between the Devices and evidence of illegality. Db8-12. As explained below, the defendant's hypercritical review of the Certification is contrary to longstanding jurisprudence. Moreover, the Certification established probable cause to search "all" Devices, because all her devices contained evidence of Official Misconduct, namely the lack of any communications on those devices to DCPP or law enforcement concerning [redacted]'s disclosures. Thus, the defendant's Motion to Suppress the Search Warrants should be denied.

Long ago, our Supreme Court admonished trial courts to "always remember" that police officers "are not constitutional lawyers." State v. Miller, 47 N.J. 273, 279 (1966). Moreover, a court reviewing a

[6] Point II is responsive to Subpoint B of the defendant's brief.

challenge to a search warrant must "accord substantial deference to the discretionary determination resulting in the issuance of the [search] warrant." Keyes, 184 N.J. at 554. The reviewing "court's role is not to determine anew whether there was probable cause for issuance of the warrant, but rather, whether there is evidence to support the finding made by the warrant-issuing judge." Chippero, 201 N.J. at 20-21 (emphasis added). Given the strong preference for detectives to obtain a search warrant, "when the adequacy of the facts offered to show probable cause is challenged after a search made pursuant to a warrant, and their adequacy appears to be marginal, the doubt should ordinarily be resolved by sustaining the search." Jones, 179 N.J. at 388-89.

Here, the defendant claims that Detective Choe made "conclusory" assertions of probable cause and that he only "vaguely" described the evidence of illegality which was sought on the Devices. This "grudging" and "negative" view toward the Certification is antithetical to longstanding Supreme Court precedent that certifications authored by detectives must not be scrutinized for the "technical nicety one would expect of a member of the bar." State v. Kasabucki, 52 N.J. 110, 117 (1968). Rather, all that matters is whether the Certification supported a judicial finding of probable cause that the Devices contained evidence of criminal activities, and Your Honor has already made that finding.

To be sure, the presumptively valid Search Warrants were supported by probable cause to believe all the Devices contained evidence of criminal activity, thereby satisfying the "nexus" requirement.

Crucially, the Certification articulated there was no record of the defendant having reported [redacted]'s disclosures to DCPP or law enforcement. Thus, there was a fair probability that all her devices contained evidence of official misconduct, that evidence being the absence of any communications by the defendant to either DCPP or law enforcement concerning [redacted]'s disclosures. In other words, there was a "fair probability" that the data on all the Devices would prove that the defendant used none of the Devices she possessed to report [redacted]'s disclosures, which was evidence that she committed Official Misconduct.

Certain facts in the Certification underscore a clear link between all the Devices and evidence of official misconduct. For example, one particularly salient fact (which the defendant disregards) is the location where the Devices were seized: the high school. That location was effectively the "scene of the crime," and her employment at the high school was the very reason she was required by law to report child abuse, and to do so through mediums accessible via cellphone (i.e., a telephone hotline and email). The Certification also established that the defendant used her cellphone to contact the Smalls over 100 times during the investigation, including the date [redacted] disclosed at school, and furthermore the Certification established that the defendant had used the same cellphone number to previously report child incidents as a vice principal in Pleasantville. Collectively, these facts showed the defendant routinely used a cellphone to communicate and that she had a record of using a cellphone to report child-related matters. E.g.,

Tanzola, 83 N.J. Super. at 46-47 (recognizing probable cause includes a consideration of 'what is commonly known to be the usual procedures and operations of offenders in perpetrating the type of crime alleged"). Thus, to prove that the defendant did not report [redacted]'s discloses, Detective Choe reasonably sought to search all Devices in her possession which had the capability to contact DCPP or law enforcement.

It was also reasonable to believe that the Devices contained communications between the defendant and the Smalls which were evidence of criminal activities. It was reasonable to infer that one of the devices seized from the defendant corresponded to (i.e., had a nexus to) the Verizon cellphone records showing over 100 contacts with the Smalls. It was also reasonable to infer that the defendant, given her repeated and frequent communications with the Smalls via phone, text, and inside of her BMW on the day of [redacted]'s disclosure at the high school, may have contacted the Smalls with the second seized cellphone, which would not be reflected in the Verizon cellphone records. Thus, Detective Choe reasonably, and with probable cause, sought authorization to search the Devices for any communications proving the defendant conspired with the Smalls not to report[redacted]'s disclosures, or that she had illegally warned them of [redacted]'s disclosure. See N.J.A.C. 6A:16-3.2 (pursuant to mandatory policies to be adopted regarding child interviews, "[s]chool officials shall not notify the student's parent(s) in instances of suspected child abuse or neglect").

