

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

v.

KRISTOPHER KNEUBUHLER,

Defendant.

CRIMINAL ACTION FILE
NO. 1:23-CR-00047-MHC-JEM

UNITED STATES MAGISTRATE JUDGE'S
NON-FINAL REPORT AND RECOMMENDATION

Pending before the Court is Defendant's Motion to Suppress the Search of 300 Anchorage Pl., Roswell, Georgia 30076. (Doc. 31.) For the following reasons, the Court **RECOMMENDS** that Defendant's motion, (Doc. 31), be **DENIED**.

I. INTRODUCTION

On December 28, 2022, United States Magistrate Judge Justin S. Anand signed a warrant authorizing the search of 300 Anchorage Place, Roswell, Georgia 30076 ("Defendant's home" or Defendant's "home address") for items related to violations of 18 U.S.C. § 2252(a)(2). (Doc. 31-2 at 1.) Section 2252(a)(2) prohibits a person from knowingly receiving, distributing, or reproducing for distribution any visual depiction of a minor engaging in sexually explicit conduct (referred to as child sexual abuse material or "CSAM") using the mails or any means of interstate or foreign commerce. 18 U.S.C. § 2252(a)(2). To obtain the warrant, Special Agent ("SA") Kasey Crump of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") submitted an

affidavit which included, *inter alia*, information about her training and experience in investigating federal criminal violations related to cybercrime and child pornography. (Doc. 31-3 ¶ 2.) Based on her training and experience, SA Crump provided information about individuals with sexual interest in children, including that they “store [CSAM] in different places, [such as] their home, their office, their car, and other areas under their control.” (*Id.* ¶ 16.) She provided information about the Tor network, which facilitates anonymous communication on the dark web by concealing a user’s Internet Protocol (“IP”) address. (*Id.* ¶ 17.) To access the Tor network, a user must install Tor software. (*Id.*) A web address on the Tor network ends in “.onion,” (*id.* ¶ 18), rather than, for example, “.com.” She also provided information about the use of cryptocurrency, such as Bitcoin, which is the primary means of payment for illegal goods and services on the dark web. (*Id.* ¶ 19.d.) It is generated and controlled through computer software operating on a decentralized peer-to-peer network. (*Id.* ¶ 19.b.) She explained that individuals using Bitcoin store their currency in digital wallets, which are identified by unique electronic public addresses. (*Id.*) Cryptocurrency transactions can be performed on any device that can access the internet. (*Id.* ¶ 19.c.) All verified and confirmed cryptocurrency transactions, as well as the public addresses of those engaging in such transactions, are recorded in a public ledger, though the true identities of the individuals behind those transactions and public addresses are not. (*Id.*) If, however, an individual is linked to a public address, it may be possible to determine what transactions were conducted by that individual. (*Id.*)

SA Crump also provided certain facts for the purpose of establishing probable cause for the search of Defendant's home. (*Id.* ¶¶ 20-31.) On June 16, 2022, the Internet Watch Foundation informed Coinbase, a cryptocurrency exchange, that a particular site on the dark web with a web address ending in ".onion" was selling access to CSAM in exchange for Bitcoin via a particular Bitcoin address. (*Id.* ¶ 22.) This site contained multiple CSAM images and videos and advertised that a potential customer must send \$89.99 worth of Bitcoin to the Bitcoin address to get full access to the site's entire CSAM collection for three months. (*Id.* ¶ 27.) Coinbase investigated the Bitcoin address, identified an account that had sent funds to that Bitcoin address on April 16, 2022, and relayed its findings to HSI, which then subpoenaed Coinbase for additional information about that account. (*Id.* ¶¶ 20-21, 23-24.) Coinbase provided HSI with subscriber and account information, which included Defendant's home address, a picture of Defendant's Georgia driver's license that listed that same address, and the email address kris@harmonic-homes.com. (*Id.* ¶ 24.) SA Crump searched Defendant's Coinbase transaction history and found the April 16, 2022, transaction to the CSAM Bitcoin address. (*Id.* ¶ 25.) SA Crump researched the email address provided by Coinbase and discovered from the State of Georgia's corporation website that Harmonic Homes, LLC is a company registered to Defendant at his home address. (*Id.* ¶ 28.) She also discovered that Defendant was receiving international packages to a storage unit, so she obtained the unit rental agreement which listed Defendant as the customer as well as his home address and the Harmonic Homes email address. (*Id.* ¶ 29.) She discovered from the

