IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
	:	
V.	:	**CRIMINAL NUMBER 25-130**
	:	
	:	
ANIRUTH KUPPUSAMY	:	

O R D E R

AND NOW, this day of , 2026, having considered defendant Aniruth Kuppusamy's Motion to Suppress and the government's response thereto, and having conducted a suppression hearing, it is hereby **ORDERED** that the defendant's Motion is **GRANTED**.

Any and all evidence received from the Emergency Disclosure Requests, from the March 9, 2025 search of 79 Militia Hill Drive, Chesterbrook, Pennsylvania 19087 and subsequent arrest of Mr. Kuppusamy, as well as all fruits of those unconstitutional searches including the custodial statement of Mr. Kuppusamy, the statements taken from his parents, and the evidence recovered during the subsequent search of his Instagram accounts are hereby **SUPPRESSED**.

It is so **ORDERED**.

BY THE COURT:

THE HONORABLE MARY KAY COSTELLO
United States District Court Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
	:	
V.	:	**CRIMINAL NUMBER 25-130**
	:	
	:	
ANIRUTH KUPPUSAMY	:	

DEFENDANT'S MOTION TO SUPPRESS

Defendant Aniruth Kuppusamy, by and through undersigned counsel, respectfully moves this Court to suppress any and all evidence recovered: during the warrantless search of his Meta accounts conducted by the FBI on March 7 and 8, 2025; the March 9, 2025 search of 79 Militia Hill Drive, Chesterbrook, Pennsylvania as well as any evidence derivative of these searches and the fruits of this unlawful conduct including the custodial statement of Mr. Kuppusamy, the statements taken from his parents and the evidence recovered during the subsequent search of his Instagram accounts.

Mr. Kuppusamy stands charged with violations of 18 U.S.C. §2251(a)(production of child pornography); 18 U.S.C. §2252(a)(2), (b)(1)(receipt of child pornography); 18 U.S.C. §2252A(a)(5), (b)(2)(possession of child pornography) and 18 U.S.C. §2422(b)(enticement of a minor to engage in sexual activity).

Mr. Kuppusamy submits that the initial warrantless search of his Meta accounts conducted on March 7-8, 2025 as well as the March 9, 2025 search of 79 Militia Hill Drive, Chesterbrook, Pennsylvania and the search of the electronic devices seized therein were unconstitutional. Furthermore, his post arrest statement made on March 9, 2025 and the subsequent search conducted of defendant's Instagram accounts on March 19, 2025 must be suppressed as fruits of

these unconstitutional searches.

WHEREFORE, for all the reasons set forth in the accompanying Memorandum of Law, defendant Aniruth Kuppusamy respectfully requests that this Court grant his motion and order the suppression of all evidence recovered as a result of these unlawful searches, as well as any evidence derivative of the illegal seizures and searches. Mr. Kuppusamy respectfully requests an evidentiary hearing on this motion.

Respectfully submitted,

/s/ *James J. McHugh, Jr.*
JAMES J. McHUGH, JR.
Assistant Federal Defender

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
	:	
V.	:	**CRIMINAL NUMBER 25-130**
	:	
	:	
ANIRUTH KUPPUSAMY	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS

Defendant Aniruth Kuppusamy was arrested on March 9, 2025 as a result of multiple illegal searches including an illegal and warrantless search of his Meta accounts and an illegal search of his alleged residence the single family home located on Militia Hill Drive in Chesterbrook, Pennsylvania (Subject Premises) and the electronic devices seized therein. The search of the Subject Premises and the unfettered searches of the electronic devices were conducted pursuant to a warrant that was fatally defective in multiple ways.

In conducting the initial warrantless search of his Meta accounts the government violated the Stored Communications Act as well as the Fourth Amendment. The warrant for the Subject Premises did not establish probable cause that evidence of a crime would be found inside the house. The warrant was also overly broad. It permitted an unfettered search of all areas of the house, the seizure of all electronic devices (computers, cell phones, ipads, hard drives etc.) regardless of who they belonged to or who had dominion and control over the devices. The warrant also permitted the agents to copy all of the devices and thereafter conduct an unfettered search of all aspects of the electronic devices seized therein – again regardless of who they belonged to and without any temporal limitations. There were also material omissions to the affidavit.

Based on this defective warrant, nineteen FBI officers descended on this residence and searched it in its entirety. Every room was turned over and every storage space searched. The agents seized 13 different electronic devices (with no limitations on who they belonged to), copied those devices and then conducted unfettered searches of every aspect of each and every one of these devices.

As Mr. Kuppusamy will demonstrate at a hearing on this Motion, the search warrant authorizing the search of this residence was based in part on illegally seized evidence and was on its face fatally defective and it contained material omissions. Furthermore, the search of the residence and the searches of the electronic devices seized were conducted in an illegal and unconstitutional manner.

I. FACTS REGARDING THE STATUTORY AND CONSTITUTIONAL VIOLATIONS

On March 7, 2025 the FBI in Atlanta received a tip from Meta that a 17 year old female had live streamed an attempt on her life and had also talked about committing homicidal acts against her family and students at her school. That same day the FBI Atlanta received the actual data from Meta that had formed the basis of the tip. The data showed the alleged attempt on her life had occurred four months earlier in December 2024. The data also showed that an adult male in Pennsylvania was grooming the female. Specifically, the female and the male had shared messages about planning homicidal terroristic acts, mass casualty events and creating firearms to conduct these acts. As a result of this information the FBI in Atlanta made an Emergency Disclosure Request ("EDR") pursuant to the Stored Communications Act ("SCA") to Meta seeking subscriber information attached to these messages. They also notified the Philadelphia FBI of this information.

That same day (March 7, 2025) the FBI in Philadelphia were notified that the Meta accounts were allegedly referencing child sexual abuse, child abduction, murder, weapon manufacturing and threats. The FBI in Philadelphia also served an EDR on Meta pursuant to the SCA requesting all of defendants "subscriber information, linked accounts by cookies, private chat communication and distributed images, IP transactional history, geolocation information, verified device information, and any financial accounts."

The Philadelphia FBI's emergency request did not in any way limit the information sought to that "relating" to the perceived/alleged emergency. Likewise, Meta's response was not limited to information relating to the emergency. Rather, the Philadelphia FBI received and reviewed *all* of the information sought – without a warrant of any kind. The information reviewed by the Philadelphia FBI included all of the defendants' private messages with all individuals for at least a six month period. This unfettered and warrantless review by the Philadelphia FBI took place despite the fact that all of the defendant's Meta accounts – Facebook and Instagram – were marked private by the defendant when they were first opened and all of the accounts were password protected.

On March 9, 2025 FBI Special Agent Jessica Prendergast prepared search warrant applications for the Subject Premises and for the person of the defendant. *See* Exhibit A attached hereto. Agent Prendergast alleged therein that the property was the residence of the defendant. She also averred that there was probable cause to search this property for evidence of violations of 18 U.S.C. Section 2251 (production of child pornography), 18 U.S.C. Section 2252 (possession of child pornography) and 18 U.S.C. Section 875(c)(kidnapping) ("Subject Offenses").

The application for the property sought authorization to search the entirety of the Subject Premises as well as the entirety of any computers and electronic devices found on the premises as well as any electronic or cloud storage connected to said devices. Her affidavit of probable cause included and relied upon extensive information from the defendant's Meta accounts that had been seized without a warrant pursuant to the EDR despite the fact that the information was not related to the emergency.

While the search warrant application was being prepared, federal and local law enforcement personnel went to the Subject Premises. They staged outside the subject premises at 6:35 pm and knocked on the front door. Defendant Kuppusamy answered and was immediately taken into custody. The agents then entered the house at 6:40 pm.

While they were staging outside the Subject Premises, Special Agent Prendergast submitted the two search warrant applications via email to Magistrate Judge Lynne E. Sitarski. At 6:42:18 pm Judge Sitarski signed the Application for a Search Warrant for 79 Militia Hill Drive confirming that it had been attested to by the applicant (FBI Agent Prendergast) by telephone in accordance with Fed. R. Crim. P. 4.1. She signed the second Application for a Search Warrant for the person of defendant at 6:43:15 pm. The Search Warrants were supported by a thirty-five page affidavit and 7 pages of attachments.

At 6:44:33 Judge Sitarski signed the warrant for 79 Militia Hill Drive. At 6:45:35 she signed the warrant for the person of defendant. At 6:47:09 -- seven minutes after the agents had entered the house -- Judge Sitarski signed the attestation indicating that Agent Prendergast had sworn to the facts set forth in the affidavit as true and correct by telephone in accordance with Fed. R. Crim. P. 4.1 and 41(d)(3). *See* Exhibit A.

The agents conducted a search of every room in the home including every closet as well as all furniture and cabinets. This search began at 6:40 and lasted until 9:40. They seized every electronic device found in the house (13) including those owned by both of defendant Kuppusamy's parents as well as those of his brother. They also seized all of the family members' passports.

After being immediately placed into custody the defendant was taken to the Tredyffrin Township Police Department. FBI agents Edward Conway and John McKinley interrogated the defendant for over ninety minutes. At the conclusion of the interrogation the defendant was then transported to the FBI Philadelphia headquarters where he was booked. During the course of the search the FBI, while still at the Subject Premises, took statements from defendant's parents, Perumal and Thana Kuppusamy. They both stated that they resided at the Subject Premises.

The FBI also conducted extensive searches of the electronic devices seized from the subject premises. No less than 10 electronic devices were searched: cell phones, laptops, desktops, think-pads, flash drives and hard drives. These searches were conducted without any care or concern that the device may not belong to the defendant or be under his dominion and control. These searches also were conducted with no temporal limits or subject matter limitations.

On March 19, 2025 FBI Special Agent John McKinley submitted to United States Magistrate Judge Pamela A. Carlos an Application for a Search Warrant to be served on Meta for two Instagram accounts allegedly used by the defendant. *See* Exhibit B attached hereto. One of these Instagram accounts had already been thoroughly searched by the FBI without a warrant based on its March 7 EDR served on Meta. The affidavit in support of this March 19 application for a search warrant was based entirely on information received from Meta in response to the EDR as

well as information from defendant's cell phone that was seized from the Subject Premises on March 9, 2025 and searched shortly thereafter. This application was approved by Judge Carlos that same day and thereafter Meta provided all information on these two Instagram accounts.

On April 21, 2025 the 17 year old female was interviewed by the FBI in Georgia. During this interview she recalled that she first met the defendant online in the fall of 2024. She stated that after the initial meeting online they began to date online. She was 16 and he was 25. They would spend hours on the phone talking and they also would communicate by way of messaging, first on Discord and then Instagram. They talked about moving in together when she turned 18 but that they never actually met in person. She stated that the defendant never sent her nude images of minors and never attempted to dox her. She informed the agent that that she had been doxed by another individual, whom she had met before the defendant, and with whom she had shared nude images of herself.

At around the time she turned 17 she and the defendant began exchanging nude photos. She was specifically asked about the photos that were the subject of this indictment and she repeatedly stated that the photos she took of herself and sent to the defendant were her idea. She also stated that the allegations that she was going to harm herself or take her mom's gun and shoot up her high school (which initiated this entire investigation) were false and were actually done by another online individual (not the defendant) to swat her and get her house raided.

The age of consent for physical sexual relations in both Georgia and Pennsylvania is 16. *See* 18 Pa. Stat. Ann. Section 3122.1; Ga. Code Ann. Section 16-6-3. There is no allegations that defendant Kuppusamy ever had any contact -- physical or virtual -- prior to her turning 16. Had

the defendant and the female engaged in consensual sexual relations during the time they were dating it would not have violated either Pennsylvania or Georgia law.

II. LEGAL ARGUMENT

The Fourth Amendment provides, in relevant part, that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Constitution, Amend. IV. Mr. Kuppusamy submits that the government's warrantless emergency request for his private communications, made pursuant to the Stored Communications Act, was illegal under this statute and the receipt and review of those private communications constituted an unconstitutional search and seizure, furthermore, the search of the Subject Premises was unconstitutional in a number of ways. All evidence seized as a result of these searches must be suppressed since the good faith exception is not applicable under the facts of this case.

1) The Government Violated The Stored Communications Act And The 4th Amendment When It Sent An Emergency Disclosure Request To Meta And Received And Reviewed Without A Search Warrant The Private Communications Of Defendant Kuppusamy.

The FBI illegally utilized the emergency exception in the Stored Communications Act, 18 U.S.C. Section 2701 *et seq.* ("SCA") to conduct a criminal investigation of suspected child sex abuse between the 17 year old juvenile and the defendant. The FBI ignored the warrant requirements of the Communications Assistance for Law Enforcement Act ("CALEA") 18 U.S.C. Section 2703 *et seq.,* and bypassed the Fourth Amendment's warrant requirement and conducted a full and unfettered warrantless search of defendant Kuppusamy's private communications under the guise of an emergency. The FBI then used the information obtained from that warrantless search to obtain a search warrant for the Subject Premises and a search warrant for his Instagram

accounts. *See* Exhibit A and Exhibit B attached hereto. The FBI's violation of the SCA to conduct a wide ranging warrantless search constitutes a clear violation of the Fourth Amendment.

Warrantless seizures like the one at issue here are presumptively unreasonable and are therefore prohibited under the Fourth Amendment unless the government establishes that one of the carefully defined exceptions to the warrant requirement applies. *See United States v. Mundy*, 621 F.3d 283, 287 (3d Cir. 2010); *United States v. Herrold*, 962 F.2d 1131, 1137 (3d Cir. 1992). The burden of proof is on the government to show that an exception applies and that the warrantless search was reasonable. *United States v. Baker,* 563 F. Supp. 3d 361, 371 (M.D. Pa. 2021). When justifying a warrantless search like the one conducted here, that burden of proof on the government is "heavy". *Welsh v. Wisconsin,* 466 U.S. 740, 749-750 (1984).

