UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA v. JOSEPH SMITH, Defendant.	Criminal Action No. 19-324 (BAH) Chief Judge Beryl A. Howell

MEMORANDUM OPINION

Defendant Joseph Smith is charged in a 19-count indictment with child sexual abuse, production and possession of child pornography, and enticing a minor, based on allegations that, between May 2016 and April 2017, he sexually abused his stepdaughter, referred to in this case by her initials "A.S." *See generally* Indictment, ECF No. 13. This case has been pending for over two years, with the trial now re-scheduled for the third time to begin on October 18, 2021, and defendant has for the first time moved to suppress all evidence obtained from the execution of a search warrant at his apartment on April 21, 2017, and, as pertinent here, the seizure of a Lenovo personal computer ("Lenovo PC"), a Motorola cell phone, and an Apple iPhone 6S. Def.'s Mot. Suppress Tangible Evid. and Electronic Data ("Def.'s Mot."), ECF No. 114. Pursuant to this and subsequent warrants obtained to search the seized electronic devices, the government searched and recovered incriminating evidence on the Lenovo PC, Motorola cell phone, and iPhone 6S and intends to offer this evidence at trial. Defendant argues that the warrant authorizing the April 21, 2017 search of his apartment lacked probable cause, was insufficiently particular, and was overbroad; that the flaws with the 2017 warrant were not cured by the subsequent warrant obtained by the government in 2019; and that the good-faith exception

to the exclusionary rule should not apply. For the reasons described below, defendant's motion to suppress is denied.

I. BACKGROUND

The factual and procedural background of this case was described in detail in a previous opinion addressing five pretrial motions. *See United States v. Smith*, Case No. 19-cr-324 (BAH), 2020 WL 5995100 (D.D.C. Oct. 9, 2020).[1] The facts and procedural history below describe the information relevant to defendant's pending motion to suppress.

A. Relevant Factual Background

On April 21, 2017, the government applied for a Search Warrant for defendant's apartment located at 1301 C Street SE, #32 Washington, D.C. Def.'s Mot., Ex. A, Aff. of Jenny Alvarenga Supp. Appl. Search Warrant ("2017 Aff."), ECF No. 114-2. The application sought authorization to search for and seize evidence including "[c]ellular phones, computers, digital storage devices, thumb drives, removable electronic devices such as external hard drives," as well as "the extraction of all electronic data stored inside of them," and "any items or materials relating to the offense of First Degree Child Sexual Abuse." *Id.* at 3.

The affidavit in support of the warrant described the events that prompted the investigation and recounted A.S.'s statements days earlier at the Children's Advocacy Center. *Id.* at 1–2. The affiant averred that on April 19, 2017, a Metropolitan Police Department

[1] In this opinion, the Court: (1) granted in part and reserved in part the government's motion to admit A.S.'s prior statements, Gov't's Mot. *in Limine* to Admit A.S.'s Prior Statements, ECF No. 24; (2) granted the government's motion to admit evidence of defendant's other bad acts, Gov't's Mot. *in Limine* to Admit Evidence Pursuant to Fed. R. Evid. 404(b), ECF No. 31; (3) granted in part and denied in part the government's motion to preclude introduction of evidence about A.S.'s sexual history under Federal Rule of Evidence 412, Gov't's Mot. *in Limine* to Bar Evid. Regarding the Sexual History of Victim and to Exclude Evid. Offered to Prove the Victim's Sexual Predisposition, ECF No. 32; and (4) denied defendant's two motions to exclude the government's proposed child sexual abuse expert, Def.'s Mot. Exclude Testimony of Gov't's Proposed Expert, ECF No. 36, and for a *Daubert* hearing, Def.'s Suppl. Mot. to Exclude Expert Testimony of Dr. Stephanie Wolf and Req. for *Daubert* Hearing ECF No. 63. *See generally Smith*, 2020 WL 5995100.

("MPD") officer contacted the Youth and Family Services Division of MPD, reporting that A.S. had disclosed to her mother that she had been sexually abused by defendant since May 2016. *Id.* at 1. That day, A.S. was forensically interviewed at the Children's Advocacy Center. *Id.* During the interview, A.S. indicated that defendant had repeatedly forced her to perform oral sex on him and forced her to receive oral sex from him beginning in May 2016. *Id.* The victim identified her stepfather, defendant Joseph Smith, as the person who abused her while she and her mother and sibling lived at his apartment. *Id.*

A.S. described defendant's use of electronic devices in perpetuating and communicating with her about the abuse. According to A.S., defendant would send text messages to her describing his expectations for future instances of sexual abuse. *Id.* at 2. She specifically disclosed that "in one of the texts the suspect sent her, he told her that for her 14th birthday he was going to put his penis in her vagina and her anus." *Id.* She further disclosed that "she would send the suspect nude pictures of herself at his request" and that "she ha[d] observed the suspect connecting his cellular phone to a computer located in his bedroom." *Id.* The victim also indicated that defendant had taken her cell phone, as well as her mother's, when the victim and her mother left the defendant's apartment on April 14, 2017, following a domestic violence incident between defendant and the victim's mother. *Id.* at 1.

In the affidavit, Detective Alvarenga described that, in her experience, sex offenders frequently "take pictures of their victims," store those images on their phones, and also "often store the[] images on their personal computers," sometimes to distribute the images on social networking sites or to sell them. *Id.* at 3.

Based on the affidavit, a D.C. Superior Court judge issued the requested search warrant, specifically authorizing the search of the premises for evidence of an offense in violation of D.C.

Code § 22-3008 (First Degree Child Sexual Abuse), and the seizure of that evidence, including extractions of electronic data from seized devices. Def.'s Mot., Ex. A, 2017 Warrant, ECF No. 114-2. The warrant authorized the search of the premises for:

> Cellular phones, computers, digital storage devices, thumb drives, removable electronic devices such as external hard drives, and the extraction of all electronic data stored inside of them to take place at the residence or a police or court facility, mail matter, any material identifying any resident of the house and to take photographs and sketches of the entire premises, and any items or material related to the offense of 1st Degree Child Sexual Abuse[,] which is [e]vidence of an offense IN VIOLATION OF DC Code 22-3008.

