EFILED
9/9/2024 7:28 PM
Julie J. Mayer
CIRCUIT CLERK
CHRISTIAN COUNTY
By: JV

IN THE CIRCUIT COURT OF THE FOURTH JUDICIAL CIRCUIT
CHRISTIAN COUNTY, ILLINOIS

THE PEOPLE OF THE STATE OF ILLINOIS, Plaintiff,	
vs.	Case No. 2022-CF-196
TODD E. DAUGHERTY, Defendant.	

MOTION TO SUPPRESS EVIDENCE ILLEGALLY SEIZED

Todd E. Daugherty, by his attorney, Tiffany Senger, respectfully requests pursuant to the Fourth Amendment to the US Constitution, Article I Section 6 of the Illinois Constitution, and 725 ILCS 5/114-12(a)(2), that this Court suppress all evidence illegally seized as a result of two warrants, and in support of his Motion, states the following:

INTRODUCTION

In this case, police obtained a search warrant for every electronic device in the home Daugherty shared with his parents. This warrant was based on a threat made on an internet message board without first establishing the post was made by Daugherty. After it became clear it was not Daugherty who made the threatening post, police handed off the devices to the FBI to conduct a search, despite having neither probable cause nor a valid warrant. Then, almost two years after this warrantless search uncovered suspected contraband, the FBI sought a second warrant that laundered the prior illegal acts of local police and the FBI by claiming that the contraband was found in plain view while executing a valid state warrant. These numerous constitutional and statutory violations require suppression.

FACTS

On March 16, 2018, an anonymous person using the name "Mark" provided a tip to the FBI stating "I don't know if this is real or not but this guy is crazy with numerous arrests (Todd Daugherty) but he just posted to a message board. 'FUCK YOU YOU STALKING MOTHER FUCKERS. I'LL SHOW YOU WHO IS AUSTIC. I'LL GO TO FUCKING MEMORIAL ELEMENTARY SCHOOL AND MAKE SANDY HOOK LOOK LIKE A SUNDAY SCHOOL PICNIC.'" FBI 1057 9-SI-2610873 *See FBI 1057.* (Exhibit A). The statement was conspicuously posted under username "Todd Daugherty N90GL" (N90GL is Daugherty's ham radio call sign) and included two photos of Daugherty holding a

handgun. Although this anonymous tipster provided their location as the United States, their internet protocol ("IP") address[1] resolved to France, likely because the tipster was utilizing the Tor network[2] or a proxy server[3] to mask their identity and physical location. *See id.* No investigation was made into the anonymous tipster.

Further calling into question the reliability of the tip is the nature of the site on which it was posted, www.hateandflame.com. This website is full of users posting anonymously, under false names, and impersonating one another or historical figures. *Hateandflame.com*, March 6-20, 2018 (Exhibit x). For example, some of the usernames include: "Ernist Hemingay", "Buddy Che Hinton"[4], "Harry Tard Snortz", "Loyd Davies, Timelord"[5], "THE PINKLE WHEEZLE", "STAINLESS STEEL FUCKBOT" or just ".". *Id.* Furthermore, people on the forum openly discuss doxing[6], spreading lies about users they are sparring with on the website, and victimizing one another in real life. *Id.* For example, on March 10, 2018, one user, "Hal Turner", indicates that someone sent "hookers and pizza" to his home without his consent. *Id.* Another user replies that the hookers and pizza were supposed to be sent to "Toad's place" (Toad is a name used on the site to belittle Todd Daugherty). *Id.* Another user "NewsGuy, Real Deal" posted "everytime that N90GL files a complaint against the board I write he neighbors to tell them that he is a sexual predatory to watch their kids." *Id.* The forum is also rife with claims that users are posting under fake names and using proxy servers to hide their identities and physical location. *Id.* In short, the usernames on hateandflame.com are obviously unreliable, the atmosphere clearly toxic, and users are openly engaging in tactics designed to harm one another's reputations in real life. *See id.* Furthermore, the individuals on the forum clearly had extensive knowledge of Todd Daugherty's personal life. They were aware of and used his ham radio call sign and his twitter handle. *See id.* A user operating under the name "Tom Randal" posted his home address. *Id.* They taunted him for collecting Japanese dolls. *Id.* The user "Loyd Davies, Timelord" accused him of plagiarism using his ham radio call sign, N90GL. *Id.* All of this was readily apparent from posts made on the days leading up to March 17, 2018.

---

[1] An IP or internet protocol address is a numerical label assigned to a device(modem) connected to the internet. *See Wikipedia IP address*, https://en.wikipedia.org/wiki/IP_address (last viewed on March 21, 2024). These can be used to identify and/or geolocate a user connecting to a website.
[2] Tor stand for The Onion Router. This is free, open source, software developed by the United States Naval Research Laboratory which enables anonymous communications by allowing individuals to obscure their internet protocol or IP address. *See Wikipedia Tor(network)*, https://en.wikipedia.org/wiki/Tor_(network)#cite_note-9 (last viewed on March 21, 2024).
[3] A proxy server acts as an intermediary between a user and a webpage and similarly to Tor it can be used to mask the true origin or IP address of a user. *See Wikipedia Proxy server*, https://en.wikipedia.org/wiki/Proxy_server (last viewed on March 21, 2024).
[4] This is a reference to Buddy Hinton, a fictional bully on the television show "The Brady Bunch." *See Fandom Buddy Hinton*, https://bradybunch.fandom.com/wiki/Buddy_Hinton (last viewed on April 16, 2024).
[5] This is a reference to the Loyd-Davies position which was popularized by Oswald Lloyd-Davies and utilized for colorectal surgery. https://en.wikipedia.org/wiki/Lloyd-Davies_position (last viewed on April 16, 2024).
[6] "Doxing or doxxing is the act of publicly providing personally identifiable information about an individual or organization, usually via the Internet and without their consent." *See Wikipedia Doxing*, https://en.wikipedia.org/wiki/Doxing (last viewed on March 26, 2024).