Fulton County Board of Assessors website that Defendant purchased his home in 2017 and currently owns it. (*Id.* ¶ 30.) HSI discovered from Fulton County Water and Sewer that the water and sewer services for Defendant's home are in his name. (*Id.*) SA Crump also surveilled Defendant's home and on multiple occasions observed two vehicles registered to Defendant's wife. (*Id.* ¶ 31.) In December 2022, SA Crump observed Defendant's wife and one of his two children enter the home from one of those vehicles. (*Id.*) SA Crump also observed multiple pictures of Defendant with his wife and children on social media. (*Id.*)

Attached to SA Crump's affidavit, and incorporated into the warrant, was an "Attachment B." (Doc. 31-3 at 19-22; Doc. 31-2 at 4-7.) Paragraph 1 of Attachment B listed the items to be searched for within and seized from Defendant's home:

Computer(s) and electronic mobile devices and electronic storage media . . . that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

(Doc. 31-2 ¶ 1.)

Paragraph 2 of Attachment B limited the search of these items:

- "Any and all computer software," (*id.* ¶ 2.a.);
- "Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of CSAM, (*id.* ¶ 2.b.);

- “In any format and medium, all originals, computer or electronic mobile device files, copies, and negatives of [CSAM,]” (*id.* ¶ 2.c.);
- “Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or electronic mobile device or by other means for the purpose of distributing or receiving [CSAM,]” (*id.* ¶ 2.d.);
- “Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting . . . [CSAM,]” (*id.* ¶ 2.e.);
- “Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of [CSAM,]” (*id.* ¶ 2.f.);
- “Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about [CSAM] or the existence of sites on the Internet that contain [CSAM] or cater to those with a sexual interest in children[,]” (*id.* ¶ 2.g.);
- “Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible [CSAM] to members[,]” (*id.* ¶ 2.h.);
- “Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files)

that establishes usage of the internet service provider at the subject premises[,]" (*id.* ¶ 2.i.);

- "Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer or electronic mobile device storage[,]" (*id.* ¶ 2.j.);
- "Any and all cameras, film, video cameras, videos, or other photographic equipment used to depict [CSAM,]" (*id.* ¶ 2.k.);
- "Any and all visual depictions of minors, in any explicit sexual conduct, or other materials related to an interest in children, which could fuel deviant sexual fantasies involving minors[,]" (*id.* ¶ 2.l.);
- "Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission . . . [of CSAM,]" (*id.* ¶ 2.m.);
- "Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of [Defendant's home,]" (*id.* ¶ 2.n.);
- "Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors engaged in sexually explicit conduct," (*id.* ¶ 2.o.).

Paragraph 3 of Attachment B defines the terms "records" and "information" as used in paragraphs 1 and 2 to include items:

in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage . . . ; any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as . . . prints, slides, negatives, videotapes, . . . or photocopies).

(*Id.* ¶ 3.)

On January 5, 2023, SA Crump and other agents executed the warrant at Defendant's home. (Doc. 38 at 5.) As a result of the search, the agents seized 15 electronic devices. (*Id.*) During the search, Defendant spoke with agents voluntarily and stated that he accessed the dark web to download CSAM, he knew the CSAM depicted minors engaged in sexually explicit conduct, and he stored the CSAM on a removable flash drive. (*Id.*) The forensic analyses of the electronic devices revealed the presence of more than 1,000 CSAM videos and images on at least six of the seized devices. (*Id.*)

II. DISCUSSION

Defendant now seeks to suppress the evidence that resulted from HSI's execution of the search warrant, arguing that (A) SA Crump's affidavit failed to establish a probable cause nexus between his home and the alleged criminality, (B) Attachment B failed for particularity, and (C) the "good faith" exception does not apply. (Doc. 31-1 at 8-17.) The Court will address each argument in turn.