Id. The search warrant was executed that same day, April 21, 2017, and law enforcement seized the Motorola cell phone, iPhone 6S, and Lenovo PC, as well as three tablets, ten additional cell phones, an Xbox, and an air mattress. *Id.*

In May 2017, forensic examination of the seized devices was conducted by the Digital Evidence Unit of the D.C. Department of Forensic Sciences ("DFS"). Def.'s Mot. at 2 (describing extraction of sixteen digital devices); *see also id.*, Ex. C., May 11, 2017 Rep. of Examination, ECF No. 114-4; *id.*, May 10, 2017 Rep. of Examination. Data extraction from the Lenovo PC revealed "internet activity purporting to depict stepfather-stepdaughter pornography and other incest, teen-anal, and similar content," Gov't's Opp'n Def.'s Mot. Suppress Tangible Evid. and Electronic Data ("Gov't's Opp'n") at 6, ECF No. 115, and user data suggesting association with defendant, *see* May 10, 2017 Rep. of Investigation at 2. "Logical extraction" of the Motorola cell phone yielded only "benign" text messages between defendant and the victim, and a more comprehensive extraction that would discover deleted text messages and images was not performed. Gov't's Opp'n at 6. The forensic investigators were unable to access content on the iPhone 6S, which belonged to the victim, beyond accessing user account information on the SIM card. *Id.*

On May 6, 2019, the government obtained a second warrant to examine and extract data from two of the devices—the victim's iPhone 6S and the Motorola cell phone—that had been seized in the 2017 search of defendant's residence. Def.'s Mot., Ex. B, 2019 Warrant, ECF No. 114-3. This 2019 warrant contained a more thorough list of information and data to be seized. *Id.*, Att. A ("2019 List of Property to be Searched") (listing the iPhone 6S and black Motorola cell phone as the devices to be searched); *id.*, Att. B ("2019 List of Property to be Seized") (describing the information and data to be seized from the two phones).[2] The 2019 warrant authorized the seizure of "fruits evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to [the charged offenses], as described in the search warrant affidavit, including, but not limited to [14 specified categories of information]." 2019 List of Property to be Seized at 1. The specified categories included records and information pertaining to the sexual abuse of A.S. as well as the devices' internet activity. *Id.* at 2–3.

This further forensic analysis of the Motorola phone and A.S.'s iPhone was accomplished with newer forensic tools and, for the iPhone, with A.S.'s passcode, and yielded substantially more incriminating evidence. Gov't's Opp'n at 6. Among the extracted files on the Motorola cell phone, DFS located sexually explicit images believed to be A.S., along with text messages between A.S. and the defendant. Gov't's Det. Mem. at 6, ECF 6; Gov't's Expert Discovery Ltr. to Counsel 2 ("Gov't's Disc. Ltr.") at 2, ECF No. 30-1. DFS was also able to perform a more thorough review of A.S.'s iPhone and located deleted text messages between A.S. and a phone

[2] The government represents that this subsequent search was conducted because "newer tools and techniques" and the availability of A.S.'s passcode for the iPhone 6S meant that more thorough "forensic examina[tion]" was possible. Gov't's Opp'n at 6.

number labeled as "Step Dad," and between A.S. and an unknown sender describing past and future intended sexual activity. Gov't's Disc. Ltr. at 2.

With this new evidence, defendant was arrested on May 10, 2019, and charged in D.C. Superior Court with one count of First Degree Sexual Abuse and four counts of Misdemeanor Sexual Abuse. Gov't's Det. Mem. at 5. On June 11, 2019, A.S. testified before a grand jury and "adopt[ed] her CAC interview and provid[ed] additional details about [defendant's] sexual assaults, threats, and production and possession of sexually explicit images of her." Gov't's Mot. *in Limine* to Admit A.S.'s Prior Statements at 3, ECF No. 24. On June 17, 2019, defendant was charged in this Court by criminal complaint, Complaint, ECF No. 1, and on September 25, 2019, he was indicted in the pending 19-count indictment on both federal and D.C. Code charges.[3]

B. Relevant Procedural History

This matter was initially set for trial on June 8, 2020, Min. Order (Nov. 18, 2019), but that schedule was disrupted by the global COVID-19 pandemic, and the trial date was pushed back, with defendant's consent, *see* Min. Order (May 14, 2020); *In re: Fourth Further Extension of Postponed Court Proceedings Due to Ongoing Exigent Circumstances Caused by COVID-19 Pandemic* ¶ 1, Standing Order No. 20-68 (BAH) (Aug. 10, 2020) (postponing "[a]ll civil and criminal . . . jury trials scheduled to commence before November 9, 2020").[4] The original

[3] Specifically, defendant is charged with one count of Production of Child Pornography, in violation of 18 U.S.C. § 2251(a), one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B), one count of Enticing a Minor, in violation of 18 U.S.C. § 2422(b), seven counts of First Degree Child Sexual Abuse with Aggravating Circumstances, in violation of 22 D.C. Code §§ 3008, 3020(a)(2), six counts of First Degree Sexual Abuse with Aggravating Circumstances, in violation of 22 D.C. Code §§ 3002(a)(1), 3020(a)(2), two counts of Second Degree Child Sexual Abuse with Aggravating Circumstances, in violation of 22 D.C. Code §§ 3009, 3020(a)(2), and one count of Misdemeanor Sexual Abuse of a Child with Aggravating Circumstances, in violation of 22 D.C. Code §§ 3010.01, 3020(a)(2). *See generally* Indictment.

[4] Available at https://www.dcd.uscourts.gov/sites/dcd/files/COVID%2019%20Standing%20Order%2020-68%20Fourth%20Further%20Extension%20of%20Postponed%20Court%20Proceedings.pdf.

pretrial conference was converted into a motions hearing on the five then-pending pretrial motions, which were argued and then resolved in *Smith*, 2020 WL 5995100. *See supra* n.1.