To justify this warrantless search of the defendant's Meta accounts the government relies on the SCA. The SCA was enacted by Congress to provide strong privacy protections to the public of their stored electronic communications. In fact, if a person or provider is found to have wrongfully accessed or disclosed stored electronic communications the SCA provides for significant criminal punishment. 18 U.S.C. Section 2701(b). The CALEA, on the other hand, was enacted by Congress to assist law enforcement in conducting criminal investigations. *See* I*n the Matter of the Application of the United States of America For an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F. 3d 304-306, 313-14 (3d Cir. 2010) The FBI, however, ignored the CALEA because it requires a warrant or a court order to obtain electronic data.

The SCA was not intended to be a tool for law enforcement to bypass the Fourth Amendment warrant requirement when attempting to investigate a crime. The SCA does,

however, provide for a very limited set of circumstances when an entity like Meta may divulge contents of stored communications and customer records in its possession to a law enforcement agency or a government entity. *Id* at Section 2702(b)(7),(b)(8) and 2702(c)(4). These exceptions to the privacy protections provided by the SCA are limited to a very few specific circumstances.

Under subsection 2702(b)(7) the SCA permits disclosure of communications pertaining to the commission of a crime to a "law enforcement agency" if the provider obtains the information *inadvertently*. The SCA also permits in emergency situations a disclosure to a "government entity" if the provider has a good faith belief that an emergency involving "danger of death or serious physical injury" to any person requires disclosure, without any delay, of information "relating to the emergency." 2702(b)(8). In this case the FBI utilized subsection(b)(8) of the SCA and submitted an emergency request to Meta.

There can be no doubt that the SCA makes a clear distinction between a "law enforcement agency" receiving communications "pertaining to a crime" and a "government entity" receiving information on an emergency basis "involving danger of death or serious physical injury to a person" so long as it is *limited to communications "related to the emergency*."

Clearly, under the plain language of the SCA a law enforcement agency like the FBI cannot utilize subsection (b)(8) of the SCA to investigate a crime. Rather, if it utilizes an emergency EDR under subsection (b)(8) it must limit its request to communications relating to the emergency. Furthermore, the FBI can only receive information of a crime under Section (b)(7) if the provider obtained the information inadvertently. The FBI did not attempt to utilize the law enforcement subsection (b)(7) of the SCA. Rather, it submitted an emergency disclosure request (EDR) under subsection (b)(8).

The EDR submitted by the Philadelphia FBI was not limited to information pertaining to the perceived emergency, it was broad and unfettered in scope and it was in clear violation of the plain language of (b)(8). The EDR submitted by the FBI Philadelphia was nothing more than an illegal attempt to bypass the warrant requirements of the CALEA and the Fourth Amendment and obtain all of the private electronic communications of the defendant in furtherance of its "criminal" investigation.

On March 7, 2025 the FBI in Atlanta received a tip from Meta that a 17 year old female had live-streamed an attempt on her life and had also talked about committing homicidal acts against her family and students at her school. That same day the FBI in Atlanta received the actual data from Meta. The data showed that the alleged attempt on her life was not an emergency but in fact had occurred in December 2024. It also showed that an adult male in Pennsylvania was grooming the female and that they had shared conversations about planning homicidal terroristic acts, mass casualty events and creating firearms to conduct these acts. As a result of this information the FBI in Atlanta made an EDR to Meta seeking *only* subscriber information.

On March 7, 2025 the FBI in Philadelphia was notified that the female and male were also discussing child sexual abuse, child abduction, murder, weapon manufacturing and terroristic threats. The Philadelphia FBI then sent an EDR to Meta, but did not limit this request to information *relating* to the emergency. Rather this EDR sought all of defendant Kuppusamy's "subscriber information, linked accounts by cookies, private chat communication and distributed images, IP transactional history, geolocation information, verified device information, and any financial accounts." This wide ranging request shows that the FBI was investigating a crime of child sex abuse.

The Philadelphia FBI's EDR did not in any way limit the information sought to that "relating" to the perceived/alleged emergency. Likewise, Meta's response was not limited to information relating to the emergency. Rather, the FBI received from Meta and reviewed *all* of the information sought – without a warrant of any kind. The information received and reviewed by the FBI included all of the defendants' private communications – not just those involving the female in question -- for a six month period. (It is interesting to note that The CALEA not the SCA limits disclosure to six months. *See* 18 U.S.C. Section 2703(a). Apparently Meta was viewing this request as one made under CALEA because it was so broad and unfettered).

After illegally seizing these communications the FBI then used them in the Affidavit of Probable Cause supporting the search of the Subject Premises and the defendant's person. Specifically, the Affidavit contained extensive quotes from the private communications between the defendant and the 17 year old female. The Affidavit also contained extensive quotes from defendant's communications with third parties who had no relationship whatsoever with the 17 year old juvenile. Clearly, the review and seizure conducted under the guise of subsection (b)(8) of the SCA went well beyond information relating to the alleged emergency.

This unfettered and warrantless seizure, search and review by the FBI of all of defendant's private communications violated the SCA and the Fourth Amendment. At a hearing on this motin the defense will show that all of his settings for his Meta accounts – Facebook and Instagram – were marked private and all of the accounts were password protected. *See United States v. Chhipa,* 2024 WL 4682296 (E.D. Va. 2024)(To determine whether the defendant had a reasonable expectation of privacy courts look to the privacy settings and the government conceded that as to

defendant's private messages there was a presumption of privacy in messages designated as private on Facebook.)

The government's warrantless seizure under the guise of the SCA went well beyond the limited exceptions permitted under the SCA and was clearly a violation of that statute and the Fourth Amendment. *See United States v. Gendron,* 2026 WL 1382363 (W.D. N.Y. 2026)(An improper EDR submitted to a provider by the government renders the government's receipt of the responses a violation of the Fourth Amendment.) For these reasons alone, all of the information from this warrantless search must be suppressed as well as the fruits of this search.

2) The search warrant for the Subject Premises lacked probable cause establishing that evidence of the Subject Offenses would be found at the Subject Premises.

The affidavit of probable cause supporting the application for the search warrant for the Subject Premises did not sufficiently establish that the Subject Premises was in fact defendant Kuppusamy's residence. The affidavit also failed to establish a nexus between the Subject Premises and the alleged Subject Offenses of Mr. Kuppusamy. For each of these reasons the search warrant for the Subject Premises was defective and all evidence seized during the search of the Subject Premises must be suppressed.

It is well settled that "[p]robable cause exists when 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Grubbs*, 547 U.S. 90, 96 (2006) (*quoting Illinois v. Gates*, 462 U.S. 213, 238 (1983)). To support a finding of probable cause "[a]n affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause[.]" *Gates*, 462 U.S. at 240.

Furthermore, the search warrant for the property to be searched must contain facts that support a finding that evidence of a crime will be found therein. "There must also be evidence '*linking* [the targeted location] to the [suspect's] activities.'" *United States v. Williams*, 974 F.3d 320, 351 (3d Cir. 2020)(quoting *United States v. Burton*, 288 F.3d 91, 104 (3d Cir. 2002) (emphasis in original). An application for a warrant must "demonstrate probable cause to believe that (1) a crime has been committed . . . and (2) enumerated evidence of the offense will be found at the place searched – the so-called 'nexus' element." *United States v. Roman,* 942 F. 3d 43, 50 (1st Cir. 2019). The nexus requirement exists because "search warrants are directed, not at persons, but at property where there is probable cause to believe that instrumentalities or evidence of crime will be found." *United States v. Jones,* 994 F 2d. 1051, 1055 (3d Cir. 1993).

Direct evidence "linking the place to be searched to the crime is not required for the issuance of a search warrant." *United States v. Conley*, 4 F.3d 1200, 1207 (3d Cir. 1993). And "probable cause can be, and often is, 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. *United States v. Jones,* 994 F.2d 1051, 1056 (3d Cir. 1993) (quoting *United States v. Jackson*, 756 F.2d 703, 705 (9th Cir. 1985)). However, in this case there are no facts that would support any inference that defendant resided at the Subject Premises nor is there a nexus between evidence of the Subject Offenses and the Subject Premises.

When analyzing if a nexus has been established it is important to remember that a warrant must be supported by *facts* demonstrating probable cause – not by police summaries of what they concluded from the facts. *Gates,* 426 U.S. at 239. Mere "conclusory statement[s]" cannot support

probable cause. *Id* Finally, the nexus must be established within the four corners of the affidavit. *United States v. Stearn,* 597 F. 3d 540, 549 (3d Cir. 2010).

A careful review of the four corners of the affidavit reveals no facts that would support a nexus between the Subject Premises and evidence of the Subject Offenses. Nor are there any facts that would support an inference establishing where defendant resided. Rather, the facts Agent Prendergast included in the affidavit are both stale and inconsistent concerning his alleged residence. This Court cannot and the Magistrate could not reasonably conclude, based on the four corners of this affidavit, that the defendant resided at the Subject Premises at the time of the search or that there was nexus between the Subject Premises and the Subject Offenses –on March 9, 2025 – or for that matter at any time. Let's take a look.

In paragraph one of the Affidavit, Agent Prendergast states that the warrant is to search the premises known as 79 Militia Hill Dr., Chesterbrook, Pennsylvania 19087. She then states the conclusion that the Subject Premises "is the residence of Aniruth Kuppusamy". Agent Prendergast then attempts to offer facts (as she must) to support this conclusory statement in paragraph 14 of the Affidavit. A careful, thorough and objective review of paragraph 14, however, reveals that it contains stale facts and facts that directly contradict the conclusion that defendant resided at the Subject Premises in March 2025.

First, Agent Prendergast avers based on her review of a data base that the defendant was issued a permit to carry a firearm on October 31, 2022 wherein his residence was listed as the Subject Premises. This information is stale. Averring that 2 years and 4 months ago, when he was 22 years old, that the defendant may have identified the Subject Premises as his residence does not credibly support the conclusion that he still resided there well over two years later in March 2025.

Next, Agent Prendergast avers that in February and March of 2025 an IP address for the defendant's alleged Meta account resolved to Frazer, Pennsylvania. She further avers that Frazer is in the same county (Chester) as the Subject Premises. This averment, although not stale, directly contradicts her conclusion that the defendant resided at the Subject Premises in March 2025. It is accurate that Frazer Pennsylvania is in the same County as the Subject Premises but it is still *6.5 miles from* the Subject Premises. In fact, it is not even in the same zip code. Frazer has a 19355 zip code and the Subject Premises has a 19087 zip code. The location of the IP address in Frazer is not stale but it directly contradicted the conclusion that the defendant resided at the Subject Premises in March 2025.

Agent Prendergast next avers that the defendant, in December 2024, provided the female in question with his phone number – the same number he had in 2022 when agents met and spoke with him and his parents at the Subject Premises. This averment offers no support for the conclusion that the defendant still resided at the Subject Premises in March 2025. Simply because he had maintained the same phone number over a two year period establishes nothing about his current residence. It goes without saying that an individual maintaining the same phone number does not establish that he has somehow remained in the same residence. She also does not aver that this was landline – and she can't because she knew it was a cellphone number.

It is important to note what else has been omitted here by Agent Prendergast. She avers that agents met and spoke to Kuppusamy and his parents in 2022 at the Subject Premises. Yet she does not aver that these same agents could confirm that he even resided at the Subject Premises in 2022 -- either by defendant admitting that to the agents during the 2022 conversation or that his parents told the agents during that same 2022 conversation that their son resided there. Merely

being present at the Subject Premises with your parents at the age of 22 does not establish that you resided there at that time (2022) or for that matter 2 years and 4 months later in March 2025.

The above review is the totality of facts that are averred to support the conclusion that defendant Kuppusamy resided at the Subject Premises in March of 2025. There is no reasonable way that one can find or infer that the government has met its burden in establishing that the defendant resided at the Subject Premises on March 9, 2025. This deficiency alone is enough to invalidate this warrant. But there is more. The government as noted above must establish a nexus between the alleged criminality and the Subject Premises. A careful and thorough review of the Affidavit of Probable Cause reveals it fails in this regard as well.

In paragraph 11 of the Affidavit, Agent Prendergast avers in a conclusory fashion "Based on my investigation, *as set forth below*, there is probable cause to believe that . . . violations of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES." (Emphasis added.) However, there are simply no facts after this conclusory statement in paragraph 11 that in any way connects evidence of the Subject Offenses to the Subject Premises. There is nothing "set forth below" as promised by Agent Prendergast that would allow for such an inference. And there are no facts that would support the finding of a nexus between evidence of the Subject Offenses and the Subject Premises.

A careful, thorough and objective review of the Affidavit reveals that it is bereft of facts supporting a nexus between the Subject Premises and the Subject Offenses. It is not averred that defendant Kuppusamy was present at or anywhere near the Subject Premises when any crimes or improper conduct took place or for that matter that he was ever physically present at the location after the 2022 conversation with the agents. It is not averred that he was seen parking his car

there or entering or exiting the location. It is not averred that he made threats to kidnap from that location or anywhere near that location. It is not averred that he enticed anyone let alone a minor to engage in sexually explicit conduct at or anywhere near that location. It is not averred that he received distributed, reproduced or possessed any depictions of minors engaging in sexually explicit conduct at or anywhere near that location. It is not averred that he was using his phone or computer or laptop at the location or anywhere near the location. It is not averred that he sent or received any improper materials or messages or communications at that location or anywhere near the location. It is not averred that he downloaded anything at the location. It is not even alleged that there was internet service at that location. It is not averred that he had a cellphone registered at the location. It is not averred that he received mail at that location or slept or ate meals there. This Court cannot and the Magistrate could not reasonably conclude, based on the four corners of this affidavit, that a nexus existed between evidence of the Subject Offenses and the Subject Premises at the time of the search – March 9, 2025.

Because the affidavit failed to adequately establish that the defendant resided at the Subject Premises and because the affidavit is devoid of any facts establishing a nexus between the Subject Premises and the Subject Offenses the warrant is fatally deficient and all evidence seized as a result of the search of he Subject Premises must be suppressed. *See e.g. United States v. Alford,* 764 F. Supp. 3d 191, 265-68 (M.D. Pa. 2025)(Search warrant invalid due to lack of averred facts that the defendant lived in the premises to be searched and lack of nexus to the location and evidence of a crime requiring suppression and good faith exception was not applicable); *See also United States v. Rodriguez,* 2014 WL 4413606 (E.D. Pa. 2014)(Search warrant invalid due to lack of averred facts that the defendant lived in the premises to be searched and lack of nexus to the location and

evidence of a crime, and good faith exception did not apply because the search warrant contained mere conclusions.)