A. SA Crump's affidavit established a probable cause nexus between Defendant's home and the alleged criminality.

To establish probable cause, an affidavit "should establish a connection between the defendant and the residence to be searched [as well as] a link between the residence and any criminal activity." *United States v. Kapordelis*, 569

F.3d 1291, 1310 (11th Cir. 2009) (quoting *United States v. Martin*, 297 F.3d 1308, 1314 (11th Cir. 2002)). A magistrate judge issuing a search warrant must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *United States v. Miller*, 24 F.3d 1357, 1361 (11th Cir. 1994) (A realistic and commonsense approach encourages use of the warrant process.). Probable cause can be inferred by considering the type of crime, the nature of the items sought, the suspect’s opportunity for concealment, and normal inferences about where a criminal might hide the fruits of his crime. *See United States v. Lebowitz*, 647 F. Supp. 2d 1336, 1354 (N.D. Ga. 2009), *aff’d*, 676 F.3d 1000 (11th Cir. 2012) (citation omitted); *see also United States v. Lockett*, 674 F.2d 843, 846 (11th Cir. 1982) (“[T]he nexus between the objects to be seized and the premises searched can be established from the particular circumstances involved and need not rest on direct observation.”) (citing *United States v. Charest*, 602 F.2d 1015 (1st Cir. 1979)). A court reviewing the issuing court’s probable cause determination employs a deferential rather than *de novo* standard of review. *Massachusetts v. Upton*, 466 U.S. 727, 728, 733 (1984) (citing *Gates*, 462 U.S. at 236; *United States v. Ventresca*, 380 U.S. 102, 108 (1965)); *Miller*, 24 F.3d at 1363 (reviewing courts owe “substantial deference to an issuing magistrate’s probable cause determinations”).

Defendant argues that the affidavit failed to establish a link between his home and the target criminality; that is, the affidavit did not include facts

creating probable cause that CSAM would be inside his home. (Doc. 31-1 at 8.) Defendant points to six facts that were not alleged in the affidavit. (*Id.* at 9.) For example, the affidavit did not state that Defendant viewed the dark web site after gaining access to it, that Defendant downloaded CSAM onto a certain electronic device in his home after gaining access to the site, that Defendant was a suspected collector of CSAM, or that any IP information was associated with Defendant's Coinbase wallet or the April 2022 Bitcoin transaction. (*Id.*) However, a reviewing court looks at the information that was — rather than was not — in the affidavit. *See W. Point-Pepperell, Inc. v. Donovan*, 689 F.2d 950, 959 (11th Cir. 1982) (“[J]udicial review of the sufficiency of an affidavit for the issuance of a warrant must be strictly confined to the information brought to the magistrate’s attention.”). An omission or absence of additional information that “might have been helpful in further confirming” a defendant’s involvement in a crime is irrelevant where the affidavit sets forth an adequate factual basis for a magistrate judge to find probable cause. *United States v. Bridges*, 2008 WL 11431069, at *8 (N.D. Ga. July 1, 2008) (rejecting argument that affidavit was deficient without more information about PayPal account used to purchase access to CSAM website), *report and recommendation adopted*, 2008 WL 11431071 (N.D. Ga. Sept. 2, 2008), *aff’d*, 347 F. App’x 459 (11th Cir. 2009); *United States v. Schwinn*, 2008 WL 782520, at *4 (M.D. Fla. Mar. 21, 2008) (“The issue before the magistrate judge in deciding whether to authorize a search warrant is not what was not in the affidavit, but whether what was in the affidavit was sufficient.”), *aff’d*, 376 F. App’x 974 (11th Cir. 2010).

Upon deferential review, the Court finds that SA Crump's affidavit established probable cause to believe that evidence of receiving CSAM would be found at Defendant's home. The affidavit showed that (1) SA Crump had training on and experience with investigating federal criminal violations related to cybercrime and child pornography, (2) individuals with a sexual interest in children commonly store CSAM in their homes, (3) Defendant's Coinbase account, which was associated with his home address, was used to send Bitcoin to a dark web site that contained multiple CSAM images and videos, (4) the site advertised full access to its entire CSAM collection for three months for \$90 worth of Bitcoin, (5) Defendant owned the home, and (6) his family lived at the home. The reasonable, practical, commonsense inferences to be drawn from those facts include that Defendant visited the CSAM site, paid approximately \$90 worth of Bitcoin to gain access to its entire CSAM collection, and received access to this collection, and that evidence related to these activities was likely to be found in his home. *See, e.g., United States v. Frechette*, 583 F.3d 374, 380 (6th Cir. 2009) ("[I]f someone spends \$80 for something, it is highly likely that the person will use it—whether it is a tie, a video game, or a subscription to a pornographic web site."), *cited with approval in Schwinn*, 376 F. App'x at 979; *United States v. Byrd*, 31 F.3d 1329, 1339 (5th Cir. 1994) ("'common sense would indicate that a person who is sexually interested in children is likely to also be inclined, i.e., predisposed, to order and receive child pornography'"); *United States v. Vincent*, No. 3:21-CR-00010-TCB-RGV, 2022 WL 1401463, at *7 (N.D. Ga. May 3, 2022) (collecting cases showing that in child pornography possession cases, evidence is