The trial was later rescheduled, with defendant's consent, for May 3, 2021, Min. Order (Aug. 19, 2020), with a pretrial conference scheduled for April 9, 2021, *see* Order, ECF No. 88. Three days before the pretrial conference, however, the government filed a notice describing an ongoing investigation into "alleged misconduct by employees of DFS." Notice of Filing at 2, ECF No. 108. Then, the day before the pretrial conference, the government filed another notice indicating that on April 2, 2021, the ANSI National Accreditation Board ("ANAB") informed DFS that it was "immediately suspending the laboratory's accreditation and initiating the process for withdrawal of accreditation" because the ANAB "received credible evidence that [DFS] has deliberately concealed information from the ANAB assessment team, violated accreditation requirements, engaged in misrepresentations and fraudulent behavior, and engaged in conduct that brings ANAB into disrepute." Gov't's Notice Regarding Recent Developments with D.C. DFS at 1, ECF No. 110. The DFS Digital Evidence Unit had performed the cell phone extractions and computer imaging of the key electronic devices in this case, and the government indicated that while it "ha[d] no reason to doubt DFS['s] initial data extraction and imaging," it did not want to turn the "trial into a mini-trial about DFS." *Id.* at 2. For that reason, "believ[ing] that it already ha[d] the necessary authority to do so," but exercising "an abundance of caution," the government obtained a third search warrant that day for the U.S. Attorney's Office Digital Lab to attempt to perform new extractions of the two cell phones and the Lenovo PC. *Id.*[5]

[5] Defendant's pending motion to dismiss does not challenge this third warrant, which the government indicates was supported by an affidavit that "did not reference any of the evidence obtained from the previous warrants" and yielded "the same evidence" when the devices were re-examined. Gov't's Opp'n at 7.

At the pretrial conference the next day, the parties jointly requested that the trial date be vacated in light of DFS's loss of accreditation and the need for additional discovery, and the trial date was vacated. *See* Min. Entry (Apr. 9, 2021). At a hearing the following month, defendant requested that a briefing schedule be set for an anticipated (and now-pending) motion to suppress the evidence seized pursuant to the 2017 warrant and examined by DFS, and the Court entered an order setting a schedule for briefing on that motion. Min. Order (May 10, 2021).[6] After briefing concluded, *see* Gov't's Opp'n; Def.'s Reply Supp. Mot. to Suppress, ECF No. 118, the parties were directed to submit their positions on whether a hearing on the motion to suppress was necessary. Min. Order (Jun. 21, 2021). While the government represented that no hearing was necessary given the purely legal, not factual, issues presented in defendant's motion, Gov't's Notice Regarding June 24 Hr'g, ECF No. 119, defendant contended otherwise and indicated that he intended to call Detective Jenny Alvarenga, the affiant on the 2017 and 2019 warrant affidavits, as a witness, Def.'s Mot. for Hr'g on Mot. to Suppress Tangible Evid. and Electronic Data, ECF No. 121. Defendant did not, however, explain what material factual issues were in dispute or how witness testimony would help resolve a motion to suppress that is predicated on the facial validity of warrants and the substance of the supporting affidavits, nor did defendant's supplementary filing, *see* Def.'s Response to Court's June 22, 2021 Min. Order, ECF No. 123, support the demand for a hearing. Accordingly, defendant's motion for a hearing was denied, Min. Order (Jun. 23, 2021), and defendant's motion to suppress is ripe for resolution.

[6] The government also requested that a briefing schedule be set for an anticipated motion *in limine* regarding DFS's involvement in handling the evidence, *see* Min. Entry (Apr. 9, 2021), and after the parties submitted a proposed briefing schedule, *see* Joint Status Rep. Regarding Proposed Tr. Dates and Briefing Schedule, ECF No. 113, a scheduling order was entered, *see* Scheduling Order (May 3, 2021). No motion *in limine* regarding the DFS-related evidence has been filed.

II. LEGAL STANDARD

The Fourth Amendment prohibits law enforcement from conducting "unreasonable searches and seizures," and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Defendant's challenges to the warrants described above raise issues related to the sufficiency of probable cause for the 2017 and 2019 warrants, as well as their particularity and overbreadth. The legal standard for each type of challenge is reviewed in turn.

A. Probable Cause

"[T]he task of evaluating probable cause [is] 'a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found . . . ." *United States v. Cardoza*, 713 F.3d 656, 659 (D.C. Cir. 2013) (first omission in original) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)); *see also Florida v. Harris*, 568 U.S. 237, 240 (2013) (noting that, in evaluating probable cause, courts use a "flexible, common-sense standard" (quoting *Gates*, 462 U.S. at 239)). This "objective standard," informed by "'a totality-of-the-circumstances analysis,'" *United States v. Burnett*, 827 F.3d 1108, 1114 (D.C. Cir. 2016) (quoting *United States v. Vinton*, 594 F.3d 14, 21 (D.C. Cir. 2010)) (citing *Gates*, 462 U.S. at 230–32), reflects the reality that "[p]robable cause 'turn[s] on the assessment of probabilities in particular factual contexts' and cannot be 'reduced to a neat set of legal rules,'" *District of Columbia v. Wesby*, 138 S. Ct. 577, 580 (2018) (second alteration in original) (quoting *Gates*, 462 U.S. at 232).

A showing of probable cause "is not a high bar," *id.* at 586, and, in the context of a search warrant, requires only a "fair probability that . . . evidence of a crime will be found in a particular place," *Gates*, 462 U.S. at 238. To evaluate whether this standard is met, courts focus on

whether the warrant application provides "a 'substantial basis' for concluding that 'a search would uncover evidence of wrongdoing'" by "demonstrat[ing] cause to believe that 'evidence is likely to be found at the place to be searched'" and that "'a nexus [exists] . . . between the item to be seized and criminal behavior.'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (omission in original) (first quoting *Gates*, 462 U.S. at 236; then quoting *Groh v. Ramirez*, 540 U.S. 551, 568 (2004); and then quoting *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967)). The task of a district court reviewing a magistrate's determination that a warrant is supported by probable cause "is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing]' that probable cause existed." *Gates*, 462 U.S. at 238–39 (alteration and omission in original) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). While courts must conscientiously review the sufficiency of the affidavits upon which warrants were issued, *id.* at 239, the affidavits are entitled to "a presumption of validity," *Franks*, 438 U.S. at 171, and the magistrate's "initial determination of probable cause" is entitled to "'great deference,'" *Griffith*, 867 F.3d at 1271 (quoting *Gates*, 462 U.S. at 236).