The defense also argues that the execution of the warrant at the Subject Premises was illegal because law enforcement entered the Subject Premises and took defendant into custody before the search warrant was finally approved by the Magistrate. Additionally, the defense argues that the searches of the electronic devices and the storage related to those devices were conducted well outside the temporal parameters of the probable cause averred in the warrant and encroached on areas where no evidence of the Subject Offenses could be found. The defense will develop these issues concerning the illegal execution of the warrant and the searches of the devices further at the evidentiary hearing on this motion.

3) The Warrant for the Subject Premises was Overbroad.

An overly broad warrant is one that "'describe[s] in both specific and inclusive generic terms what is to be seized,'" but nonetheless "authorizes the seizure of items as to which there is no probable cause." *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents ($92,422.57)*, 307 F.3d 137, 149 (3d Cir. 2002) (citation omitted). Overly broad warrants can be cured by redaction, i.e., by "striking … those severable phrases and clauses that are invalid for lack of probable cause or generality." *Id.*

To determine whether a warrant was overbroad, this Court "must compare the scope of the search and seizure authorized by the warrant with the ambit of probable cause established by the supporting affidavit." *In re Impounded Case (L. Firm)*, 840 F.2d 196, 200 (3d Cir. 1988). The permissible scope of a search depends on "the particular factual context of each case and also the information available to the investigating agent that could limit the search at the time the warrant

application is given to the magistrate." *United States v. Yusuf*, 461 F.3d 374, 395 (3d Cir. 2006). A warrant is overbroad if it "requests the seizure of lawfully possessed material of no evidentiary value." *United States v. Cochran*, 806 F. Supp. 560, 564 (E.D. Pa. 1992).[1]

First, the warrant provided for the search of the entire Subject Premises without any limitation as to areas allegedly occupied by the defendant. Every room in the house was fair game including home offices and bedrooms of anybody who resided there. It authorized a complete search of the premises without any regard to the personal privacy of other innocent individuals that resided there. This unfettered search of a residence flies in the face of the fundamental protections provided by the Fourth Amendment. *See Florida v. Jardines,* 569 U.S. 1, 6 (2013)(The "very core" of the Fourth Amendment is to be "free from unreasonable governmental intrusion" into one's home. Indeed the home is "first among equals" in Fourth Amendment protection.)

The warrant also provided for seizure, copying and search of all digital devices including but not limited to computers, laptops, tablets, smartphones, routers, modems and network equipment found in the Subject Premises – again with total disregard of the privacy of others citizens besides defendant that resided there. It also included all storage connected with said devices including hard drives as well as electronic and cloud storage. This unfettered search of any and all electronic devices including cloud storage flies in the face of the fundamental protections provided by the Fourth Amendment. *See United States v. Williams,* 813 F. Supp. 3d

1 The factors to consider when determining whether a warrant is overbroad include "(1) whether probable cause exists to seize all items of a particular type described in the warrant, (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not, and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued." *U.S. v. Mann,* 389 F.3d 869, 878 (9th Cir. 2004).

503, 515 (E.D. Pa. 2025)("An individual's phone must be afforded heightened protections as it "is the digital equivalent of its owner's home, capable of holding a universe of private information'"); *See also United States v. Holcomb,* 2025 WL 5088357 (9th Cir. 2026)("Given the vast amount of data 'stored on computers, a 'heightened' specificity requirement applies 'in the computer context.' ")

The search permitted by the warrant also contained no temporal limits. In other words the agents could search these devices going as far back as they wanted, well beyond the time frame for which probable cause was alleged to exist. *See* Exhibit A attachment B ("the items to be searched are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to . . . the Subject Offenses, involving Anniruth Kuppusamy and/or *including* occurring on or after January 1, 2024.)(emphasis added). Clearly the government with the use of the word "including" gave itself an unfettered time period with zero consideration to probable cause of the Subject Offenses.

A temporal limit restricting the authorized search to the time frame of the criminal conduct is a factor that can enhance the particularity of the warrant. *See United States v. Zelaya-Veliz,* 94 F 4th. 321, 341(4th Cir. 2024); *See also United States v. McCall,*84 F. 4th 1317, 1328 (11th Cir. 2023)(government conceded warrant for cloud storage fell short of particularity requirement because it allowed a search of all conceivable data on the account without any meaningful temporal or subject matter limitations.); *See also United States v. Williams,* 813 F. Supp. 3d 503, 527 (E.D. Pa. 2025)(The warrant failed the particularity test and constituted a general warrant because it failed to limit the search to a reasonable time frame making it facially invalid.) Yet the warrant in

this case contained no temporal limitations and the search conducted went well beyond the relevant time period.

4) **The Affidavit of Probable Cause Contained Material Omissions.**

The warrant application is also misleading because it left out a critical piece of material information. The defense submits that Special Agent Prendergast recklessly withheld information linking the Subject Premises to defendant's parents: Thana Kuppusamy (mother) and Perumal Kuppusamy (father). She also omitted the fact that the phone number reference in paragraph 14 of the affidavit (484-719-9066) was a cell phone number.

The defense submits that Agent Prendergast and other law enforcement officers were aware or should have been aware that as of March 9, 2025 Thana and Perumal Kuppusamy owned the Subject Premises, resided at the Subject Premises and had resided there for many years. This critical information was never provided to the magistrate judge. She was also aware that the phone number in paragraph 14 was a cell phone number.

When Special Agent Prendergast applied for the warrants to search the Subject Premises, she recklessly omitted all information regarding the fact that Thana and Perumal Kuppusamy owned and resided at the Subject Premises. Had the Magistrate been made aware that defendant's parents – law abiding citizens – owned and resided at the Subject Premises – there is no way she would have approved a warrant that allowed the government to search every inch of the house and search and seize every electronic device and (cloud storage) found therein – with zero regard to who had dominion and control over the premises and the devices. The magistrate would also not have found that the Subject Premises was defendant's residence if made aware that the number alleged to be a link to the Subject Premises was for a cell phone.

The Supreme Court has established a two-step procedure for a defendant to prevail on a motion to suppress on the basis of an alleged false statement or omission in an affidavit of probable cause: 1) the defendant must make a "substantial preliminary showing" with respect to both *Franks v. Delaware* elements—falsehood or omission and materiality—to warrant a hearing; and 2) "at the [*Franks*] hearing, the defendant must carry his ultimate burden of proving both elements." *United States v. Gordon*, 664 F. App'x 242, 245 (3d Cir. 2016) (*citing Franks v. Delaware,* 438 U.S. 154 at 155-56, 172 (1978)).

Mr. Kuppusamy submits that he is entitled to a *Franks* hearing, at which he will prove Special Agent Prendergast's deliberate material omissions void the search warrant and require suppression of all fruits of the unconstitutional search. *See Wong Sun v. United States*, 371 U.S. 471 (1963); *United States v. Coggins*, 986 F.2d 651, 653 (3d Cir. 1993).

To obtain a *Franks* hearing due to omissions "a defendant must make a 'substantial preliminary showing' that the omissions demonstrated a 'reckless disregard for the truth' and the challenged omissions were "essential to the court's finding of probable cause ." *United States v. Harding,* 2025 WL 3295130 (D. NJ. 2025). An omission is made with reckless disregard for the truth "when an officer recklessly omits facts that any reasonable person would want to know." *See Wilson v. Russo*, 212 F.3d 781, 787 (3d Cir. 2000)). Once granted a hearing, the defendant "must ultimately prove by a preponderance of the evidence that : (1) the affiant with a reckless disregard for the truth, made omissions that create a falsehood in applying for a warrant; and (2) that such omissions were material, or necessary, to the probable cause determination." *United States v. Yusuf*, 461 F.3d 374, 383 (3d Cir. 2006) (*citation omitted*).

To remedy a material omission, a court "remove[s] the falsehood created by [the] omission by supplying the omitted information to the original affidavit." *Id.* at 384 (*first alteration in original*) *(internal quotation marks omitted*). "In the end, the defendant must prove by a preponderance of the evidence that probable cause does not exist under the corrected affidavit, i.e., that the deficiency in the affidavit was material to the original probable cause finding." *Id.* at 383. "If the defendant is able to ultimately meet this burden, 'the Fourth Amendment requires that . . . the fruits of the search [must be] excluded to the same extent as if probable case was lacking on the face of the affidavit." *Id.* at 384 (alterations in original) (*quoting United States v. Frost*, 999 F.2d 737, 743 (3d Cir. 1993) (*quoting Franks*, 438 U.S. at 156)).

The warrant application for the Subject Premises makes no references to the fact that the defendant's parents owned and resided at the Subject Premises. Whether or not the agents knew or know that these individuals resided there remains unknown. The failure to include this information and that the number was a cell phone number deprived the magistrate judge of critical evidence related to the warrants' relationship to the Subject Premises and the likelihood that evidence related to the Subject Offenses would be discovered there. The omissions also would have without question caused the Magistrate to substantially limit the scope of the warrant. Thus, Agent Prendergast's Affidavit in support of the Warrant contains material omissions and, when corrected under *Franks*, fails to set forth sufficient probable cause for the Subject Premises. Accordingly, Mr. Kuppusamy is entitled to a hearing pursuant to *Franks* to correct the affidavit

5) The Good Faith Exception does not Apply Here

"Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Zimmerman,* 277 F. 3d 426, 438 (3d Cir. 2002) *quoting United States*

v. Reilly, 76 F. 3d 1271, 1280 (2nd Cir. 1996). Mr. Kuppusamy submits that the FBI's use of the SCA to intentionally avoid the warrant requirements of the CALEA and the Fourth Amendment can not be excused by good faith. *See Davis v. United States,* 564 U.S. 229, 240 (2011) (suppression is appropriate if the police acted "deliberately, recklessly, or with gross negligence")

Furthermore, the reliance on the search warrant for the Subject Premises was not reasonable and no federal agent would have or should have relied on it in good faith. A search warrant that relies on conclusions instead of facts cannot support a finding of good faith. As such, the good faith exception to the exclusionary rule announced in *United States v. Leon*, 468 U.S. 897, 900 (1984) does not apply in this case.

Normally law enforcement's reliance on a search warrant suffices to establish good faith. However, there are situations where an officer's reliance is not reasonable and would not trigger the good faith exception. Specifically, there are four such situations "1. Where the magistrate issued the warrant in reliance on a deliberately or reckless false affidavit; 2. Where the magistrate abandoned his or her judicial role and failed to perform his or her neutral and detached function; 3. Where the warrant was based on an affidavit so lacking in probable cause as to render official belief in its existence entirely unreasonable; or 4. Where the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized." *United States v. Zimmerman,* 277 F. 3d 426, 436-7 (3d Cir. 2002). The defense submits that a number of these factors were present here and will establish them at the hearing on this motion.

6) The Evidence Recovered Must Be Suppressed as a Fruit of the Fourth Amendment Violation.

It is well settled that "[e]vidence obtained through unreasonable searches and seizures must be suppressed as 'fruit of the poisonous tree.'" *United States v. Dowdell*, 70 F.4th 134, 139

(3d Cir. 2023) (*quoting United States v. Bey*, 911 F.3d 139, 144 (3d Cir. 2018)). The proceeds of the search of the Meta accounts and the Subject Premises must be suppressed as fruits of the poisonous tree. *Wong Sun*, 371 U.S. at 488.

"[T]he exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" *Segura v. United States*, 468 U.S. 796, 804 (1984) (internal citations omitted). The Supreme Court has held that any evidence that has been "come at by exploitation of [the] illegality" of an unconstitutional seizure or search, even if indirectly, is tainted by that illegality and must be suppressed. *Wong Sun v. United States*, 371 U.S. 471, 488 (1963).

Here the defense submits that the following evidence must be excluded as fruits of the illegal searches discussed above: all evidence recovered from the EDR submitted to Meta, all evidence recovered during the search of the Subject Premises, defendant's custodial statement, the statement of defendant's parents taken at the time of the search of the Subject Premises, the evidence from the search of all electronic devices, and the evidence from the search of the defendant's Instagram accounts. *See United States v. Vasquez De Reyes,* 149 F. 3d 192 (3d Cir. 1998).

III. CONCLUSION

For all the reasons set forth above, as well as any that may become apparent at the requested evidentiary hearing, or that the Court deems just, Mr. Kuppusamy respectfully requests that the Court grant his Motion to Suppress and preclude the government from introducing into evidence at trial all evidence recovered as a result of these multiple unconstitutional searches.

/s/ *James J. McHugh, Jr.*
JAMES J. MCHUGH, JR.
Assistant Federal Defender

CERTIFICATE OF SERVICE

I, James J. McHugh, Jr., Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that I have caused a copy of the Defendant's Motion to Suppress, to be filed and served through the Eastern District Clerk's Office Electronic Case Filing ("ECF") upon:

Michelle Rotella
Assistant United States Attorneys
United States Attorney's Office
615 Chestnut Street, Suite 1250
Philadelphia, Pennsylvania, 19106.