likely to be found in the defendant's home, which he believes is safe, secure, and private), *report and recommendation adopted*, 2022 WL 2452301 (N.D. Ga. July 6, 2022); *United States v. Lebowitz*, 647 F. Supp. 2d 1336, 1353 (N.D. Ga. 2009) (“numerous courts have recognized the strong link between pedophilic behavior and possession of child pornography”), *aff’d*, 676 F.3d 1000 (11th Cir. 2012).

Defendant compares the affidavit in this case to the affidavit at issue in *Schwinn*, 376 F. App'x 974. In *Schwinn*, the court found that even though the affidavit “did not include an averment that Schwinn was himself a collector” of CSAM, it was nevertheless sufficient because it “included declarations about the profile of child pornography collectors . . . [as well as Schwinn's] status as a sex offender and [his] alleged pattern of purchasing brief memberships to multiple websites containing child pornography.” 376 F. App'x at 979. Defendant argues that, unlike in *Schwinn*, SA Crump's affidavit did not state that Defendant was a sex offender or that his IP address was associated with purchasing access to multiple websites flagged for CSAM. (Doc. 31-1 at 10.) However, the court in *Schwinn* did not find that the affidavit was sufficient only because it contained these facts; rather, the court found that the affidavit established probable cause because it included these facts, among others, which allowed the issuing court to infer that CSAM was likely inside the defendant's home. *See Schwinn*, 376 F. App'x at 979 (“[I]nvestigators and courts frequently rely upon an *inference* that the suspect is a collector of child pornography -- and therefore is unlikely to dispose of his images -- to establish that evidence of a crime will be present at some point in the future. . . [Here,] the magistrate was entitled to infer that

Schwinn was a collector based on other information in the affidavit[.]”)
 (emphasis added) (citing *United States v. Lemon*, 590 F.3d 612, 614-15 (8th Cir. 2010)). The Court also notes that, according to SA Crump’s affidavit, the CSAM site ended in “.onion,” indicating that it had been accessed via the Tor network, which conceals a user’s actual IP address. See *United States v. Vanbrackle*, 397 F. App’x 557, 560 (11th Cir. 2010) (“Although IP address information could have definitively shown that a computer used at Vanbrackle’s home received the images in question, [the affiant] was only obligated to provide enough facts to show a fair probability that evidence of a crime would be found at Vanbrackle’s residence.”) (internal citation omitted).

Defendant argues that three cases outside of this Circuit – *United States v. Zimmerman*, 277 F.3d 426 (3d Cir. 2002), *United States v. Doyle*, 650 F.3d 460 (4th Cir. 2011), and *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) – also support his position, (Doc. 31-1 at 11-12), but they are distinguishable. In *Zimmerman*, the court held that “there was no probable cause to search Zimmerman’s home for child pornography” because “the government concede[d] that . . . the affidavit contained no information that [he] had ever purchased or possessed child pornography.” 277 F.3d at 432. In *Doyle*, the court held that the warrant lacked probable cause to search Doyle’s home because “the only mention . . . regarding the presence of pornography was the statement that one of the alleged victims ‘disclosed to an Uncle that Doyle had shown the victim pictures of nude children’” and because of “the complete absence of any indication as to when the pictures were possessed.” 650 F.3d at 472, 474. In *Falso*, the court found no

probable cause because the affidavit relied only on the allegations that Falso's email address appeared on a list of "several possible subscribers" to a members-only child pornography site and on an 18-year-old conviction involving sexual abuse of a minor. 544 F.3d at 113-114. Here, in contrast to the affidavits at issue in *Zimmerman*, *Doyle*, and *Falso*, SA Crump specifically alleged facts showing that on April 16, 2022, Defendant purchased three months' worth of access to a CSAM site and that this transaction was confirmed by his Coinbase account records. (Doc. 31-3 at 14-16, ¶¶ 20-27.)