B. Particularity and Overbreadth

In addition to probable cause, the Fourth Amendment limits searches by law enforcement to "the specific areas and things for which there is probable cause to search," and requires that a search "be carefully tailored to its justifications" and "not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (footnote omitted). Thus, a search warrant must "particularly describ[e] the place to be searched[] and the person or things to be seized." U.S. CONST. amend. IV; *see also Garrison*, 480 U.S. at 84; *Griffith*, 867 F.3d at 1275; *Jones v. Kirchner*, 835 F.3d 74, 79 (D.C. Cir. 2016). This requirement "ensures that the search will be carefully tailored to its justifications," that is, to the probable cause shown. *Garrison*, 480 U.S. at 84. "Consequently, a

warrant with an 'indiscriminate sweep' is 'constitutionally intolerable,'" *Griffith*, 867 F.3d at 1275 (quoting *Stanford v. Texas*, 379 U.S. 476, 486 (1965)), and courts "will hold a warrant invalid when 'overly broad,'" *id.* (quoting *United States v. Maxwell*, 920 F.2d 1028, 1033–34 (D.C. Cir. 1990)). As the proper scope of a warrant is confined to the breadth of the probable cause that supports it, "the requirement of particularity is closely tied to the requirement of probable cause." *Id.* (internal quotation marks and citation omitted). "[A] broader sweep," however, may be permissible "when a reasonable investigation cannot produce a more particular description" prior to obtaining and executing the warrant. *Id.* at 1276 (citing *Andresen v. Maryland*, 427 U.S. 463, 480 n.10 (1976)).

III. DISCUSSION

Defendant brings a multi-pronged challenge to the search warrants that uncovered highly inculpatory evidence corroborating multiple details in A.S.'s reports of defendant's alleged almost year-long sex abuse of her. First, defendant contends that the 2017 warrant authorizing the search of his apartment and the seizure and search of his electronic devices violated the Fourth Amendment because the search of his electronic devices was without probable cause to believe that evidence of the alleged crime would be found on any particular one of the electronic devices authorized to be searched. Second, defendant argues that the warrant was insufficiently particularized and overbroad by authorizing (1) the seizure and examination of all cell phones and computers in the apartment, and (2) the extraction and review of all data from those devices limited only by reference to the criminal offense with which defendant was charged. Third, defendant contends that the 2017 warrant provided no authorization to search the data stored on the seized electronic devices and that neither this nor any of the alleged deficiencies with the 2017 warrant were cured by the 2019 warrant. Finally, defendant urges a finding that the good-faith exception to the exclusionary rule does not apply here. Based on these arguments,

defendant seeks the suppression of all material obtained pursuant to the 2017 and 2019 warrants, including the text messages, browser history, and sexual images of A.S. that the government plans to admit at trial.

Each of these arguments is without merit for the reasons explained below.[7]

A. Probable Cause

Defendant argues that the search warrants and affidavits "failed to provide 'a substantial basis for determining the existence of probable cause.'" Def.'s Mot. at 5 (quoting *Gates*, 462 U.S. at 239). More specifically, defendant contends that that the affidavits "fail to provide any specificity or basis to believe that evidence of a crime related to Mr. Smith would be located on either his cellular phone or computer" and "make only vague claims related to the general nature of electronic devices without any connection to suggest documentation of criminal activity would likely be found on a particular phone or computer in [defendant's] home." *Id.* Defendant's argument on this point is not entirely clear. He apparently concedes at least probable cause to believe that "texts and photos" from a "discre[te] time period" existed on his cell phone, *id.* at 7, but then offers the conclusory statement that the affidavit "did not even purport to establish probable cause to believe that evidence of [defendant] being involved in a crime would be found on [defendant's] cell phones or computer," *id.* at 7–8.

The issuing judge had far more than just a substantial basis to find probable cause for the search existed. The affidavit for the 2017 search warrant contained detailed allegations: (1) that defendant sexually abused A.S., as described in A.S.'s detailed statements when interviewed at

[7] The government argues that defendant's pretrial motion to suppress is untimely and that defendant has not established good cause for the delay in bringing the motion, Gov't's Opp'n at 1 n.1, since pretrial motions were originally due by March 24, 2020, *see* Scheduling Order (Nov. 18, 2019), which date was extended at the parties' joint request until April 7, 2020, *see* Min. Order (Mar. 24, 2020). Defendant does not seriously contest that the motion is untimely. *See* Def.'s Reply at 2. Nevertheless, the Court has discretion to consider the motion regardless of whether it is untimely, *United States v. Mangieri*, 694 F.2d 1270, 1283 (D.C. Cir. 1982), and will do so here, given the fundamental constitutional challenges asserted here against key inculpatory evidence against defendant.

the Children's Advocacy Center; (2) that evidence of this sexual abuse would be located on various electronic devices, including defendant's phone, defendant's computer, and A.S.'s phone, based on A.S.'s statements; and (3) that those electronic devices would be in defendant's apartment, which was the premises to be searched. *See supra* Part I.A; 2017 Aff. at 1–2. The 2017 affidavit relays A.S.'s statements that defendant sexually abused her, sent her texts describing and planning the sexual abuse, and took explicit pictures of her and requested that she send (using their phones) sexually explicit images to him. 2017 Aff. at 1–2. Law enforcement would have every reason to believe that the key cell phones—defendant's and A.S.'s—would be found on the premises, since the apartment belonged to defendant, and the affidavit indicates that defendant took A.S.'s phone when she and her mother fled the apartment for the last time. *Id.* at 1. Similarly, law enforcement had ample reason to believe that this incriminating information would be found on defendant's computer, which A.S. said he connected to the phone with which he exchanged the incriminating pictures and texts. *Id.* at 2.

The affidavit provided ample grounds to believe that defendant committed First Degree Child Sexual Abuse, *see* D.C. Code § 22-3008, and that incriminating evidence regarding that suspected offense would be found on his cell phone and his computer to which he connected his cell phone, and A.S.'s cell phone. No more is necessary to provide probable cause for the search, seizure, and extraction of data from the cell phones and personal computer in his home. *See Griffith*, 867 F.3d at 1273 (to justify the search for and seizure of a cell phone, "police needed reason to think not only that [the defendant] possessed a phone, but also that the device would be located in the home and would contain incriminating evidence about his suspected offense"). Moreover, as described in detail below, the issuing judge had a reasonable basis to conclude that evidence would be found across defendant's various electronic devices.