/s/ *James J. McHugh, Jr.*
JAMES J. MCHUGH, JR.
Assistant Federal Defender

DATE: August 13, 2026

Exhibit A

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of 79 Militia Hill Drive, Chesterbrook, Pennsylvania 19087	)	Case No. 25-MJ-503-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-1

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Sections	*Offense Description*
18 U.S.C. §§ 875(c), 2251, 2252	interstate threats, production and receipt of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Jessica Prendergast
Applicant's signature

Jessica Prendergast, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 3/9/2025

Lynne A. Sitarski
Digitally signed by Lynne A. Sitarski
Date: 2025.03.09 18:42:18 -04'00'
Judge's signature

City and state: Philadelphia, PA

HON. LYNNE A. SITARSKI, USMJ
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of 79 Militia Hill Drive, Chesterbrook, Pennsylvania 19087	)	Case No. 25-MJ-503-1

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-1

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 23, 2025 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3/9/2025

Lynne A. Sitarski

Digitally signed by Lynne A. Sitarski
Date: 2025.03.09 18:44:33 -04'00'

Judge's signature

City and state: Philadelphia, PA

HON. LYNNE A. SITARSKI, USMJ

Printed name and title

Return

Case No.: 25-mj-503-1	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of THE PERSON OF ANNIRUTH KUPPUSAMY	)	Case No. 25-MJ- 503-2

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-2

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Sections	*Offense Description*
18 U.S.C. §§ 875(c), 2251, 2252	interstate threats, production and receipt of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Jessica Prendergast
Applicant's signature

Jessica Prendergast, Special Agent, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 3/9/2025

Lynne A. Sitarski
Digitally signed by Lynne A. Sitarski
Date: 2025.03.09 18:43:15 -04'00'
Judge's signature

City and state: Philadelphia, PA

HON. LYNNE A. SITARSKI, USMJ
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of THE PERSON OF ANNIRUTH KUPPUSAMY	)	Case No. 25-MJ-503-2

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-2

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 23, 2025 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty .
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3/9/2025

Lynne A. Sitarski
Digitally signed by Lynne A. Sitarski
Date: 2025.03.09 18:45:35 -04'00'
Judge's signature

City and state: Philadelphia, PA

HON. LYNNE A. SITARSKI, USMJ
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:25- mj-503-2	*Date and time warrant executed:*	*Copy of warrant and inventory left with:*
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF 79 MILITIA HILL DR CHESTERBROOK, PA 19087 AND THE PERSON OF ANIRUTH KUPPUSAMY	Case No. 25-mj-503 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jessica Prendergast, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 79 Militia Hill Dr, Chesterbrook, Pennsylvania 19087 (hereinafter the "**SUBJECT PREMISES**"), which is the residence of ANIRUTH KUPPUSAMY (hereinafter the "KUPPUSAMY"). The **SUBJECT PREMISES** is further described in Attachment A, and the things to be searched are described in Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI). I have been employed in this position since January 2021. I am currently assigned to the Philadelphia division, Newtown Square Resident Agency. where I am tasked with investigating violent crimes and gangs, including commercial robberies and burglaries and other violations of the Hobbs Act, carjackings, interstate transportation of stolen property, and other violations of federal law to include violent crimes against children involving child sex abuse material ("CSAM"). Prior to being assigned to the Violent Crimes Task Force, I was assigned to the Safe Streets Task Force on two different gang squads in the Chicago Division of the FBI. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part. Where I assert that an event took place on a particular date or at a particular time, I am asserting that it took place on or about the date or at or near the time asserted.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 875(c) (collectively, the "SUBJECT OFFENSES") have been committed, are being committed, or will be committed by KUPPUSAMY and other persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

5. Title 18, United States Code § 875(c) provides that, "whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

6. Title 18, United States Code § 2251 prohibits a person from employing, using, persuading, inducing, enticing or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or transmitting a live visual depiction of such conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including

by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

7. Title 18, United States Code § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

8. "Child pornography,[1]" as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

9. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

10. The FBI and other federal law enforcement agencies have been investigating an online group known as "the Com." During my involvement in this investigation, I have learned

[1] I use the term child pornography and child sexual abuse material interchangeably.

that the Com consists of a geographically diverse group of individuals, organized in various subgroups, who communicate through online applications, such as Discord, Telegram, Facebook, Instagram, and Snapchat. Members of the Com use these communication platforms to share resources, tactics, and tools needed to conduct their illegal activity. They also confirm membership within the Com through individual actors' presence in certain online groups or servers and social media mutual friends or connections. In particular, male members of certain subgroups of the Com often engage in acts of violence and groom females, often minors, who then agree to produce child pornography (CSAM) and commit acts of self-harm ("cutting").

11. I am currently assigned to an investigation involving KUPPUSAMY, who appears to be engaging in illegal behavior consistent with association with certain subgroups of The Com, specifically production of CSAM, planning acts of violence, and exploiting minors.[2] Based on my investigation, as set forth below, there is probable cause to believe that KUPPUSAMY has enticed an underage female to produce and share CSAM, harm herself, and has discussed and taken steps to plan an act of violence and praised violent attacks committed by racially motivated violent extremists, and has transmitted interstate threats, including by threatening to harm [redacted] mother, and discussing the manufacturing, altering, and provision of firearms, and that violations of the SUBJECT OFFENSES will be found at the **SUBJECT PREMISES.**

12. On March 8, 2025, in coordination with FBI Special Agents assigned to the Atlanta Division, Special Agents of the Philadelphia Division of the FBI began reviewing information obtained from an emergency disclosure request from Meta Platforms (Facebook and Instagram). The response included conversation between Instagram users totallykindday (UID 59803352284),

[2] Records received from Meta revealed that on January 26, 2025, KUPPUSAMY sent a message to the minor [redacted] that referenced The Com: "promise you wont just use me not talking to you as a reason to talk to the same people you did before . . . com people. . ."

and [redacted] and others. As described below, the FBI identified the user of totallykindday as KUPPUSAMY and the user of [redacted] and [redacted] as a minor female, [redacted].[3]

13. The email account used to register [redacted] and [redacted] appears to be based on the name of a minor, [redacted]. A search of FBI databases for the name [redacted] revealed a report listing [redacted] as making threats to conduct a school shooting in January 2025. The report provided an address of [redacted]. After consulting with FBI Agents from the Atlanta Division, I learned that [redacted] has been fully identified as a minor female who turned 17 in January of 2025 and resides in Georgia. [redacted] is known to FBI Atlanta from prior investigations. On March 8, 2025, FBI Atlanta made contact with Rabun County Sheriff's Office who confirmed that [redacted] resides at [redacted] and previously attended school in Highlands, North Carolina. FBI Atlanta contacted the Principal of the Highlands School where [redacted] attended, who provided [redacted] date of birth as January [redacted] 2008.

14. KUPPUSAMY is a 25-year-old male residing at the **SUBJECT PREMISES**. I know from a check of databases available to me that KUPPUSAMY has a valid permit to carry a firearm issued on October 31, 2022, listing the **SUBJECT PREMISES** as his residence. Records received from Meta revealed that the user totallykindday provided a birthdate of September 24, 1999, which matches KUPPUSAMY's birthday and that the totallykindday account was accessed from IP addresses resolving to Frazer, Pennsylvania in February and March of 2025. Frazer is a neighborhood within Chester County, Pennsylvania, within the Eastern District of Pennsylvania.

[3] [redacted] full name is known to law enforcement but is not set forth in full herein because she is a minor. I have confirmed [redacted] full identity with Agents from the Atlanta Division of the FBI who have encountered [redacted] in prior investigations. The emergency disclosure included conversations between [redacted] and KUPPUSAMY from, at least, November of 2024, however the conversations indicated that they had been communicating prior to that date.

Moreover, on December 8, 2024, the user totallykindday provided his phone number to [redacted] as (484) 719-9066. Databases available to me confirm that the (484) 719-9066 telephone number is associated with KUPPUSAMY. In addition, in a message on December 18, 2024, KUPPUSAMY send a message from the totallykindday account to [redacted], informing her that his name is "aniruth" which is KUPPUSAMY's first name. In 2022, agents from FBI Philadelphia met and spoke with KUPPUSAMY and his parents at the **SUBJECT PREMISES**. At the time, KUPPUSAMY provided the same phone number he provided to [redacted] on December 8, 2024.

15. Information obtained pursuant to an exigent pen trap/trace device installed on ES's Meta accounts revealed that KUPPUSAMY, using the totallykindday account, was communicating with [redacted] throughout March 8 and March 9, 2025.

Evidence of CSAM Production, Enticement, and Exploitation of Minor [redacted]

16. On February 2, 2025, at 17:21:18 UTC Instagram account [redacted], used by [redacted], sent video 1124949112191691 to totallykindday, used by KUPPUSAMY. A Special Agent from the Atlanta Division reviewed the content of that video, which is approximately 2 seconds long. The video depicts a while female who is completely nude on her hands and knees on a bed. The female's anus and vagina are exposed to the camera. The female looks at the camera to start the video and can be identified as [redacted].

17. I also reviewed the above video and have reviewed other conversations between [redacted] and KUPPUSAMY. Below is an excerpt from their conversation on February 7, 2025, beginning at 04:15:32 UTC where the two discuss meeting to have sex and in which KUPPUSAMY directs [redacted] to send him explicit images of herself:

> **totallykindday:** u free this week?
> im serious this time
> thursday-sat in 30E

[redacted]: RLLY

totallykindday: ya ill figure out the money this weekend and book it

[redacted]: [2 emojis] omg

totallykindday: but NOT A SOUL CAN KNOW

[redacted]: i undrstand i know i promise

totallykindday: baby im serious i dont wanna be put on blast by all of twitter like luc okay

[redacted]: oki i promise i love u!!!!!

totallykindday: like even if u change ur mind keep it a secret
i love u smsmsmsmsms

[redacted]: aaaa omg ur taking my virginity [2 emojis]

totallykindday: yessir

[redacted]: [liked an image]

totallykindday: lemme see you i havent seen you in forever

[redacted] need need need need need
mnnnnbbnbnn hehehehehhe

totallykindday: send pic neow

[redacted]: me or meeeeee

totallykindday: u owe me for ignoring me for 2 days

[redacted]: [liked a message]

totallykindday: youuuuu

[redacted]: [liked an image]

totallykindday: i love youuu
i want to put my hand on your waist so bad ive been fantasizing about this specifically

[redacted]: hehehehe i loveeee youuuuuuuuuu >_<
[liked a message]

totallykindday: this is how ill break the touch barrier
im gonna lift ur shirt up to put my hand on ur waist and take a pic of that contrast
btw if u steal a shirt of mine u should make a tiktok or two
in it
would be funny

[redacted]: [liked a message]
[liked a message]
[liked a message]
[sent video file 1323062935694183 of her exposing her breasts]

18. Below is an excerpt from their conversation on February 11, 2025, beginning at 03:54:33 UTC where KUPPUSAMY requests [redacted] produce CSAM:

totallykindday: lemme see sum chop chop
dont need to be elaborate pull your pants down

[redacted]: mmm haven't shaved but i'll do anything for u

totallykindday: you think i care about that i might not even let you shave when you at mine
[redacted]: [liked an image]
[sent video file 617124297573376 of a white female naked from the waist down. She then touches her vagina before directing the camera up to her chest where she lifts her shirt and bares her breasts]
video for u

totallykindday: amazing
question
what u smell likw

[redacted]: mmnmnmn vanilla perfume and coconut oil

totallykindday: no hoe ur pussy
ur scent
coconut oil is nice tho

19. Below is an excerpt from their conversation on February 12, 2025, beginning at 12:34:08 UTC where KUPPUSAMY requests [redacted] to produce CSAM:

totallykindday: have morning wood[4] now take ur slut responsibilities

[4] Based on my training and experience, I believe that KUPPUSAMY is telling [redacted] that he has an erection and that he is directing her to send him explicit materials as her "slut responsibilities."

[sent an attachment]
hoe

[redacted]: [liked a message]
[liked a message]
Sendink!!!!!
[sent video file 960162809412596 where she lifts up her shirt to expose her naked breasts then pulls down her pants to expose her pubic area]

totallykindday: my property for breakfast

[redacted]: [liked a message]
teysyyeysyeyys!!!

totallykindday: im gonna piss on this
and spit
need my own property to chain u to a tree on a really muddy day
and the chain is too short to stand up so ur forced to lie down
ull be brown like me

20. Below is an excerpt from their conversation on February 22, 2025, beginning at 16:46:59 UTC where the KUPPUSAMY acknowledges that [redacted] is a minor and asks her to produce CSAM:

[redacted]: shower time!!

totallykindday: proof?

[redacted]: [sent photo file 582699611433676 of herself kneeling completely naked in front of a mirror, exposing her breasts and vagina with her face clearly visible]
hate taking out tampons
[sent photo file 1409055660443680 of herself standing completely naked in front of a mirror, exposing her breasts and vagina]

totallykindday: i eat
you are so fucking beautiful holy shit
your bush coming in amazingly

[redacted]: [liked a message]
[liked a message]
hehehehehe
YAYYY
[liked a message]

[sent photo file 935933121986980 of herself standing completely naked in front of a mirror, exposing her breasts and vagina]

totallykindday: i bet it smells so nice

[redacted]: [liked a message]

totallykindday: fuck u look delicious

[redacted]: [liked a message]
come overrr

totallykindday: strong chance ill move in march <3

[redacted]: the door is unlocked [2 smile emojis]
[liked a message]
HEHEHEHE RLLLY

totallykindday: yayyayay
yesss

[redacted]: [liked a message]
[liked a message]
YAYAYYAYY

totallykindday: if i get job far away i can just kidnap u right
need to spirit u away and hold u hostage then elope when ur 18

21. In addition to the preceding paragraph where KUPPUSAMY acknowledges that [redacted] is not yet 18 years old, on several other occasions KUPPUSAMY acknowledges that [redacted] is a minor. For example, below is an excerpt from their conversation on December 4, 2024 beginning at 16:05:45 UTC where the KUPPUSAMY acknowledges that [redacted] is a minor:

totallykindday: i need to come before ur bday
ill never get 16yo [redacted] back after that…

On December 7, 2024 at 03:19:51 UTC, KUPPUSAMY writes a message to [redacted] stating, "baby im 25 u knew this". In a conversation on January 18, 2025, with another Instagram user, the other user asks KUPPUSAMY "how did you catch feelings for a 15 year old" to which KUPPUSAMY responds "16 and idk dude it was like a train crashed into me".