Defendant also argues that three Eleventh Circuit cases support his position, citing *United States v. Lovvorn*, 524 F. App'x 485 (11th Cir. 2013) (per curiam), *United States v. Carroll*, 886 F.3d 1347 (11th Cir. 2018), and *Kapordelis*, 569 F.3d at 1311. (Doc. 31-1 at 11.) Defendant contends that the holding of these cases was "that access to a known CSAM website *together with other factors[] may* establish a nexus between criminality and the home under the totality of the circumstances." (*Id.*) (emphasis in original). This is a misstatement of the holdings in these cases. In *Lovvorn*, the court held that the affidavit established a "fair probability [that] child pornography would be found on Lovvorn's computer" because it included statements from his wife about his use of the computer to possess, view, and sell CSAM, "along with [her] sworn affidavit confirming these facts[.]" 524 F. App'x at 487. In *Carroll*, the court held that the affidavit was sufficient because the "affiant . . . was specially trained in computer investigations involving crimes against children," she explained how law enforcement used a file sharing program to download CSAM files "from an IP

address traced to Carroll's internet service provider[,]” and she described the contents of the files as well as the file names, which contained an acronym commonly used to identify CSAM files. 886 F.3d at 1351-52. In *Kapordelis*, the court held that the affidavit was sufficient because “it [made] clear . . . that [Kapordelis] had the means to obtain and store . . . images and other data that he had gathered . . . or created or collected . . . on a computer located in his home and by means of access to the Internet from his home.” 569 F.3d at 1311. Likewise, as explained above, Judge Anand correctly determined that SA Crump's affidavit established probable cause to believe that evidence of receiving CSAM would be found in Defendant's home.

B. Attachment B does not fail for particularity.

The Fourth Amendment requires a search warrant to “‘particularly describe the place to be searched, and the persons or things to be seized.’” *United States v. Betancourt*, 734 F.2d 750, 754 (11th Cir. 1984) (citation omitted in original). This “requirement is aimed at preventing ‘general, exploratory rummaging in a person's belongings.’” *United States v. Wuagneux*, 683 F.2d 1343, 1348 (11th Cir. 1982) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). However, the description in the warrant need not be elaborately specific; it need only enable the searcher to reasonably ascertain and identify the things authorized to be searched for and seized. *Betancourt*, 734 F.2d at 754-55. The reviewing court determines *de novo* whether a warrant lacked the requisite particularity. *United States v. Bradley*, 644 F.3d 1213, 1258-59 (11th Cir. 2011). Here, Defendant challenges the particularity of the search warrant by arguing

that it authorized a general, overbroad search for items in his home and a general, overbroad search of the items seized from his home. (Doc. 31-1 at 13-15.) The Court addresses each in turn.

1. The warrant authorized a particularized search for items in Defendant's home.

Defendant argues that paragraph 1 of Attachment B, which lists the items to be searched for, encompassed every electronic media and electronic storage device in his home. (Doc. 31-1 at 13.) Defendant also takes issue with the fact that SA Crump's affidavit lacked any allegation about what type of device was used to commit the crime and whether any such device was located in Defendant's home. (*Id.*) Therefore, he argues, the warrant authorized a search that was "clearly overbroad" when compared to the statement of probable cause. (*Id.*) The government responds that the warrant did not permit a general search of Defendant's home because it was limited to only electronic devices and electronic storage media that could be used to distribute, possess, or depict child pornography or erotica. (Doc. 38 at 14) (citing Doc. 31-3 at 19.) The government points to *United States v. McDaniel*, in which a court in this District found that a warrant authorizing the seizure of all "computer(s) and computer systems and files and contents therein" and "computer storage media/medium including hard drives, floppy discs, hard discs, compact discs (C.D.'s), zip discs, and disc drives" that might contain evidence of a violation of Georgia's electronic child pornography statute was sufficiently particularized. (Doc. 38 at 14) (citing 2009 WL 10674310, at *3-4 (N.D. Ga. May 18, 2009)). The court noted that the

defendant's attack on the warrant's particularity "ignore[d] that the warrant specifically connects the items to be seized with the criminal conduct of 'computer pornography and child exploitation.'" *McDaniel*, 2009 WL 10674310, at *9. The government argues that paragraph 1 of Attachment B contained similar limiting language that precluded a free-ranging search. (Doc. 38 at 15.)