B. Particularity and Overbreadth

The gravamen of defendant's arguments lies with the scope—i.e., breadth and particularity—of the 2017 warrant. The warrant authorized the seizure of "all electronic data . . . and any items or materials relating to the offense of First Degree Child Sexual Abuse." 2017 Warrant. While defendant concedes, as already noted, that the affidavit could have provided probable cause to search a specific phone for specific text messages and images over a limited time period, defendant argues that the authorization to search "all data" of the electronic devices for evidence of child sexual abuse went too far. Def.'s Mot. at 8. Defendant argues that the warrant was overbroad and insufficiently particular both because it (1) authorized law enforcement to seize *all* of the cell phones and other electronic devices in defendant's apartment rather than only those described in the affidavit, *id.* at 4, 7, and (2) authorized law enforcement to seize all data on the devices that was evidence of First Degree Sexual Abuse, rather than limiting the objects of the search and seizure to particular file types or kinds of data relevant to the specific evidence described in the affidavit and limited to a certain time period, *id.* at 8. Each objection is addressed in turn.

1. *Devices*

Defendant argues that the warrant was insufficiently specific because the affidavit failed to describe with particularity the specific cell phone defendant allegedly used to text with and take pictures of A.S., or overbroad because the warrant was not limited to that single device. *See* Def.'s Mot. at 4 ("The government did not then and does not now have probable cause for a black Motorola cellular phone."); *see also id.* at 7–8. Defendant notes that the phone used by defendant was later "identified as an iPhone 6+," *id.* at 4, and the affidavit does not specify the type of phone defendant used. This argument is specious. Defendant presents no reason to believe that law enforcement, at the time of the search, could specifically identify the cell phone

in question, and presents no authority that a warrant must provide sufficient detail to identify precisely the phone belonging to an individual that was used for a given purpose. *See Griffith*, 867 F.3d at 1276 (observing that there "may be circumstances in which police have probable cause to seize a phone, yet still lack specific information about the phone's make or model"). Rather, where agents could not have known which device a defendant used to engage in the conduct relevant to the search, courts have upheld warrants broadly authorizing the seizure of "[a]ny computers, cell phones, and/or electronic media that could have been used as a means to commit" described offenses." *United States v. Loera*, 59 F. Supp. 3d 1089, 1151–52 (D.N.M. 2014); *see also United States v. Manafort*, 314 F. Supp. 3d 258, 265 (D.D.C. 2018) (describing and relying upon *Loera*). The affidavit plainly provided probable cause to believe that one or more of defendant's cell phones would contain evidence of the offense and, consequently, the warrant was not overbroad simply because it did not particularly describe the phone with which defendant sent the texts or took the photos.

Next, the affidavit states that A.S. "observed the suspect connecting his cellular phone to a computer located in his bedroom," 2017 Aff. at 2, and the affiant indicated, based on her experience investigating child sex crimes, that individuals who "participat[e] in the sexual exploitation of children" store child pornography both on their cell phones and on personal computers, *id.* at 3. "[I]n a case involving possible evidence of child pornography or sexual exploitation of a child, the probable cause inquiry 'must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology.'" *United States v. Reichling*, 781 F.3d 883, 887 (7th Cir. 2015) (quoting *United States v. Carroll*, 750 F.3d 700, 704 (7th Cir. 2014)). As the government notes, there is ample evidence—given the evidence described in the affidavit, the nature of the alleged offense, and the behavior of sex offenders—

providing reason to believe that evidence of defendant's criminal conduct would be found on other electronic devices in the apartment capable of storage. *See* Gov't's Opp'n at 11–12. The judge issuing the warrant could certainly make the inference from the affiant's statements about computer and cell phone use, A.S.'s observations about defendant's connection of his phone with his computer, and the common-sense notion that files may be transferred or synced between electronic devices, to conclude that other electronic devices in defendant's apartment could contain the text messages and images described in the affidavit, or other digital evidence of sexual abuse.

Moreover, there was reason to believe that other devices in the residence—even if they did not belong to defendant—would contain evidence of the offense. *Cf. Griffith*, 867 F.3d at 1276 (finding a search warrant overbroad where it "failed to establish probable cause to suspect that any cell phones or other electronic devices belonging to [defendant] and containing incriminating information would be found in the apartment"). The affidavit does not suggest that anyone else lived in the residence, and while defendant took both A.S.'s and her mother's phones when they left the apartment after the domestic violence incident, *see supra* Part I.A, both phones could have held evidence relevant to the offense. Based on A.S.'s statements repeated in the affidavit, her phone would likely contain the text messages and images exchanged with defendant. *See* Gov't's Opp'n at 11–12 & n.2.Her mother's phone could contain location or other data corroborating A.S.'s statement that defendant abused her while her mother was hospitalized. *See id.*

2. *Scope of Data Seizure*

Defendant also argues that the warrant was insufficiently particular in describing as the object of the search "any items or materials relating to the offense of First Degree Child Sexual Abuse" and overly broad in authorizing the extraction of "all electronic data" stored in the

electronic devices. *See* Def.'s Mot. at 8. Defendant essentially argues that the only evidence for which law enforcement had probable cause to search were the text messages and images described in the affidavit, and that the warrant was invalid insofar as it permitted the search of data files outside of defendant's text messages and images during a specific time period, even though the search was cabined to evidence of First Degree Child Sexual Abuse. The government responds, relying largely on *United States v. Burke*, 633 F.3d 984 (10th Cir. 2011), that the warrant was sufficiently particular because it was confined to evidence of a "narrowly defined statute that sufficiently limits the scope of the search." Gov't's Opp'n at 16 (internal quotation marks omitted). The government has the better argument, though the 2017 warrant could have provided more examples—as the 2019 follow-up warrant did—of specific kinds of evidence that might constitute evidence related to the criminal offense.

A warrant authorizing the search of electronic data is sufficiently particular if its scope is limited to evidence pertaining to a specific crime. *United States v. Bishop*, 910 F.3d 335, 337 (7th Cir. 2018) ("It is enough . . . if the warrant cabins the things being looked for by stating what crime is under investigation."); *accord United States v. Castro*, 881 F.3d 961, 965 (6th Cir. 2018) ("A warrant that empowers police to search for something satisfies the particularity requirement if its text constrains the search to evidence of a specific crime."); *Burke*, 633 F.3d at 992 (holding that a warrant authorizing the search and seizure of "Any and all types of media storage related to the storage of information of computer files" which were "contraband, evidence, fruits, or instrumentalities of [the charge of sexual exploitation of a child]" was sufficiently particular); *see also Andresen v. Maryland*, 427 U.S. 463, 479–80 (1976) (upholding a warrant authorizing a search for "other fruits, instrumentalities and evidence of crime at this

(time) unknown" where "crime" was interpreted to refer to the specific offense described in the warrant).