22. On January 27, 2025, starting at 16:50:02 UTC, KUPPUSAMY has a conversation with another Instagram user after [redacted] tells him she is taking her phone to the police. In that conversation, part of which is excerpted below, KUPPUSAMY discusses deleting evidence of his relationship with [redacted] to protect himself:

totallykindday: DUDE
totallykindday: HOW FUCKED AM I
Other Instagram User: ITS TOMORROW
Other Instagram User: YOU HAVE TIME
Other Instagram User: temporary plan1. wipe ur dms with [redacted] on instagram by closing
Other Instagram User: 2. unsend/censor any proof of identity youve sent her
totallykindday: oh there is none
totallykindday: except
Other Instagram User: 3. unsend/censor any sexual shit in your dms
totallykindday: i can wipe
Other Instagram User: wiping discord dms
Other Instagram User: is possible
Other Instagram User: because i dont think they are retained at all
Other Instagram User: but if you delete your discord account
Other Instagram User: its going to be retained for weeks
Other Instagram User: they will force you or discord to undelete it
Other Instagram User: there are tools
totallykindday okay discorf deletion script
Other Instagram User: yes i have
Other Instagram User: make her use it too on a laptop
totallykindday: she doesn't have a laptop
totallykindday: i have her login for her current discorf
Other Instagram User: https://greasyfork.org/en/scripts/518587-deletcord-delete-all-messages-in-a-discord-channel-or-dm-mass-deletion
totallykindday: they need a warrant to unlock the phone

23. On February 9, 2025, at 12:36:40 UTC, KUPPUSAMY sends the following message to another user on Instagram, referring to [redacted], "and if i make her an enemy she could start targeting me for doxxing cp etc". Based on my training and experience, I believe that the "cp" referenced to mean child pornography, showing KUPPUSAMY is aware the images [redacted] has sent

him are illegal CSAM. I also know that "doxxing" is the act of gathering an individual's personal identifying information and posting it online to an Internet-based community.

24. Based on my training and experience, I believe that the images of [redacted] genitals that are discussed herein constitute child pornography under Title 18, United States Code, Section 2256(8), as it is a visual depiction of sexually explicit conduct where the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, which includes a lascivious exhibition of the genitals or pubic area of any person

25. In addition, on at least two occasions, KUPPUSAMY sent images and/or videos of what I believe to be his genitals to [redacted] including a video depicting the individual ejaculating.

Evidence of Enticing Minor [redacted] to Commit Acts of Self Harm

26. I have reviewed conversations between KUPPUSAMY and [redacted] that occurred on February 10, 2025. In those messages, excerpted below, KUPPUSAMY requests [redacted] cut herself while he watches on camera:

> totallykindday 7:26:44pm PST: maybe u should do a cutsign[5] for me
> totallykindday 7:27:04pm PST: u remember that sigil?
> [redacted] 7:27:19pm PST: yes i'll cut it
> 7:27:23pm PST: on cam

Evidence of Discussion of Planned Acts of Violence and Firearms Violations

27. I have reviewed additional conversations between KUPPUSAMY and [redacted] Based upon the messages, KUPPUSAMY and [redacted] have discussed racially motivated violent extremist actors and their admiration those actors, including individuals responsible for mass casualty terrorist attacks.

[5] Based on my training and experience and the training and experience of other agents upon whom I rely, I know that a cutsign is a term used in The Com and affiliated groups to refer to an individual cutting themselves with a specific symbol or marking that identifies them as being associated with, or property of, a particular person.

28. For example, on January 31, 2025, KUPPUSAMY and [redacted] share their desire to be together by March 15, 2025. I know that March 15 is the anniversary of the two consecutive mass shootings committed by Brenton Tarrant in Christchurch, New Zealand, which resulted in the deaths of 51 people. Tarrant livestreamed his attack, which was posted to the Internet. An excerpt of the chat as reviewed appears below:

totallykindday: i hope we'll be moved in together before march

totallykindday: then we can watch tarrant on the anniversary together

[redacted]: YES OMMGMFMFMGMG

I believe "tarrant" refers to the shooter, Brenton Tarrant, and that KUPPUSAMY and [redacted] are discussing watching his livestream of the Christchurch shooting on the anniversary of the attack.

29. On December 19, 2024, KUPPUSAMY expresses his admiration of Oklahoma City Bomber, Timothy McVeigh:

totallykindday: timothy mcveigh is the ultimate saint not a fucking turk

30. As excerpted below, KUPPUSAMY frequently expresses his desire to harm others:

totallykindday (59803352284) - 12/08/2024 6:27:15pm PST: im gonna kill your mom

totallykindday 12/18/2024 5:41:24pm PST: anyway i constantly think about killing people too if it makes you feel any better im just very conscious it would hurt people i dont wanna hurt and it wouldn't accomplish anything and people would laugh at me and hate me if i didn't set a record

[redacted] 12/18/2024 5:41:52pm PST: i do too but it feels gross and different

totallykindday 12/18/2024 5:41:52pm PST: don't kill anyone else without my guidance either

***

totallykindday 12/19/2024 7:04:57am PST: i want to learn how to properly sacrifice humans

***

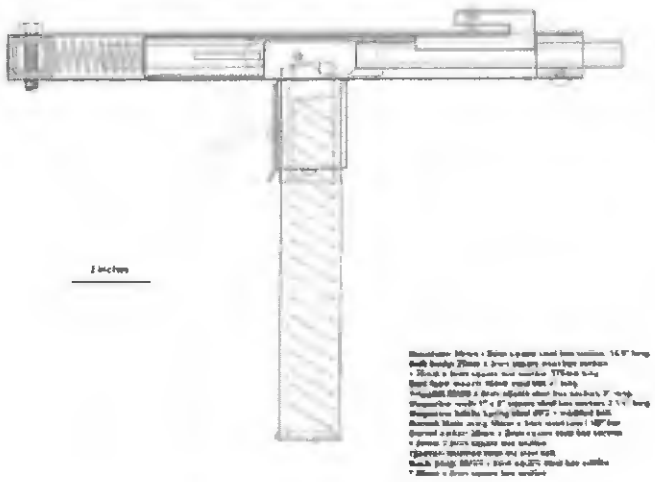
totallykindday 02/20/2025 10:24:41am PST: i want to stab someone so bad i think about it all the time

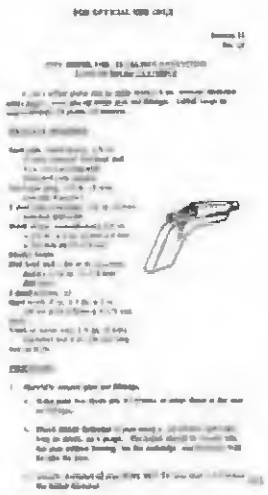
[redacted] 02/20/2025 10:24:44am PST: i also love the sounds of the knives going in and the shoes hitting their skulls

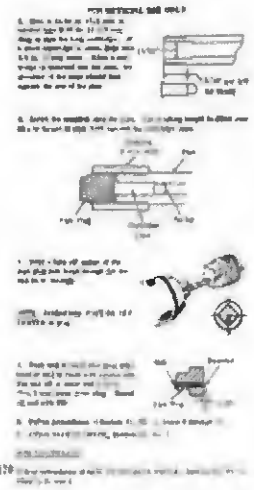
***

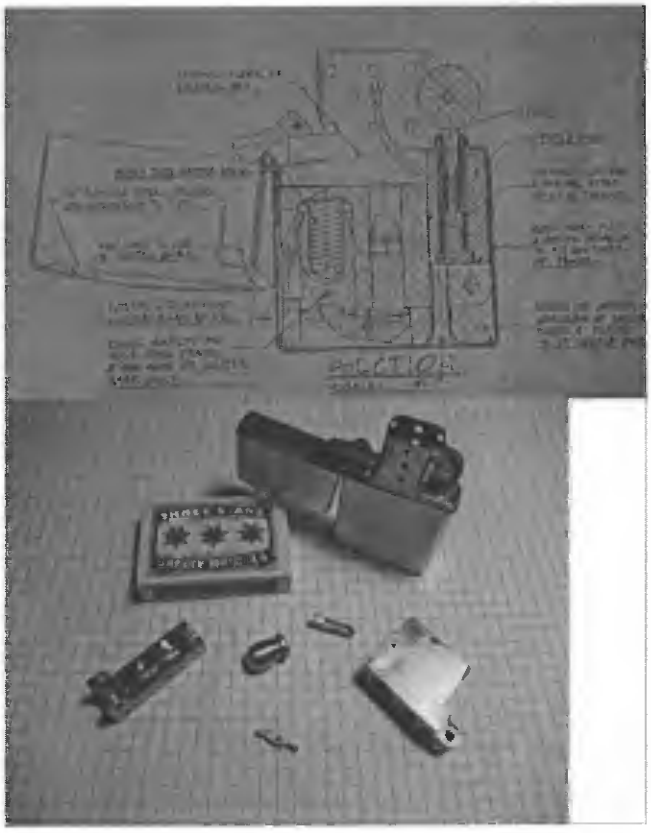
totallykindday 03/06/2025 8:52:26pm PST: need to kill someone by handcuffing them in their own car and putting a brick on the accelerator into a lake

31. A review of the messages also revealed that on March 1, 2025, KUPPUSAMY shared, with [redacted] detailed schematics of how to construct homemade firearms, including what appears to be a semi-automatic weapon with an extended magazine, a "pipe pistol", and a lighter designed to shoot a single round as well as a photograph of a lighter with parts removed. The images below were also sent:









32. Between March 2 and 3, 2025, KUPPUSAMY and [redacted] discussed firearms, including weapons that KUPPUSAMY claims to have purchased and manufactured. Notably, during this time frame, [redacted] was posting messages regarding her friendship with "Sam Rupnow"

including a post that stated "oomf shot up her school while i was in the psych ward at least wait for me to get out." I know that Natalie Samantha Rupnow was a 15-year-old student who committed a shooting attack at Abudnant Life Christian School in Madison, Wisconsin, that resulted in the deaths of three people and which injured six others. It appears that in response to these posts, KUPPUSAMY sent [redacted] the following messages, in which they discuss plans and intentions to commit violent acts and KUPPUSAMY cautions [redacted] to be careful about discussing her plans to commit violent acts because law enforcement may be present in their social media chats:

> totallykindday (59803352284) - 03/02/2025 7:15:14pm PST: dont say the shit you say w me regarding plans intentions etc there are 1000% informants in tcc circles trust no one but me
>
> totallykindday (59803352284) - 03/02/2025 7:17:32pm PST: like regardless of what ur doing who ur talking to at least dont get us both jailed
>
> totallykindday (59803352284) - 03/02/2025 7:19:44pm PST: what's the plan if someone connects this to ur identity btw
>
> totallykindday (59803352284) - 03/02/2025 7:21:49pm PST: the gun pic is fine i think if it's not up on fb or something but the other two id strongly advise u to delete, post without face if u really want to
>
> [redacted] - 03/02/2025 7:44:17pm PST: https://www.quadrato309.com/2019/07/introduction-to-system-q309.html?m=1
>
> totallykindday (59803352284) - 03/02/2025 8:30:07pm PST: slitting ur throat and poasting it on story if u talk to any of ur mutuals btw #iloveyou
>
> [redacted]) - 03/02/2025 9:13:33pm PST:

totallykindday (59803352284) - 03/02/2025 9:16:01pm PST: u can buy some german guns but it's like nice car money

totallykindday (59803352284) - 03/02/2025 9:16:42pm PST: bruh it's going 10-15k for SEMI

totallykindday (59803352284) - 03/02/2025 9:17:32pm PST: insane it must be super rare

totallykindday (59803352284) - 03/02/2025 9:17:40pm PST: stg44 u can get more easily in full auto

totallykindday (59803352284) - 03/02/2025 9:17:55pm PST: i buy [redacted] all the guns and i build some too

totallykindday (59803352284) - 03/03/2025 9:26:49am PST: if i gifted u a gun would ur mom take it

[redacted] 03/03/2025 9:27:02am PST: she wouldn't find it

Based on your affiant's training and experience, I believe that KUPPUSAMY and [redacted] are discussing the unlawful conversion of a firearm to fully automatic when he tells her that a stg44 can more easily be obtained in "full auto." Based on my training and experience, I know that a StG 44 is a German assault rifle developed during World War II. I have not been able to verify that

KUPPUSAMY meets the definition of a licensed importer, licensed manufacturer, or licensed dealer (firearms dealer) permitted to engage in the business of importing, manufacturing, or dealing in firearms as defined in 18 U.S.C § 922. Thus, absent an actual firearms dealer license, KUPPUSAMY would be violating the firearms act by providing weapons to anyone, much less a minor, which 18 USC 922 prohibits even firearms dealers from doing so.

33. During that same conversation, KUPPUSAMY and [redacted] discuss, among other things, Robert Bowers (the perpetrator of the Tree of Life Synagogue attack), "fbi attention on Terrorgram", miss gorehound, with KUPPUSAMY stating "i wish miss gorehound didnt get arrested i wouldve introduced u."[6]

Evidence of Risk of Destruction of Evidence

34. As noted above, KUPPUSAMY and [redacted] previously discussed deleting incriminating communications between them. I have reviewed additional messages between KUPPUSAMY and [redacted] which indicates the two created communication accounts and shared the usernames and passwords, thus allowing either party to access the content and be in a position to delete evidence.

[6] On September 9, 2024, the Department of Justice charged Dallas Humber, 34, of Elk Grove, California, and Matthew Allison, 37, of Boise, Idaho — leaders of the Terrorgram Collective, a transnational terrorist group —in a 15-count indictment for soliciting hate crimes, soliciting the murder of federal officials, and conspiring to provide material support to terrorists. Humber used the moniker miss gorehound. According to the indictment, Humber and Allison are the leaders of the Terrorgram Collective, a transnational terrorist group that operates on the digital messaging platform Telegram, where it promotes white supremacist accelerationism: an ideology centered on the belief that the white race is superior; that society is irreparably corrupt and cannot be saved by political action; and that violence and terrorism are necessary to ignite a race war and accelerate the collapse of the government and the rise of a white ethnostate. *See https://www.justice.gov/archives/opa/pr/leaders-transnational-terrorist-group-charged-soliciting-hate-crimes-soliciting-murder*

35. For instance, on January 20, 2025, KUPPUSAMY advised [redacted] that he had created a new email account and shared the password:

totallykindday: new email

totallykindday: [redacted]@outlook.com

totallykindday: password is [redacted]

36. Similarly, on the same date, [redacted] notified KUPPUSAMY that she had created at least one a new account on a yet to be determined application and provided the username along with a screenshot of the account creation displaying the password[7]:

[redacted]: username is rudysprincess

37. I am aware that Atlanta FBI Agents and partner law enforcement officers are conducting an investigation at the residence of [redacted] scheduled for March 9, 2025. Given the frequent communication between KUPPUSAMY and [redacted], FBI Philadelphia seeks to conduct a search warrant concurrent with the FBI Atlanta investigation in order to prevent KUPPUSAMY from destroying evidence associated with shared accounts as wells as his personal devices and other evidence located in the **SUBJECT PREMISES**.