Despite the clear adequacy of the Certification, the defendant argues, in various[7] iterations, that there was no nexus between the Devices and evidence of illegal activities. Db9-12. However, these arguments read more like a trial summation concerning proof beyond a reasonable doubt rather than mere probable cause to issue a warrant. Moreover, the crux of the defendant's arguments is that Detective Choe needed direct evidence that she used each device to engage in illegality, such as a conspiracy, before probable cause existed. However, the State need not present direct evidence linking items being searched for and the locations being searched. Judges are entitled to draw reasonable inferences about where evidence is likely to be kept based on the nature of the evidence and the circumstances of the offense being investigated. E.g., State v. Harris, 143 N.J. Super. 314 (Law Div. 1976) (presence of defendant's fingerprints at the scene of a

[7] For example, the defendant argues that only one phone number exchanged the calls and texts in the Verizon cellphone records and thus warrants should not have been granted for two phones. Db11. However, there was a fair probability that one device corresponded to the Verizon cellphone records, there was a fair probability that both devices contained communications with the Smalls, and there was a fair probability that both Devices contained an absence of any communications by the defendant to DCPP concerning [redacted]'s disclosures. Furthermore, a detective need not "link" a phone number to an exact device before a judge can find probable cause that the device contains evidence of illegality. In fact, the defendant's argument in this regard is contradicted by Missak where there was no evidence that the defendant used the cellphone found on his person to send the sexual messages to the detective posing as a juvenile, but yet the Appellate Division had no difficulty drawing inferences from all the circumstances to conclude there was "probable cause to believe the phone found in defendant's possession contained some evidence of the crimes charged." Missak, 476 N.J. Super at 320.

residential burglary supported probable cause to issue a search warrant for the defendant's home and vehicle, because it was reasonable to infer that a burglar would secrete stolen items in such locations).

Here, for the reasons expressed in Point I and above, the facts cited in the Certification - combined with the reasonable inferences to be drawn from those facts - provided probable cause to search all the Devices for evidence of criminality. Nevertheless, the defendant attempts to defeat probable cause by self-servingly characterizing her contacts with the Smalls as "innocent." Db11-12. These arguments misapprehend that, as a matter of law, the totality of the defendant's conduct must be considered through the eyes of Detective Choe, who recognized such conduct to be consistent with criminality based on his extensive experience investigating child abuse and official misconduct incidents, which he described in the Certification. E.g., State v. Arthur, 149 N.J. 1, 11-12 (1997) (reversing lower court order suppressing evidence; finding that although the defendant's conduct was susceptible to "purely innocent connotations," such conduct should have been viewed through the training and experience of the observing police officer who recognized the conduct to be consistent with wrongdoing).

The defendant also claims she is entitled to a Franks hearing because the Certification omitted her "closeness" to the Smalls and her work as Mr. Small's campaign manager. Db11. No such hearing is required. Rather than defeat probable cause, these facts would have strengthened probable cause to believe that the defendant failed to report [redacted]'s

disclosures to "benefit" her friend, Mr. Small, by sparing him an embarrassing allegation that would negatively impact him politically. See State v. Smith, 212 N.J. 369, 398-99 ("[W]here the challenger alleges the affidavit is fatally inaccurate by reason of omission," the "issue" is "whether inclusion of the omitted information would defeat a finding of probable cause; it is not . . . whether a reviewing magistrate would want to know the information") (emphasis added).

In sum, the Certification contained ample facts supporting this Court's finding of probable cause to issue the Search Warrants. But even if this was a "close case," which the State strongly disputes, the defendant's Motion should be denied. That is because our Supreme Court has held that if in hindsight the "adequacy" of a certification's contents "appears to be marginal," substantial deference should be afforded to the initial probable cause determination. Indeed, any "doubt should ordinarily be resolved by sustaining the search."

Respectfully submitted,

WILLIAM E. REYNOLDS
ATLANTIC COUNTY PROSECUTOR

By: */s/ Christopher Santo D'Esposito*
Assistant Prosecutor

/s/ Kathleen E. Robinson
Chief Assistant Prosecutor

/s/ Joseph Remy
Assistant Prosecutor

C Defense Counsel (via eCourts)