The 2017 warrant was not fatally lacking in particularity. The nature of the offense here, First Degree Child Sexual Abuse, sufficiently limited the scope of the search. Investigators knew based on the offense that they were supposed to be searching for a narrowly defined category of evidence, such as photographs, communications, online activities, and user-attribution. In *Andresen v. Maryland*, the Supreme Court upheld a warrant that provided for the relatively broad search for "fruits, instrumentalities and evidence of [a] crime" found *anywhere* in the defendant's files, in addition to a list of "particularly described documents." 427 U.S. at 479. The warrant at issue here, which approved the seizure of any evidence relating to first degree sexual abuse on any of defendant's electronic devices, is similar to that at issue in *Andresen*.[8]

Defendant suggests that *Riley v. California*, 573 U.S. 373 (2014), requires that the breadth of a warrant to search a cell phone be narrowly tailored to specific categories of data, *see* Def.'s Mot. at 4, 8–9, but *Riley* said nothing of the sort. *Riley* pertained to *warrantless* searches. 573 U.S. at 393–94 (declining to extend the search-incident-to-arrest doctrine to allow law enforcement to conduct warrantless searches of modern cell phones). Thus, *Riley* is irrelevant here, where law enforcement obtained a warrant to search defendant's electronic devices and seize data relevant to a criminal offense. *See, e.g.*, *United States v. Henry*, 827 F.3d 16, 28 (1st Cir. 2016) (finding "*Riley*'s concerns about the warrantless search of digital data stored within a

[8] Federal courts of appeals have determined that similarly broad warrants authorizing the seizure of digital information were not insufficiently particular or overbroad. *See Bishop*, 910 F.3d at 337; *Castro*, 881 F.3d at 965; *Burke*, 633 F.3d at 992. The warrants in these cases were slightly more particular than the 2017 warrant, in that they listed some examples of records or information to be seized before providing more general authorization to seize any evidence of the listed crime, but this distinction does not mean that the 2017 warrant was invalid. The scopes of the authorized searches and seizures are, ultimately, the same insofar as they are limited by the named crimes.

smart phone are not implicated . . . because by the time the phones were searched, a warrant had been obtained" and "thus . . . the officers did exactly what the Supreme Court suggested they do: seize the phones to prevent destruction of evidence but obtain a warrant before searching the phones"). Furthermore, nothing in *Riley* provides a heightened particularity requirement for searches of cell phones. *See Bishop*, 910 F.3d at 337 (approving of a search warrant that "permit[ted] the search of every document on the cell phone, which (like a computer) serves the same function as the filing cabinets in Andresen's office" (citing *Riley*, 573 U.S. at 393–94)); *United States v. Blackwell*, 636 F. App'x 668, 672-73 (6th Cir. 2016) (affirming denial of suppression motion where "police obtained a warrant before they searched [the defendant's] cell phones and SIM cards," explaining *Riley* "did not create a standard of higher specificity for such warrants or a heightened showing of probable cause" to search cell phones).

Similarly, the warrant was not overbroad or insufficiently particular by not being restricted to specific file types. "Federal courts . . . have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity such that a broad, expansive search of the computer may be required." *United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015) (internal quotation marks, citations, and alterations omitted); *accord United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *United States v. Mann*, 592 F.3d 779, 782 (7th Cir. 2010). This principle applies with full force here. The affidavit provided ample reason to believe that evidence of the sexual abuse offense existed on defendant's electronic devices, but law enforcement could not know for certain on which or where on the devices that evidence would be found.

Nor was the warrant invalid due to the absence of date limitations for the evidence to be searched. The government contends—and defendant does not contest—that "not all categories of data typically include dates" and that "[d]eleted files . . . typically have no date associated with when they were deleted or when the original item was entered into the phone." Gov't's Opp'n at 18. While the sexual abuse described in the affidavit allegedly occurred between May 2016 and April 2017, at the latest, the warrant was not required to limit the object of the search to files generated during that time period if doing so would exclude relevant evidence. "Warrants need not contain specific time limits, when 'dates of specific documents' relevant to the offenses at issue 'could not have been known to the Government,' or when 'evidence that date[s] from outside of the time period' described in a warrant affidavit 'may be relevant to the activity within the time period.'" *United States v. Manafort*, 313 F. Supp. 3d 213, 235 (D.D.C. 2018) (first quoting *United States v. Shilling*, 826 F.2d 1365, 1369 (4th Cir. 1987) (per curiam) (overruled on other grounds); and then quoting *United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006)).

Defendant's arguments to the contrary rely on cases that are not only nonbinding but lie outside of the Article III courts, and are unavailing. First, defendant relies on *Burns v. United States*, 235 A.3d 758 (D.C. 2020), for the proposition that the warrant "must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established . . . ." Def.'s Mot. at 5 (quoting *Burns*, 235 A.3d at 773). Not only is this understanding of the warrant requirement nonbinding on this Court and contrary to substantial federal caselaw, *see e.g.*, *Bishop*, 910 F.3d at 337; *Castro*, 881 F.3d at 965, but *Burns* articulated this proposition without citation to any authority beyond *Riley*. As described above, *Riley*

addressed only *warrantless* searches and said nothing about the appropriate scope of the search of a cell phone pursuant to a warrant.

Moreover, *Burns* is distinguishable on its facts. In that case, the court concluded that the warrant authorizing the government to search the defendant's phones for "evidence" of the relevant murder was insufficiently particular because the affidavit only established that one of defendant's phones would contain three pieces of evidence relating to the murder: text messages, records of a phone call, and GPS data showing the location of the phone on the night of the murder. *Id.* at 777. There was no reason to believe that evidence tying the defendant to the murder would be pervasive throughout the phones, and the defendant in that case was not even a suspect at the time his phones were searched, "ma[king] the existence of any nexus between the great majority of the data on the phones and the crime under investigation even more unlikely." *Id.* at 779. Broad offense-based searches may be excessive in murder investigations in which the cell phone is not used in carrying out the offense, but well-within Fourth Amendment bounds in the case of child sexual abuse, where the cell phone may be integral to the offense and the kinds of evidence and contraband likely to be stored on the phone are varied and well-known to law enforcement. *See Burke*, 633 F.3d at 992. Notably, the D.C. Court of Appeals took pains to make this very point and distinguished *Burns* from other cases in which "affidavits submitted in support of the warrants made robust showings of probable cause for a range of relevant evidence likely to be contained within the phones' data, without a way of knowing in advance precisely where within that data the evidence would be found." *Burns*, 235 A.3d at 776 (citing *Bishop*, 910 F.3d at 337; *Bass*, 785 F.3d at 1049). This case is likewise distinguishable from *Burns*.