[7] It remains unclear if [redacted] is creating a seperate account to be associated with the username rudysprincess or is changing the username from [redacted]0893 as displayed on the screenshot she sent to KUPPUSAMY.

Technical Terms

38. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, digital devices, or other storage media. Thus, the warrant applied for would authorize the seizure of digital devices, electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. *Probable cause.* I submit that if a digital device, computer, or storage medium is found on the **SUBJECT PREMISES,** there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and

durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning),

or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

42. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

44. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are

designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby

thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones

employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

45. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

i. Upon securing the **SUBJECT PREMISES**, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices within the scope of this warrant as defined above, deemed capable of containing the

information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the **SUBJECT PREMISES**. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

ii. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

iii. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment

B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC CHARACTERISTICS

46. This warrant permits law enforcement agents to obtain from the person ANIRUTH KUPPUSAMY (but not any other individuals present at the **SUBJECT PREMISES** at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

47. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

48. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

49. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

50. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

51. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

52. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

53. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

54. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from

the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the **SUBJECT PREMISES**; (2) hold the Device(s) found at the **SUBJECT PREMISES** in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the **SUBJECT PREMISES** in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

55. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

REQUEST FOR WARRANT AND SEALING

56. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation. For the same reasons, I also request that the Court sign the proposed nondisclosure order to prevent the service providers from notifying the subjects about the existence of this investigation.

57. Based upon the above, there is probable cause to believe that KUPPUSAMY has solicited and is in possession of CSAM, has exploited a minor, committed or is preparing to commit firearms violations, is taking steps to commit an act of violence and that evidence of planning and instruments of the offenses will be found on KUPPUSAMY and at the **SUBJECT PREMISES**, to include his devices. I submit that this affidavit supports probable cause for a warrant to search the **SUBJECT PREMISES** described in Attachment A-1, the person described in Attachment A-2, and seize the items described in Attachment B.

Respectfully submitted,

/s/ Jennifer Prendergast
Jennifer Prendergast
Special Agent, Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this day of March, 2025.

Lynne A. Sitarski

Digitally signed by Lynne A. Sitarski
Date: 2025.03.09 18:47:09 -04'00'

THE HONORABLE LYNNE A. SITARSKI
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1
Location to be Searched

79 Militia Hill Drive, Chesterbrook, Pennsylvania 19087

The residence is a single-family carriage home, two stories tall with a wooden front door. According to Zillow, there are three bedrooms and two bathrooms. The residence has light-colored brick siding and a single car driveway. A placard with "79" is hung directly to the right of the front door.

ATTACHMENT A-2
Location to be Searched

The person of ANNIRUTH KUPPUSAMY

ANNIRUTH KUPPUSAMY, depicted below, is described as an Asian male, approximately 5' 4" tall, with a date of birth of September 24, 1999.

ATTACHMENT B
Items to be Searched for and Seized

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 United States Code 875(c) (interstate threats), Title 18, United States Code, Section 2251(sexual exploitation of children known colloquially as production of child pornography), Title 18, United States Code, Section 2252 (violations, attempt to violate, and conspiracy to violate, manufacturing, possession, receipt, or distribution of child pornography) (collectively, the SUBJECT OFFENSES), involving ANNIRUTH KUPPUSAMY and/or [redacted] including, occurring on or after January 1, 2024:

1. All visual depictions of minors engaged in sexually explicit conduct or self harm produced using minors engaged in such conduct, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened emails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened emails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.

3. All communications, photographs, files, or other documents or records with or about potential minors involving sexual topics or in an effort to seduce or to meet a minor.

4. All documents, communications, records, information, and evidence concerning threats to commit acts of violence, mass casualty attacks, including evidence regarding ANNIRUTH KUPPUSAMY state of mind.

5. All firearms or parts used to manufacture or alter firearms.

6. Schematics describing the manufacture of firearms.

7. Any documentation or communications regarding the planned used of firearms to commit an act of violence or other plans or reasoning justifying an act of violence.

8. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256.

9. Records, information, and evidence relating to the identification of persons who either (i)collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the SUBJECT OFFENSE; or (ii) communicated about matters relating to the SUBJECT OFFENSE, including records that help reveal their whereabouts;

10. Digital devices used in the planning of the above described offenses, including laptop computers, tablets, and smartphones.

    a. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":
        i. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
        ii. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
        iii. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
        iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
        v. evidence of the times the Device(s) was used;
        vi. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
        vii. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
        viii. records of or information about Internet Protocol addresses used by the Device(s); and
        ix. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
        x. Routers, modems, and network equipment used to connect computers to the Internet.

11. Records, information, and evidence of who used, owned, or controlled the Devices such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence;

12. Records, information, and evidence of all communications, including call logs, text messages, iMessages, encrypted messaging applications, audio messages, voice mails, as well as any messages in any internet messaging applications (i.e., "apps"), between the users of the Devices and other people relating to planning, collaborating, conspiring, assisting (knowingly or unknowingly), executing, concealing, or covering up the commission of the SUBJECT OFFENSES, including records that help reveal their whereabouts

13. Notes, photographs, videos, logs, communications, cloud information, applications, and data from any mobile applications on the Devices relating to planning, collaborating, conspiring, assisting (knowingly or unknowingly), executing, concealing, or covering up the SUBJECT OFFENSES;

14. Communications between the users of the device and other people relating to planning, collaborating, conspiring, assisting (knowingly or unknowingly), executing, concealing, or covering up the commission of the SUBJECT OFFENSES , including records that help reveal their whereabouts;

15. Notes, photographs, videos, logs, communications, cloud information applications, and data from any mobile applications on the Devices relating to planning, collaborating, conspiring, assisting (knowingly or unknowingly), executing, concealing, or covering up the SUBJECT OFFENSES

16. Records, information, and evidence of the times the Devices were used;

17. Passwords, encryption keys, and other access devices that may be necessary to access the Devices;

18. Documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

19. Records, information, and evidence about Internet Protocol addresses used by the Devices;

20. Records, information, and evidence of or about Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from ANNIRUTH KUPPUSAMY (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the Device(s) found at the PREMISES,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

Exhibit B

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INSTAGRAM ACCOUNTS UID 59803352284 AND UID 72514323885, THAT ARE STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.

Case No. 25-mj-577

USAO# 2025-R00130

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2251, 2252, 875(c)	sexual exploitation of children, possession, manufacturing, receipt of child pornography, interstate threats

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ John A. McKinley
Applicant's signature

John A. McKinley, Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: PAMELA A. CARLOS Digitally signed by PAMELA A CARLOS Date: 2025.03.19 10:31:08 -04'00'

Judge's signature

City and state: Philadelphia PA

Hon. Pamela A. Carlos, US Magistrate Judge
Printed name and title

USAO25CR130000049

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INSTAGRAM ACCOUNTS UID 59803352284 AND UID 72514323885, THAT ARE STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	)	Case No. 25-mj-577 USAO# 2025-R00130

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before April 1, 2025 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: PAMELA A. CARLOS Digitally signed by PAMELA A. CARLOS Date: 2025.03.19 10:33:11 -04'00'

Judge's signature

City and state: Philadelphia PA Hon. Pamela A. Carlos, US Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 25-mj-577	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH INSTAGRAM ACCOUNTS UID 59803352284 AND UID 72514323885, THAT ARE STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	USAO# 2025-R00130 Mag No. 25-mj-577 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, John A. McKinley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (the "**SUBJECT ACCOUNTS**"), that are stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc. ("Meta"), a social media services company headquartered at 1 Meta Way, Menlo Park, CA 94025. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI). I have been employed in this position since January 2017. I am currently assigned to the Philadelphia division, Newtown Square Resident Agency. where I am tasked with investigating violent crimes and gangs, including commercial robberies and burglaries and other violations of the Hobbs Act, carjackings,

interstate transportation of stolen property, and other violations of federal law to include violent crimes against children involving child sex abuse material ("CSAM"). Prior to being assigned to the Violent Crimes Task Force, I was assigned to the Joint Terrorism Task Forces in both the Houston and Philadelphia Divisions of the FBI, where I conducted international and domestic terrorism investigations. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part. Where I assert that an event took place on a particular date or at a particular time, I am asserting that it took place on or about the date or at or near the time asserted.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 875(c) (collectively, the "SUBJECT OFFENSES") have been committed, are being committed, or will be committed by KUPPUSAMY and other persons known and unknown and that evidence of the SUBJECT OFFENSES will be found in the Instagram account identified with UID 59803352284 and username totallykindday (**"SUBJECT ACCOUNT 1"**); and Instagram account identified with UID 72514323885 and usernames "aniruth__._" and "aniona8814" (**SUBJECT ACCOUNT 2**); (collectively, the **"SUBJECT ACCOUNTS"**). There is also probable cause to search the

information described in Attachment A for evidence of these crimes further described in Attachment B.

5. Title 18, United States Code § 875(c) provides that, "whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

6. Title 18, United States Code § 2251 prohibits a person from employing, using, persuading, inducing, enticing or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or transmitting a live visual depiction of such conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

7. Title 18, United States Code § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

8. "Child pornography" as defined in 18 U.S.C. § 2256(8),[1] is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a

[1] I use the term child pornography and child sexual abuse material interchangeably.

minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

9. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

10. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), cert. denied, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), aff'd sub nom, *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), aff'd, 813 F.2d 1231 (9th Cir. 1987), cert. denied, 484 U.S. 856 (1987).

11. The *Dost* factors include: (1) whether the focal point of the visual depiction is on the child's genitalia or pubic area; (2) whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child; (4) whether the child is fully or partially clothed, or nude; (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer. *See also United States v. Villard*, 885 F.2d 117, 122 (3d Cir.1989). Significantly, "[a] visual depiction need not involve all of these factors to be 'lascivious exhibition' of the genitals or pubic area." *Dost,* 636 F. Supp. at 832. The

determination is based on the overall content of the visual depiction, taking into account the age of the minor. *Id.; see also Villard*, 885 F.2d at 122 ("Although more than one factor must be present in order to establish lasciviousness, all six factors need not be present.").

JURISDICTION

12. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

13. On March 9, 2025, Aniruth Kuppusamy ("KUPPUSAMY") was charged by complaint with one count of manufacturing child pornography in violation of 18 U.S.C. § 2251. *See* 25-mj-504. That same day, FBI agents executed a search warrant at KUPPUSAMY's residence and seized his cellular telephone. *See* 25-mj-503. KUPPUSAMY is a 25-year-old male who resided in the Eastern District of Pennsylvania at the time of his arrest. As set forth in the complaint and based on information obtained throughout the investigation, there is probable cause to believe that KUPPUSAMY has enticed an underage female to produce and share CSAM, harm herself, has discussed and taken steps to plan an act of violence, praised violent attacks committed by racially motivated violent extremists, and has transmitted interstate threats, including by threatening to harm the Victim's mother, and discussed the manufacturing, altering, and provision of firearms, and that violations of the SUBJECT OFFENSES will be found in the **SUBJECT ACCOUNTS**.

14. On March 8, 2025, in coordination with FBI Special Agents assigned to the Atlanta Division, Special Agents of the Philadelphia Division of the FBI began reviewing information

obtained from an emergency disclosure request from Meta Platforms (Facebook and Instagram). The response included conversation between **SUBJECT ACCOUNT 1** and two accounts used by the minor Victim. The information provided by Meta as part of that emergency disclosure was limited to six months prior to the date of disclosure.

15. Information obtained from Meta revealed that **SUBJECT ACCOUNT 1** was created on May 11, 2023, with the email address notdoomerbrown@tutanota.com and a date of birth of September 24, 1999, which matches KUPPUSAMY's date of birth. The investigation has revealed that "doomerbrown" is an online moniker used by KUPPUSAMY. **SUBJECT ACCOUNT 1** was accessed from IP addresses resolving to Frazer, Pennsylvania in February and March of 2025. Frazer is a neighborhood within Chester County, Pennsylvania, within the Eastern District of Pennsylvania. On December 8, 2024, the user of **SUBJECT ACCOUNT 1** provided his phone number to the Victim as (484) 719-9066, which is KUPPUSAMY's phone number. In addition, in a message on December 18, 2024, KUPPUSAMY sent a message from **SUBJECT ACCOUNT 1** to the Victim informing her that his name is "aniruth" which is KUPPUSAMY's first name. Information obtained from Meta revealed that **SUBJECT ACCOUNT 2** had the vanity name aniruth__._ and aniona8814.

Evidence of CSAM Production, Enticement, and Exploitation of Minor Victim

16. In November of 2024, **SUBJECT ACCOUNT 1** sent a message to an Instagram account used by the Victim ("Victim Account 1") asking "btw how far are u from Raleigh". When asked by Victim Account 1 the reason for the inquiry, **SUBJECT ACCOUNT 1** responded that he was "trying to do research on companies in ga" which I believe indicates that KUPPUSAMY was aware of where Victim 1 lived and was making efforts to be physically closer to her. The emergency disclosure included conversations between the Victim and **SUBJECT ACCOUNT 1**

from, at least, November of 2024 onward. However, based on my review of their communications, I believe that KUPPUSAMY and Victim Account 1 had been communicating prior to November of 2024,

17. On February 2, 2025, at 17:21:18 UTC, Victim Account 1 cutsent video 1124949112191691 to **SUBJECT ACCOUNT 1.** A Special Agent from the Atlanta Division reviewed the content of that video, which is approximately 2 seconds long. The video depicts a white female who is completely nude on her hands and knees on a bed. The female's anus and vagina are exposed to the camera. The female looks at the camera to start the video and can be identified as the Victim.