The Court agrees with the government. Paragraph 1 of Attachment B limited the items for which the HSI agents could search:

Computer(s) and electronic mobile devices and electronic storage media . . . that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

(Doc. 31-2 ¶ 1.) The statement of probable cause identified the criminal act underlying the search warrant application as Defendant's use of the internet to purchase access to CSAM. Therefore, the language in paragraph 1 of Attachment B specifically connected the items to be searched for and seized (i.e., electronic devices) to the alleged criminal conduct (i.e., violations of 18 U.S.C. § 2252(a)(2)). *See, e.g., McDaniel*, 2009 WL 10674310, at *9; *United States v. Carroll*, No. 3:15-CR-00012-TCB-RGV, 2015 WL 13741254, at *7 (N.D. Ga. Nov. 3, 2015) ("[T]he face of the warrant here was written with sufficient particularity because the items listed on the warrant were qualified by phrases that emphasized that the items sought were those related to child pornography. . . Indeed, law enforcement officers executing the warrant . . . could search for evidence of child pornography only in

certain specified places, such as computers[.]” (internal quotation marks, citations, and alterations omitted), *report and recommendation adopted*, No. 3:15-CR-00012-TCB, 2015 WL 8491011 (N.D. Ga. Dec. 10, 2015), *aff’d*, 886 F.3d 1347 (11th Cir. 2018); *United States v. Graham*, No. 3:13-CR-11-TCB, 2014 WL 2922388, at *3, 16 (N.D. Ga. June 27, 2014) (finding that a search warrant “authorizing a search for computer storage media and other items which may be used to receive, transmit, or store child pornography . . . described with sufficient particularity the items to be seized and limited these items to evidence relating to child pornography”); *see also United States v. Rondeau*, 626 F. Supp. 3d 403, 416 (D. Mass. 2022) (“A warrant authorizing seizure of a suspect’s home computer equipment and digital storage media . . . is not overbroad or unreasonable, as long as the probable-cause showing in the warrant application demonstrates a ‘sufficient chance of finding some needles in the computer haystack.’”) (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999)). And, as the court in *McDaniel* explained, “the ubiquitous nature of personal computer equipment and digital storage media precluded [SA Crump] from giving a more exact description of the items to be seized.” 2009 WL 10674310, at *8. Therefore, the Court finds that the warrant authorized a particularized search for evidence in Defendant’s home.

2. The warrant authorized a particularized search of the items seized from Defendant’s home.

Defendant argues that the searches of the seized items were warrantless because the face of the warrant listed only Defendant’s home as the place to be

searched and not the devices. (Doc. 31-1 at 14, n.9.) The government responds, and the Court agrees, that the affidavit and Attachment B made clear that searches of the electronic devices themselves were authorized. (Doc 38 at 13 n.6.) In the closing paragraph of the affidavit, SA Crump requested that the Court “issue a warrant . . . authorizing the seizure and search of the items described in Attachment B.” (Doc. 31-3 at 17.) Paragraph 2 of Attachment B discusses the limitations on the “search of such equipment” listed in paragraph 1. (Doc. 31-2 at 4.) Regardless, the Federal Rules of Criminal Procedure state that, unless otherwise specified, a warrant authorizing the seizure of electronic storage media or electronically stored information also authorizes a later review of the media or information. Fed. R. Crim. P. 41(e)(2)(B).

Defendant also argues that the warrant authorized a general search of the seized items because it failed to limit the searchable subject matter and it failed to limit the searches to a relevant time period. (Doc. 31-1 at 14.) As to the subject matter, Defendant argues that the references to CSAM within the various subparagraphs of paragraph 2 do not limit the searchable subject matter to CSAM-related evidence because of the “any and all” modifier at the beginning of each subparagraph and because of the “limitless definition of ‘records’ and ‘information’” in paragraph 3. (*Id.*) The government does not respond to these specific arguments; rather, the government responds that the warrant limited the agents’ search of the seized devices to specific categories of data by including specific references to “child pornography,” “the sexual exploitation of children,”

and “visual depictions of minors engaged in sexually explicit conduct” in paragraph 2. (Doc. 38 at 13-15, 19-21.)