Second, defendant relies on a U.S. Army Court of Criminal Appeals case, *Morales v. United States*, 77 M.J. 567 (A. Ct. Crim. App. 2017). In that case, the court held that a search

warrant authorizing the search of the defendant's phone for depictions of the sexual assault victim was overbroad because the supporting affidavit only referenced relevant text messages between the defendant and the victim, and provided no reason to believe that the defendant had taken photos or videos of the victim. *Id.* at 574–75. This case is nonbinding, appears to be in tension with federal appellate courts' decisions in *Andresen, Bishop* and *Burke*, and is also distinguishable insofar as the affidavit in this case sets forth probable cause to search for multiple file types and to believe that data may have been transmitted between devices or transferred to other individuals, and that the cell phone was used in furtherance of the sexual abuse. As both *Bishop* and *Burke* persuasively hold, a warrant may authorize the search of electronic devices for file types that go beyond those expressly referenced in the supporting affidavit, no matter the holding in *Morales*.

This case is also distinguishable from *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), which defendant does not raise but features a warrant with similar language to the one at issue here. In that case, law enforcement obtained a warrant to search the apartment in which the defendant lived with his girlfriend and seize "all electronic devices" as evidence of the defendant's involvement with a homicide committed over a year earlier. *Id.* at 1270. The D.C. Circuit held that the warrant lacked probable cause and was overbroad because the government was authorized to search for a cell phone owned by the defendant, but the affidavit supporting the warrant "provided virtually no reason to suspect that" the defendant, who had been incarcerated for much of the year preceding execution of the warrant, "in fact owned a cell phone, let alone that any phone belonging to him and containing incriminating information would be found in the residence." *Id.* at 1271. Moreover, there was no particular reason to believe that any phone defendant did possess would contain evidence of the crime, beyond the

affiant's assertion that gang members frequently maintain contact with each other and share information using cell phones. *Id.* at 1274. Here, by contrast, law enforcement (1) knew that defendant owned a phone; (2) knew that he had used the phone to engage in in the relevant offense; and (3) knew based on experience that information relevant to the offense might be spread or shared across different devices. *See supra* Part III.A; *see also United States v. Wagner*, 951 F.3d 1232, 1248 n.14 (10th Cir. 2020) (distinguishing *Griffith* in upholding a warrant authorizing the "seizure of any computer located at the residence regardless of ownership" in a child pornography case).

* * *

The 2017 warrant provided probable cause to search the electronic devices at defendant's home for evidence of First Degree Child Sexual Abuse. The warrant was sufficiently particular and not overbroad in permitting law enforcement to search all of the data on the seized electronic devices for evidence of that crime. Defendant's arguments to the contrary are without merit.

C. Extraction Authorization, the 2019 Follow-Up Warrant, and Unreasonable Delay

Defendant also argues that the initial 2017 search warrant lacked authorization to extract data from the electronic devices seized in the April 2017 search, observing that prior to the extractions carried out by the DFS Digital Evidence Unit, "the government never applied for an additional search warrant to extract electronic data from the fifteen seized devices." Def.'s Mot. at 3; *see also id.* at 15. Obtaining another search warrant was unnecessary, however, because the 2017 search warrant itself explicitly authorized "the extraction of all electronic data" on the electronic devices. 2017 Warrant.

Defendant appears to rely on *Riley* for the proposition that the government needed *an additional* warrant to extract data from the phones. *See* Def.'s Mot. at 4. *Riley* is inapposite. In

that case, as already noted, the Supreme Court held that after the lawful seizure of a cell phone during a search incident to arrest, law enforcement would need to obtain a warrant before searching the cell phone. *Riley*, 573 U.S. at 401 (holding that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest"). Here, of course, law enforcement had already obtained a warrant. The warrant authorized the (1) search of defendant's apartment, (2) the seizure of various kinds of electronic devices that might contain data, and (3) the extraction of all data on those devices. 2017 Warrant. A second warrant was not required to extract and seize the data or information contained in the electronic devices "relating to the offense of First Degree Child Sexual Abuse." As the Seventh Circuit pointedly explained in addressing a similar argument:

> [B]y explicitly authorizing the police to seize the electronic devices found in [defendant's] apartment, the warrant implicitly authorized them to search those devices as well. . . . After all, the whole point of a search warrant is to authorize police to *search* for evidence of a crime. And it seems inescapable that if there's probable cause to seize an object because it might contain evidence of a crime, then there's also probable cause to search the object for the evidence it might contain. Why, then, would the issuing judge order the police to seize an item—such as a computer, a phone, or even a safe (all listed in the warrant)—only to have them reapply for an essentially identical warrant to search the item seized? Why, when the same probable cause that justified the seizure also justifies the search?
>
> We think it generally makes more sense to read a search warrant's command to seize an electronic device as including a concomitant directive to search that device's digital contents.

United States v. Fifer, 863 F.3d 759, 766 (7th Cir. 2017). The 2017 warrant went a step further, not just authorizing the seizure of the electronic devices, but also authorizing "the extraction of all electronic data stored inside th[e devices.] *See* 2017 Warrant.