18. Messages seized on KUPPUSAMY's phone revealed that he also used **SUBJECT ACCOUNT 2** to communicate with the Victim. For example, on February 2, 2025, starting at 1:13:58 UTC, **SUBJECT ACCOUNT 2** sent a series of messages to Victim Account 1, stating, that **SUBJECT ACCOUNT 2** was thinking "about [diminutive of Victim 1's name] licking my butt". When the Victim inquired whether KUPPUSAMY used **SUBJECT ACCOUNT 2** "or the other one," **SUBJECT ACCOUNT 2** responded "i had this one open on phone but I can switch easy here".

19. On February 3, 2025, **SUBJECT ACCOUNT 2** sent Victim Account 1 the following messages: "i feel like my head is being torn apart i fear that you've already done something and im praying so hard that you are unharmed"; "Everyone who did this to you will be tortured"; "Everyone responsible for this will suffer"; "No one culpable will live a good life"; "I love you to death". On February 3, 2025, **SUBJECT ACCOUNT 2** also replied to a story posted by Victim Account 1 and wrote "I love you so much keep staying string my dear" followed by "strong* wtf".

20. In addition, records seized from KUPPUSAMY's phone appear to show contact between **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2** in March of 2025, although I am unable to discern the content of those messages.

21. I also reviewed the above video in paragraph 17 and have reviewed other conversations between the Victim and KUPPUSAMY. Below is an excerpt from their conversation on February 7, 2025, beginning at 04:15:32 UTC where the two discuss meeting to have sex and in which KUPPUSAMY directs the Victim to send him explicit images of herself:

SUBJECT ACCOUNT 1: u free this week?
im serious this time
thursday-sat in 30E

Victim Account 1: RLLY

SUBJECT ACCOUNT 1: ya ill figure out the money this weekend and book it

Victim Account 1: [2 emojis] omg

SUBJECT ACCOUNT 1: but NOT A SOUL CAN KNOW

Victim Account 1: i undrstand i know i promise

SUBJECT ACCOUNT 1: baby im serious i dont wanna be put on blast by all of twitter like luc okay

Victim Account 1: oki i promise i love u!!!!!

SUBJECT ACCOUNT 1: like even if u change ur mind keep it a secret
i love u smsmsmsmsms

Victim Account 1: aaaa omg ur taking my virginity [2 emojis]

SUBJECT ACCOUNT 1: yessir

Victim Account 1: [liked an image]

SUBJECT ACCOUNT 1: lemme see you i havent seen you in forever

Victim Account 1: need need need need need
mnnnnbbnbnn hehehehehhe

SUBJECT ACCOUNT 1: send pic neow

Victim Account 1: me or meeeeee

SUBJECT ACCOUNT 1: u owe me for ignoring me for 2 days

Victim Account 1: [liked a message]

SUBJECT ACCOUNT 1: youuuuu

Victim Account 1: [liked an image]

SUBJECT ACCOUNT 1: i love youuu
i want to put my hand on your waist so bad ive been fantasizing about this specifically

Victim Account 1: hehehehe i loveeee youuuuuuuuuu >_<
[liked a message]

SUBJECT ACCOUNT 1: this is how ill break the touch barrier
im gonna lift ur shirt up to put my hand on ur waist and take a pic of that contrast
btw if u steal a shirt of mine u should make a tiktok or two
in it
would be funny

Victim Account 1: [liked a message]
[liked a message]
[liked a message]
[sent video file 1323062935694183 of her exposing her breasts]

22. Below is an excerpt from their conversation on February 11, 2025, beginning at 03:54:33 UTC where KUPPUSAMY requests the Victim produce CSAM:

SUBJECT ACCOUNT 1: lemme see sum chop chop
dont need to be elaborate pull your pants down

Victim Account 1: mmm haven't shaved but i'll do anything for u

SUBJECT ACCOUNT 1: you think i care about that i might not even let you shave when you at mine

Victim Account 1: [liked an image]
[sent video file 617124297573376 of a white female naked from the waist down. She then touches her vagina before directing the camera up to her chest where she lifts her shirt and bares her breasts]

video for u

SUBJECT ACCOUNT 1: amazing
question
what u smell likw

Victim Account 1: mmnmnmn vanilla perfume and coconut oil

SUBJECT ACCOUNT 1: no hoe ur pussy
ur scent
coconut oil is nice tho

23. Also on February 7, 2025, **SUBJECT ACCOUNT 2** replied to a story posted by Victim Account 1.

24. Below is an excerpt from their conversation on February 12, 2025, beginning at 12:34:08 UTC where KUPPUSAMY requests the Victim to produce CSAM:

SUBJECT ACCOUNT 1: have morning wood[2] now take ur slut responsibilities
[sent an attachment]
hoe

Victim Account 1: [liked a message]
[liked a message]
Sendink!!!!!
[sent video file 960162809412596 where she lifts up her shirt to expose her naked breasts then pulls down her pants to expose her pubic area]

SUBJECT ACCOUNT 1: my property for breakfast

Victim Account 1: [liked a message]
teysyyeysyeyys!!!

SUBJECT ACCOUNT 1: im gonna piss on this
and spit
need my own property to chain u to a tree on a really muddy day
and the chain is too short to stand up so ur forced to lie down
ull be brown like me

[2] Based on my training and experience, I believe that KUPPUSAMY is telling the Victim that he has an erection and that he is directing her to send him explicit materials as her "slut responsibilities."

25. Below is an excerpt from their conversation on February 22, 2025, beginning at 16:46:59 UTC where KUPPUSAMY acknowledges that the Victim is a minor and asks her to produce CSAM:

Victim Account 1: shower time!!

SUBJECT ACCOUNT 1: proof?

Victim Account 1: [sent photo file 582699611433676 of herself kneeling completely naked in front of a mirror, exposing her breasts and vagina with her face clearly visible]
hate taking out tampons
[sent photo file 1409055660443680 of herself standing completely naked in front of a mirror, exposing her breasts and vagina]

SUBJECT ACCOUNT 1: i eat
you are so fucking beautiful holy shit
your bush coming in amazingly

Victim Account 1: [liked a message]
[liked a message]
hehehehehe
YAYYY
[liked a message]
[sent photo file 935933121986980 of herself standing completely naked in front of a mirror, exposing her breasts and vagina]

SUBJECT ACCOUNT 1: i bet it smells so nice

Victim Account 1: [liked a message]

SUBJECT ACCOUNT 1: fuck u look delicious

Victim Account 1: [liked a message]
come overrr

SUBJECT ACCOUNT 1: strong chance ill move in march <3

Victim Account 1: the door is unlocked [2 smile emojis]
[liked a message]
HEHEHEHE RLLLY

SUBJECT ACCOUNT 1: yayyayay
yesss

Victim Account 1: [liked a message]
[liked a message]
YAYAYYAYY

SUBJECT ACCOUNT 1: if i get job far away i can just kidnap u right
need to spirit u away and hold u hostage then elope when ur 18

26. In addition to the preceding paragraph where KUPPUSAMY acknowledges that the Victim is not yet 18 years old, on several other occasions KUPPUSAMY acknowledges that the Victim is a minor. For example, below is an excerpt from their conversation on December 4, 2024, beginning at 16:05:45 UTC where the KUPPUSAMY acknowledges that the Victim is a minor:

SUBJECT ACCOUNT 1: i need to come before ur bday
ill never get 16yo [diminutive of Victim's name] back after that…

On December 7, 2024 at 03:19:51 UTC, KUPPUSAMY using **SUBJECT ACCOUNT 1** writes a message to the Victim stating, "baby im 25 u knew this". In a conversation on January 18, 2025, with another Instagram user, the other user asks KUPPUSAMY "how did you catch feelings for a 15 year old" to which KUPPUSAMY, using the **SUBJECT ACCOUNT,** responds "16 and idk dude it was like a train crashed into me".

27. On January 27, 2025, starting at 16:50:02 UTC, KUPPUSAMY has a conversation with another Instagram user after the Victim tells him she is taking her phone to the police. In that conversation, part of which is excerpted below, KUPPUSAMY discusses deleting evidence of his relationship with the Victim to protect himself:

SUBJECT ACCOUNT 1: DUDE
SUBJECT ACCOUNT 1: HOW FUCKED AM I
Other Instagram User: ITS TOMORROW
Other Instagram User: YOU HAVE TIME
Other Instagram User: temporary plan1. wipe ur dms with [diminutive of Victim's name] on instagram by closing
Other Instagram User: 2. unsend/censor any proof of identity youve sent her

SUBJECT ACCOUNT 1: oh there is none
SUBJECT ACCOUNT 1: except
Other Instagram User: 3. unsend/censor any sexual shit in your dms
SUBJECT ACCOUNT 1: i can wipe
Other Instagram User: wiping discord dms
Other Instagram User: is possible
Other Instagram User: because i dont think they are retained at all
Other Instagram User: but if you delete your discord account
Other Instagram User: its going to be retained for weeks
Other Instagram User: they will force you or discord to undelete it
Other Instagram User: there are tools
SUBJECT ACCOUNT 1 okay discorf deletion script
Other Instagram User: yes i have
Other Instagram User: make her use it too on a laptop
SUBJECT ACCOUNT 1: she doesn't have a laptop
SUBJECT ACCOUNT 1: i have her login for her current discorf
Other Instagram User: https://greasyfork.org/en/scripts/518587-deletcord-delete-all-messages-in-a-discord-channel-or-dm-mass-deletion
SUBJECT ACCOUNT 1: they need a warrant to unlock the phone

28. On February 9, 2025, at 12:36:40 UTC, KUPPUSAMY, using **SUBJECT ACCOUNT 1** sends the following message to another user on Instagram, referring to the Victim, "and if i make her an enemy she could start targeting me for doxxing cp etc". Based on my training and experience, I believe that the "cp" referenced to mean child pornography, showing KUPPUSAMY is aware the images the Victim has sent him are illegal CSAM. I also know that "doxxing" is the act of gathering an individual's personal identifying information and posting it online to an Internet-based community.

29. Based on my training and experience, I believe that the images of the Victim's genitals that are discussed herein constitute child pornography under Title 18, United States Code, Section 2256(8), as it is a visual depiction of sexually explicit conduct where the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, which includes a lascivious exhibition of the genitals or pubic area of any person.

30. In addition, on at least two occasions, KUPPUSAMY sent images and/or videos of what I believe to be his genitals to the Victim, including a video depicting the individual ejaculating. In the search warrant executed on KUPPUSAMY's residence on March 9, 2025, a comforter with geometric shapes seen in these two videos was found in a hamper in KUPPUSAMY's bedroom closet.

Evidence of Enticing Minor [redacted] o Commit Acts of Self Harm

31. I have reviewed conversations between KUPPUSAMY and the Victim that occurred on February 10, 2025. In those messages, excerpted below, KUPPUSAMY requests the Victim cut herself while he watches on camera:

> **SUBJECT ACCOUNT 1** 7:26:44pm PST: maybe u should do a cutsign[3] for me
> **SUBJECT ACCOUNT 1** 7:27:04pm PST: u remember that sigil?
> Victim Account 1 7:27:19pm PST: yes i'll cut it
> Victim Account 1 7:27:23pm PST: on cam

SUBJECT ACCOUNT 1 and Victim Account 1 also discuss branding the Victim and putting cigarettes out on her skin.

Evidence of Discussion of Planned Acts of Violence and Firearms Violations

32. I have reviewed additional conversations between KUPPUSAMY, using **SUBJECT ACCOUNT 1** and the Victim. Based upon the messages, KUPPUSAMY and the Victim have discussed racially motivated violent extremist actors and their admiration those actors, including individuals responsible for mass casualty terrorist attacks. In addition, KUPPUSAMY has discussed mass casualty attacks and racially motivated violent extremism with other individuals using **SUBJECT ACCOUNT 1.**

[3] Based on my training and experience and the training and experience of other agents upon whom I rely, I know that a "cutsign" is a term used in online violent extremist communities to refer to an individual cutting themselves with a specific symbol or marking that identifies them as being associated with, or property of, a particular person.

33. For example, on September 6, 2024, **SUBJECT ACCOUNT 1** made the following comment: "⚡⚡ Heil St Breivik". I know that on July 22, 2011, Anders Behring Breivik committed a racially motivated violent mass shooting at a summer camp in Norway that killed 69 participants and detonated a bomb in Norway resulting in the deaths of eight people. I also know that two lightning bolts are frequently used to indicate support for or allegiance with Nazi Germany and are derived from the Schutzstaffel (SS) of Nazi Germany.

34. On January 31, 2025, KUPPUSAMY and the Victim shared their desire to be together by March 15, 2025. I know that March 15 is the anniversary of the two consecutive mass shootings committed by Brenton Tarrant in Christchurch, New Zealand, which resulted in the deaths of 51 people. Tarrant livestreamed his attack, which was posted to the Internet. An excerpt of the chat as reviewed appears below:

SUBJECT ACCOUNT 1: i hope we'll be moved in together before march

SUBJECT ACCOUNT 1: then we can watch tarrant on the anniversary together

Victim Account 1: YES OMMGMFMFMGMG

I believe "tarrant" refers to the shooter, Brenton Tarrant, and that KUPPUSAMY and the Victim are discussing watching his livestream of the Christchurch shooting on the anniversary of the attack.