The Court is not persuaded by Defendant’s argument that the “any and all” modifier at the beginning of each subparagraph renders the warrant unconstitutionally broad. Subparagraphs 2.b. through 2.h., 2.k. through 2.m., and 2.o. are limited by specific references to CSAM terms, (*see* Doc. 31-2 at 4-7), and they are therefore sufficiently particularized and connected to the alleged criminality. The remaining subparagraphs, 2.a., 2.i., 2.j., and 2.n., do not include references to CSAM terms. (*See id.*) Nevertheless, they limited the agents’ search of the seized evidence to other categories of data – respectively, “computer software,” (*id.* ¶ 2.a.), “usage of the internet service provider at the [home,]” (*id.* ¶ 2.i.), “online storage or other remote computer or electronic mobile device storage,” (*id.* ¶ 2.j.), and “occupancy or ownership of the [home,]” (*id.* ¶ 2.n.). Though broad, these categories are specific, related to the alleged criminality, and related to the evidence one would expect to be connected with that criminality. This is particularly true in light of SA Crump’s sworn testimony that “to access the Tor network, a user must install Tor software[,]” (Doc. 31-3 ¶ 17), cryptocurrency is “generated and controlled through computer software[,]” (*id.* ¶ 19.b.), cryptocurrency “transactions can be performed on any device that can access the internet,” (*id.* ¶ 19.c.), due to the nature of “[m]agnetic storage . . . [i]t is only with careful laboratory examination of electronic storage devices that it might be possible to recreate the evidence trail” of CSAM-related crime, (*id.*

¶ 12), and individuals with a sexual interest in children “tend to keep their images for periods exceeding several years. . . in digital formats[] . . . [and] in different places, including their home, their office, their car, and other areas under their control[,]” (*id.* ¶ 16.c.). The Court therefore concludes that the “any and all” modifier in each subparagraph did not render the warrant overbroad.¹ See *United States v. Grimmer*, 439 F.3d 1263, 1267, 1270 (10th Cir. 2006) (upholding in a child pornography case a “warrant [that] authorized, among other things, the search and seizure of ‘any and all computer hardware,’ and ‘any and all computer software.’”))

The Court also is not persuaded by Defendant’s argument that the definition of “records” and “information” is limitless and thus renders the warrant unconstitutionally broad. It is true that paragraph 3 defines these terms as including both electronic and non-electronic evidence, thereby broadening the searchable evidence beyond merely electronic devices as initially represented in paragraph 1. (See Doc. 31-2 ¶ 3.) However, “[t]he fact that [a] warrant call[s] for seizure of a broad array of items does not, in and of itself, prove that the warrant fails to meet this requirement of particularity.” *United States v. Sharp*, No. 1:14-CR-227-TCB, 2015 WL 4644348, at *10 (N.D. Ga. Aug. 4, 2015) (quoting *United States v. Sugar*, 606 F. Supp. 1134, 1151 (S.D.N.Y. 1985); citing *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents*, 307

¹ For these reasons, the Court also rejects Defendant’s contention that subparagraphs 2.a., 2.i., 2.j., and 2.n were “broad enough to subsume any type of stored information” related to his business and therefore constituted an “all records” search subject to heightened scrutiny. (Doc. 31-1 at 14-15.)

F.3d 137, 149 (3d Cir. 2002) (“Although the scope of the warrant was certainly extensive, the warrant was not general.”)). Moreover, the terms “records” and “information,” as defined by paragraph 3, are connected to specific and relevant categories of data within paragraphs 1 and 2. The term “records” is referenced in paragraphs 2.b., 2.e., 2.f., 2.g., 2.h., 2.i., 2.j., 2.m., 2.n., and 2.o. (Doc. 31-2 at 4-7.) In paragraphs 2.b., 2.e., 2.f., 2.g., 2.h., 2.m., and 2.o., “records” is modified by specific references to “child pornography” and/or “visual depictions of minors engaged in sexually explicit conduct” and/or “personal contact and any other activities with minors engaged in sexually explicit conduct[.]” (Doc. 31-2 ¶¶ 2.b., 2.e., 2.f., 2.g., 2.h., 2.m., 2.o.) In the remaining subparagraphs, “records” is modified by the phrases “establishes usage of the internet service provider at [Defendant’s home,]” (*id.* ¶ 2.i.), “that concern online storage or other remote computer or electronic mobile device storage[.]” (*id.* ¶ 2.j.), and “pertaining to occupancy or ownership of [Defendant’s home,]” (*id.* ¶ 2.n.). As previously discussed, these categories are broad but specific, related to the alleged criminality, and related to the evidence one would expect to be connected with that criminality.