Even if the 2017 warrant were insufficiently particular with respect to the authorization to extract all data from the devices, the 2019 warrant would have cured any deficiencies and supported the seizure of data from the iPhone 6S and Motorola cell phone that were the subjects

of the warrant. *See* 2019 List of Property to be Searched. The 2019 warrant was still grounded to the sexual abuse charges and authorized the seizure of evidence of the sex abuse offenses "in whatever form and however stored . . . including, but not limited to" the enumerated categories of data. 2019 List of Property to be Seized. Unlike the 2017 warrant, however, the 2019 warrant provided a detailed list of examples of data or information to be seized. *Id.* at 1–3. Defendant implies that the 2019 warrant application relied on the 2017 extraction for probable cause, noting that the latter warrant "specifically mentions the text messages and the extractions performed by DFS." Def.'s Reply at 3. The warrant mentions only the *fact* of the earlier extractions, not the content of the extractions, so there is no reason to believe that the earlier extraction played any role in providing the probable cause for the 2019 seizure such that the data seized from the phones in the second search would be fruits of the first extractions that defendant argues were unconstitutional.[9]

D. The Good-Faith Exception

"When police obtain evidence by way of an unlawful search, the exclusionary rule may require exclusion of that evidence in some circumstances." *United States v. Glover*, 681 F.3d 411, 418 (D.C. Cir. 2012). Suppression of evidence is, however, a "last resort" meant to deter

[9] Defendant also argues that even if the 2019 warrant were valid, the government's two-year delay in obtaining it was unreasonable. Def.'s Mot. at 15. This argument is unconvincing. First, the 2017 warrant was valid and authorized the seizure of the phones and their data, *see supra* Part III.A–B, so no follow-up warrant was necessary. Second, even if the 2017 warrant were overbroad or in some way deficient as to the cell phones, it was certainly valid insofar as it authorized the seizure of the cell phones. Defendant presents no reason to believe that the delay was unreasonable given that the government believed the items to contain evidence of a crime, and defendant presents no authority for the proposition that the delayed search of validly seized property may be unreasonable where the defendant, as here, never asked for return of the property. Indeed, the Supreme Court has held to the contrary. *See United States v. Johns*, 469 U.S. 478, 487 (1985) (holding that defendants who "never sought return of the property" had "not even alleged, much less proved, that the delay in the search . . . adversely affected legitimate interests protected by the Fourth Amendment").

Defendant also argues in a conclusory footnote that the 2019 warrant also lacked probable cause and particularity, and was overbroad. Def.'s Mot. at 4 n.4. This argument is wholly without merit. The 2019 warrant was accompanied by a similar but even more detailed affidavit establishing probable cause, *see* Def.'s Mot., Ex. B, Aff. of Jenny Alvarenga Supp. Appl. Search Warrant ("2019 Aff.), ECF No. 114-3, and was somewhat more particular than the 2017 warrant, *see supra* Part I.A.

future Fourth Amendment violations by law enforcement. *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Recognizing that suppression "generates 'substantial social costs,' which sometimes include setting the guilty free and the dangerous at large," *id.* at 591 (quoting *United States v. Leon*, 468 U.S. 897, 907 (1984)), the Supreme Court has cautioned that the exclusionary rule should be limited to cases in which "the deterrent value of exclusion is strong and tends to outweigh the resulting costs," *Davis v. United States*, 564 U.S. 229, 238 (2011).

Under the logic of the good-faith exception, when a seemingly valid search warrant that is ultimately found to be unlawful purports to authorize a search, the "exclusionary rule has limited force." *Glover*, 681 F.3d at 418. Thus, "'evidence seized in reasonable, good-faith reliance on a search warrant' need not be excluded even if the warrant turns out to have been unsupported by probable cause" or otherwise invalid. *Griffith*, 867 F.3d at 1278 (quoting *Leon*, 468 U.S. at 905). This application of the good-faith exception to the exclusionary rule reflects the policies behind the suppression remedy, which "was adopted to deter unlawful searches by police, not to punish the errors of magistrates and judges." *Massachusetts v. Sheppard*, 468 U.S. 981, 990 (1984) (quoting *Gates*, 462 U.S. at 263 (White, J., concurring in judgment)).

The good-faith exception does not apply, however, if a warrant is "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923 (internal quotation marks and citation omitted). Similarly, "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* In contrast, when "the police act with an objectively reasonable good-faith belief that their conduct is lawful, . . . the deterrence rationale loses much of its force, and exclusion cannot pay it way." *Davis*, 564 U.S. at 238 (internal quotation marks and citations omitted). In such cases,

a good-faith exception, first set forth in *United States v. Leon*, 468 U.S. 897 (1984), applies and exclusion is not warranted.

Here, even if it were deficient in some way, the 2017 warrant would not be so facially deficient as to warrant suppression nor was the affidavit lacking indicia of probable cause. First, as to the facial validity of the warrant, the warrant described the premises to be searched, the kinds of devices from which data was to be extracted, and indicated that only evidence of First Degree Child Sexual Abuse was to be seized. 2017 Warrant. Defendant argues that a reasonable officer would have identified the warrant as invalidly overbroad by allegedly granting law enforcement "unbridled discretion to search for and seize whatever they wished," Def.'s Mot. at 14, but it did no such thing. The limitation to evidence of the specified offense and for electronic devices specifically inside defendant's home means that the warrant, even if overbroad or lacking particularly, would not be so facially invalid as to render a reasonable officer's reliance on it unreasonable. *See e.g.*, *Bishop*, 910 F.3d at 337–38.

Second, the affidavit was not lacking in indicia of probable cause. The affidavit articulated specific facts detailing the nature of criminal activity and describing the relationship between A.S. and the defendant, and their connection to the defendant's apartment, the reasonable basis for believing electronic devices, including defendant's phone and defendant's computer, would hold evidence of the criminal activity under investigation. 2017 Aff. at 1–2. It described how the defendant used his phone to further the alleged sexual abuse and indicated various types of evidence likely to found on defendant's electronic devices, including text messages, the sexual photos taken of A.S., and potential internet activity related to transmission of the photos. *Id.* Defendant asserts that the affidavit "lacked all factual support for a search of data such as text messages, Internet activity, photographs, and communications with persons

other than the complainant." Def.'s Mot. at 13. This assertion is just wrong. As described above, the affidavit *did* provide factual support for a broader search of the cell phone, and of defendant's other electronic devices. Defendant's argument boils down to seeking a legal conclusion that the government has probable cause to search for only the precise incriminating files about which it has knowledge and information. Probable cause does not require knowledge to a near-certainty, however, and defendant presents no authority for the proposition that, having probable cause to believe that a defendant committed a crime as well as probable cause to believe that various kinds of evidence will be present on a phone or other electronic device, the government may not conduct a fairly broad search of that device closely cabined to evidence of that crime.

IV. CONCLUSION

The 2017 warrant, like the 2019 warrant, was not constitutionally deficient in any of the ways posited by defendant and was certainly not so deficient as to fall outside the good-faith exception to the exclusionary rule. Accordingly, defendant's motion to suppress evidence seized pursuant to the 2017 warrant is denied.

An appropriate Order accompanies this Memorandum Opinion.

Date: July 15, 2021

BERYL A. HOWELL
Chief Judge