35. On December 19, 2024, KUPPUSAMY expressed his admiration of Oklahoma City Bomber, Timothy McVeigh:

SUBJECT ACCOUNT 1: timothy mcveigh is the ultimate saint not a fucking turk

36. As excerpted below, KUPPUSAMY frequently expressed his desire to harm others:

SUBJECT ACCOUNT 1 - 12/08/2024 6:27:15pm PST: im gonna kill your mom

SUBJECT ACCOUNT 1 12/18/2024 5:41:24pm PST: anyway i constantly think about killing people too if it makes you feel any better im just very conscious it would hurt

people i dont wanna hurt and it wouldn't accomplish anything and people would laugh at me and hate me if i didn't set a record

Victim Account 1 12/18/2024 5:41:52pm PST: i do too but it feels gross and different
SUBJECT ACCOUNT 1 12/18/2024 5:41:52pm PST: don't kill anyone else without my guidance either

***

SUBJECT ACCOUNT 1 12/19/2024 7:04:57am PST: i want to learn how to properly sacrifice humans

***

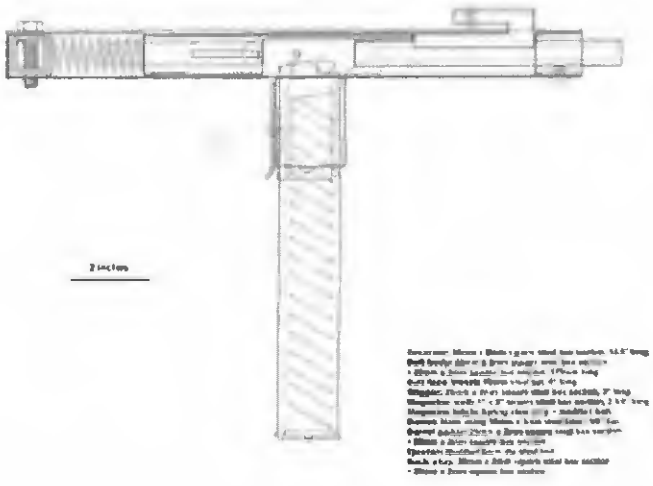
SUBJECT ACCOUNT 1 02/20/2025 10:24:41am PST: i want to stab someone so bad i think about it all the time

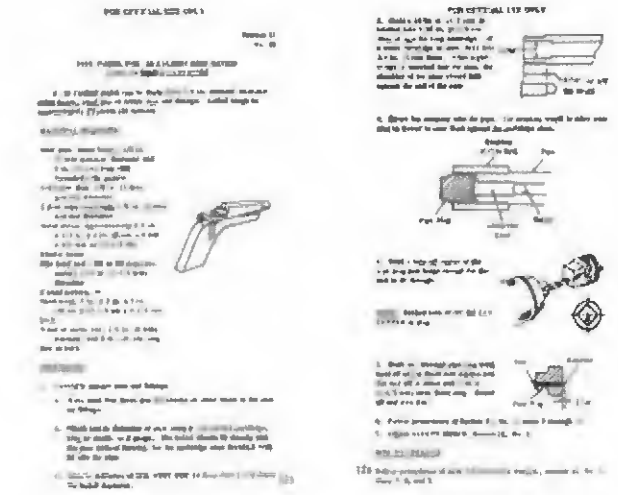
Victim Account 1 02/20/2025 10:24:44am PST: i also love the sounds of the knives going in and the shoes hitting their skulls

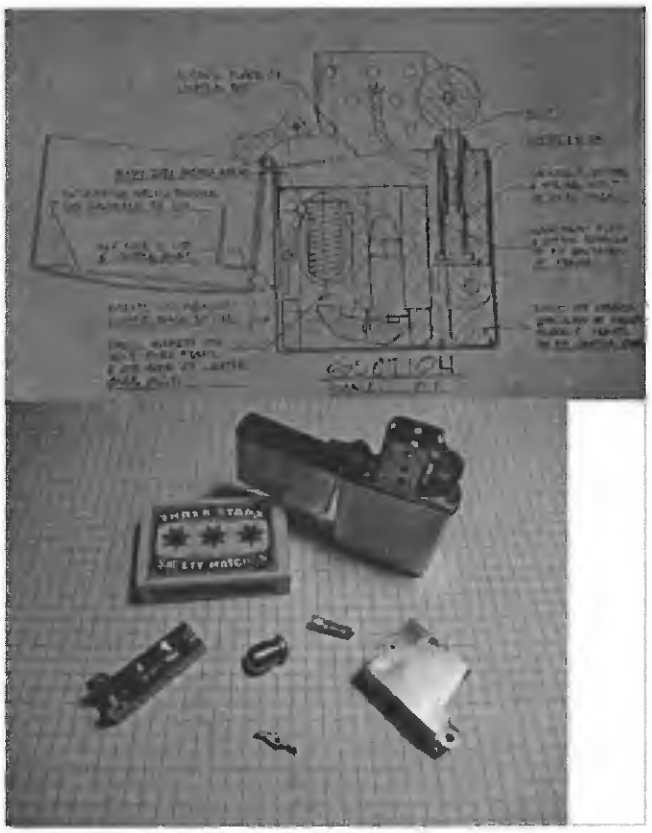
***

SUBJECT ACCOUNT 1 03/06/2025 8:52:26pm PST: need to kill someone by handcuffing them in their own car and putting a brick on the accelerator into a lake

37. A review of the messages also revealed that on March 1, 2025, **SUBJECT ACCOUNT 1** shared with the Victim detailed schematics of how to construct homemade firearms, including what appears to be a semi-automatic weapon with an extended magazine, a "pipe pistol", and a lighter designed to shoot a single round as well as a photograph of a lighter with parts removed. The images below were also sent:







38. Between March 2 and 3, 2025, **SUBJECT ACCOUNT 1** and the Victim discussed firearms, including weapons that KUPPUSAMY claims to have purchased and manufactured. Notably, during this time frame, the Victim was posting messages regarding her friendship with

"Sam Rupnow" including a post that stated "oomf shot up her school while i was in the psych ward at least wait for me to get out." I know that Natalie Samantha Rupnow was a 15-year-old student who committed a shooting attack at Abundant Life Christian School in Madison, Wisconsin, that resulted in the deaths of three people and which injured six others. It appears that in response to these posts, **SUBJECT ACCOUNT 1** sent the Victim the following messages, in which they discuss plans and intentions to commit violent acts and KUPPUSAMY cautions the Victim to be careful about discussing her plans to commit violent acts because law enforcement may be present in their social media chats:

> **SUBJECT ACCOUNT 1** - 03/02/2025 7:15:14pm PST: dont say the shit you say w me regarding plans intentions etc there are 1000% informants in tcc circles trust no one but me
>
> **SUBJECT ACCOUNT 1** - 03/02/2025 7:17:32pm PST: like regardless of what ur doing who ur talking to at least dont get us both jailed
>
> **SUBJECT ACCOUNT 1** - 03/02/2025 7:19:44pm PST: what's the plan if someone connects this to ur identity btw
>
> **SUBJECT ACCOUNT 1** - 03/02/2025 7:21:49pm PST: the gun pic is fine i think if it's not up on fb or something but the other two id strongly advise u to delete, post without face if u really want to
>
> **Victim Account 2** - 03/02/2025 7:44:17pm PST: https://www.quadrato309.com/2019/07/introduction-to-system-q309.html?m=1
>
> **SUBJECT ACCOUNT 1** - 03/02/2025 8:30:07pm PST: slitting ur throat and poasting it on story if u talk to any of ur mutuals btw #iloveyou
>
> **Victim Account 2** (18042991273) - 03/02/2025 9:13:33pm PST:

SUBJECT ACCOUNT 1 - 03/02/2025 9:16:01pm PST: u can buy some german guns but it's like nice car money

SUBJECT ACCOUNT 1 - 03/02/2025 9:16:42pm PST: bruh it's going 10-15k for SEMI

SUBJECT ACCOUNT 1 - 03/02/2025 9:17:32pm PST: insane it must be super rare

SUBJECT ACCOUNT 1 - 03/02/2025 9:17:40pm PST: stg44 u can get more easily in full auto

SUBJECT ACCOUNT 1 - 03/02/2025 9:17:55pm PST: i buy [diminutive of Victim's name] all the guns and i build some too

SUBJECT ACCOUNT 1 - 03/03/2025 9:26:49am PST: if i gifted u a gun would ur mom take it

Victim Account 2 - 03/03/2025 9:27:02am PST: she wouldn't find it

Based on your affiant's training and experience, I believe that KUPPUSAMY and the Victim are discussing the unlawful conversion of a firearm to fully automatic when he tells her that a "stg44" can more easily be obtained in "full auto." Based on my training and experience, I know that a StG 44 is a German assault rifle developed during World War II.

39. During that same conversation, KUPPUSAMY, using **SUBJECT ACCOUNT 1** and the Victim discuss, among other things, Robert Bowers (the perpetrator of the Tree of Life Synagogue attack), "fbi attention on Terrorgram", and miss gorehound, with KUPPUSAMY stating, "i wish miss gorehound didnt get arrested i wouldve introduced u."[4]

Evidence of Risk of Destruction of Evidence

40. As noted above, KUPPUSAMY, using **SUBJECT ACCOUNT 1** and the Victim previously discussed deleting incriminating communications between them. I have reviewed additional messages between KUPPUSAMY, suing **SUBJECT ACCOUNT 1** and the Victim which indicates the two created communication accounts and shared the usernames and passwords, thus allowing either party to access the content and be in a position to delete evidence.

41. For instance, on January 20, 2025, KUPPUSAMY, using **SUBJECT ACCOUNT 1,** advised the Victim that he had created a new email account and shared the password: The email referenced KUPPUSAMY's moniker "doomerbrown" and the password included a diminutive of the Victim's name.

42. Similarly, on the same date, the Victim notified KUPPUSAMY through **SUBJECT ACCOUNT 1** that she had created at least one a new account on a yet to be determined application and provided the username along with a screenshot of the account creation displaying the password:

[4] On September 9, 2024, the Department of Justice charged Dallas Humber, 34, of Elk Grove, California, and Matthew Allison, 37, of Boise, Idaho — leaders of the Terrorgram Collective, a transnational terrorist group —in a 15-count indictment for soliciting hate crimes, soliciting the murder of federal officials, and conspiring to provide material support to terrorists. Humber used the moniker "miss gorehound." According to the indictment, Humber and Allison are the leaders of the Terrorgram Collective, a transnational terrorist group that operates on the digital messaging platform Telegram, where it promotes white supremacist accelerationism: an ideology centered on the belief that the white race is superior; that society is irreparably corrupt and cannot be saved by political action; and that violence and terrorism are necessary to ignite a race war and accelerate the collapse of the government and the rise of a white ethnostate. *See https://www.justice.gov/archives/opa/pr/leaders-transnational-terrorist-group-charged-soliciting-hate-crimes-soliciting-murder*

Victim Account 1: username is rudysprincess

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ENGAGE IN CHILD PORNOGRAPHY OFFENSES

43. Based on my education, training, and experience, as well as information obtained from other experienced law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, access, and possess child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to

children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children. Many individuals who collect child pornography also collect other sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not meet the legal definition of child pornography, but which nonetheless fuel their sexual fantasies involving children.

d. Based upon your Affiant's training and experience, your Affiant knows that many users who possess, receive, distribute, or produce child pornography transfer these files between their different storage devices and online accounts, such as the **SUBJECT ACCOUNTS**, for reasons that include concealing the files, storing them in one account versus another account, or having the files accessible to the user on multiple devices. I am aware of cases where users transfer child pornography files between devices and/or online accounts, and commonly use email or other online messaging accounts to complete the transfer, such as the **SUBJECT ACCOUNTS**.

BACKGROUND CONCERNING INSTAGRAM[5]

44. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

[5] The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," https://privacycenter.instagram.com/policy/; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

45. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

46. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

47. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

48. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

49. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

50. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

51. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

52. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

53. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

54. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

55. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

56. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

57. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

58. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

59. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

60. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

61. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

62. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

63. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

64. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, voice messages, photos, videos, and documents]] are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

65. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers

or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

66. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, stored communications, contact lists, photos, and videos can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

68. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

69. Based on the forgoing, I request that the Court issue the proposed search warrant.

70. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc. Because the warrant will be served on Meta Platforms, Inc.,

who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

71. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

/s/ John A. McKinley
John A. McKinley
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this day of March, 2025.

PAMELA A. CARLOS
Digitally signed by PAMELA A. CARLOS
Date: 2025.03.19 10:29:45 -04'00'

HON. PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Instagram accounts:

UID 59803352284

UID 72514323885

that are stored at the premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered at 1 Meta Way, Menlo Park, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period May 11, 2023 to present:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata,;

C. All content, records, and other information relating to communications sent from or received by the account, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Instagram users, including but not limited to:

1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account; and

F. All location information, including location history, login activity, information geotags, and related metadata.

Meta is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. INFORMATION TO BE SEIZED

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of Title 18 United States Code 875(c) (interstate threats), Title 18, United States Code, Section 2251(sexual exploitation of children known colloquially as production of child pornography), Title 18, United States Code, Section 2252 (violations, attempt to violate, and conspiracy to violate, manufacturing, possession, receipt, or distribution of child pornography) and those violations involving ANIRUTH KUPPUSAMY, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications between the account user and other people relating to planning, collaborating, conspiring, assisting (knowingly or unknowingly), executing, concealing, or covering up the commission of the SUBJECT OFFENSES, including records that help reveal their whereabouts;

b. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

c. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

d. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

e. Evidence relating to or suggesting a sexual interest in minors, including but not limited to Victim 1;

f. Communications with or concerning Victim 1;

g. Evidence concerning the enticement or sexual exploitation of minors;

h. All visual depictions of, or evidence concerning, minors engaged in sexually explicit conduct or self-harm,

i. All evidence pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed;

j. Evidence concerning minors or potential minors involving sexual topics or in an effort to seduce or to meet a minor.

k. Evidence concerning threats to commit acts of violence, mass casualty attacks, including evidence regarding ANIRUTH KUPPUSAMY'S state of mind;

l. Evidence concerning firearms, ammunition, explosives, terrorist or mass casualty attacks, or racially motivated violent extremism and/or nihilistic violent extremism;

m. Evidence regarding the commission of an act of violence or other plans or reasoning justifying an act of violence;

n. Evidence bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, § 2256.

o. Evidence relating to the identification of persons who either (i)collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the SUBJECT OFFENSES; or (ii) communicated about matters relating to the SUBJECT OFFENSES, including records that help reveal their whereabouts; and

p. Evidence regarding other accounts or platforms that could be used to commit the SUBJECT OFFENSES.