The term “information” is referenced in paragraph 1 and is modified by the phrases “pertaining to a sexual interest in child pornography[.]” “pertaining to sexual activity with children[.]” and “pertaining to an interest in child pornography or child erotica.” (Doc. 31-2 ¶ 1.) That term is also referenced in paragraph 2.f. and is modified by the phrase “concerning . . . child pornography . . . or visual depictions of minors engaged in sexually explicit

conduct[.]” (*Id.* ¶ 2.f.) Again, though broad, such evidence is specific and clearly connected to the alleged criminality. “Because the warrant in this case was already sufficiently particularized based on the subject matter limitation[,] . . . the lack of an additional time period limitation in the warrant does not render the search unconstitutional.” *United States v. Capote*, No. 1:15-CR-00338-MHC-CMS, 2016 WL 11650552, at *3 (N.D. Ga. May 5, 2016), *report and recommendation adopted*, No. 1:15-CR-338-4-MHC, 2016 WL 3086412 (N.D. Ga. May 31, 2016).

C. Even if the search was unlawful, the *Leon* good faith exception would apply.

In general, evidence seized through an unlawful search must be suppressed. *United States v. Morales*, 987 F.3d 966, 972 (11th Cir. 2021) (citing *Martin*, 297 F.3d at 1312). But when the law enforcement officers “obtained and relied on a warrant from a neutral magistrate and had no reason to think that probable cause was absent despite the magistrate’s authorization[.]” the seized evidence should not be suppressed. *Id.* at 974; *United States v. Leon*, 468 U.S. 897, 925 (1984). In *Leon*, the Supreme Court noted that “searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” 468 U.S. at 922. The Supreme Court then identified four specific situations in which this good faith exception does not apply, including when the supporting affidavit is “so lacking in indicia of probable cause as to render official belief in its existence unreasonable.” *Id.* at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 610-611 (1975)).

Here, Defendant argues that this is the nature of SA Crump's affidavit. (Doc. 31-1 at 16.) Specifically, Defendant argues that the affidavit was "conclusory" because it lacked allegations that any device connected with Defendant's home had visited the dark web site, downloaded anything from the dark web site, or otherwise contained contraband images. (*Id.*) Rather, he argues, SA Crump "drew attenuated inferences from one Coinbase transaction" completed by an unidentified device, the location of which was unknown. (*Id.* at 17.) As explained above, to determine whether an affidavit lacks indicia of probable cause, the reviewing court looks to the facts included in the affidavit, not the facts that purportedly could have or should have been included but were not. *United States v. Robinson*, 336 F.3d 1293, 1296 (11th Cir. 2003) (citing *Martin*, 297 F.3d at 1313). In doing so, the reviewing court examines whether, based on the totality of the circumstances, a reasonably well-trained officer would have relied on the warrant. *United States v. Taxacher*, 902 F.2d 867, 872 (11th Cir. 1990) (citing *Leon*, 468 U.S. at 922). Here, SA Crump's affidavit established the impossibility of identifying a specific device that interacted with a dark web site using the Tor network. Otherwise, as previously discussed, SA Crump's affidavit contains, at the very least, indicia of probable cause. *See* Section II.A., *supra*. Therefore, the Court finds that the HSI agents reasonably relied on the warrant.

III. CONCLUSION

For the foregoing reasons, the Court **RECOMMENDS** that Defendant's Motion to Suppress the Search of 300 Anchorage Pl., Roswell, Georgia 30076,

(Doc. 31), be **DENIED**. Defendant has no other motions pending before me.

Accordingly, his case is **CERTIFIED READY FOR TRIAL**.

SO RECOMMENDED August 3, 2023.



J. ELIZABETH McBATH

UNITED STATES MAGISTRATE JUDGE