On March 17, 2018, officers Dickey and Thomason visited with Daugherty at his home regarding the threatening post bearing his name and photograph. *See Report of Officer C. Dickey*, at pg. 1 (Exhibit B). After being transported to the Taylorville Police Department, Daughtery denied making the post, explained to them that someone had been impersonating him online, and stated that he personally did not post on hateandflame.com. *Id.* He also explained he believed a user "squashtoad" was the one impersonating him. *Id.* Thomason recognized the photographs on the post of Daugherty holding a gun from a previous incident, and Daugherty explained he had previously posted them on a blog and so they were publicly available. *Id.* Despite the fact that the identity of the person who reported the threat to the FBI could not be confirmed, and that there was no evidence that Daugherty was responsible for the post, he was arrested. No investigation was made into "squashtoad" or the very likely possibility that someone had simply posted using Daugherty's name as a form of harassment or swatting.[7]

Subsequent investigation further supported Daugherty's claims that the posts were made by someone impersonating him. On March 18, 2018, Todd Daugherty's brother Jeremy Daugherty contacted the Taylorville Police Department and provided screenshots and links to hateandflame demonstrating that individuals were making posts purporting to be Todd Daugherty while he was in police custody. *See Jeremy Daugherty emails*, (3/18/2018) (Exhibit C). On March 19, 2018, Jeremy Daugherty contacted FBI special agent Alaina Arnold to report that his brother had been set up by someone,likely named Bryan Crow, who had been harassing his brother online and over ham radio communications for years. *See SA Arnold* 302, 7/2/18 (Exhibit D). Arnold then called the State's Attorney, Mike Havera, who indicated that he had spoken to a Canadian man named Karl Madera who also said Todd Daugherty was being set up by someone named Bryan Crow. *Id.* Havera informed Arnold he was waiting on further information before dropping the charges. *Id.*

On March 19, 2018, police obtained a warrant for Computer Techniques Inc. (hereinafter the "CTI Warrant") (the internet service provider for Daugherty) for "any and all electronic data transfers and/or records…" related to Daugherty's account. They obtained these records on the same day. *Warrant Return*, 18-MR-37 (Exhibit E). The records showed Daugherty's MAC address to be EC:4F:82:29:B4:03 and his IP address was 72.9.123.215. *Id.*

[7] "Swatting is a criminal harassment act of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into sending a police or emergency service response team to another person's address. This is triggered by false reporting of a serious law enforcement emergency, such as a bomb threat, murder, hostage situation, or a false report of a mental health emergency, such as reporting that a person is allegedly suicidal or homicidal and may be armed, among other things." *Wikipedia Swatting*, https://en.wikipedia.org/wiki/Swatting (last viewed on March 26, 2024).

On March 21, 2018, officer Christian Nelson obtained a warrant for Daugherty's home (hereinafter the "Device Warrant") to seize "any and all computers… including but not limited to hard disk drives, floppy disks, compact discs, DVD's USB devices… and any and all information and data stored in the form of magnetic or electronic coding on computer media or media capable of being read by a computer…" *Search Warrant*, 18-MR-40 (Exhibit F). The Device Warrant further provided "authority to analyze and search any magnetic or optical media seized for the relevant evidence as outlined in this search warrant…" The Device Warrant did not mention what electronic evidence or data the police could seize pursuant to this warrant, nor did it name the crime for which the police had probable cause. Instead, it allowed an unlimited search of all of the devices. Furthermore, it did not expressly incorporate the affidavit into the warrant terms. Pursuant to this warrant, police seized fifteen items: a black and blue Seagate hard drive, serial number NA7DWTK4; one Seagate 1TB hard drive, serial number 5vPG12DV, a Cyperton computer tower, serial number GA-78LMT-USB3; a Compaq computer, serial number CNH4520P00; a Gateway 7320 laptop, serial number N3451-710-03782; a Gateway computer, serial number PTE590XD01960595B2700; three DVD-Rs, one CDR, one CTI router, and four assorted USB drives. *Warrant Return*, 18-MR-40.

The affidavit for the Device Warrant stated that the "FBI Springfield office received a tip that Todd E. Daugherty (M/W D.O.B. 07/05/1968 posted on internet social forum Hateandflame.com the following comment 'FUCK YOU YOU STALKING MOTHER FUCKERS. I'LL SHOW YOU WHO IS AUSTIC. I'LL GO TO FUCKING MEMORIAL ELEMENTARY SCHOOL AND MAKE SANDY HOOK LOOK LIKE A SUNDAY SCHOOL PICNIC.'" The affidavit also stated that the post was "issued by someone" with the username "N90GL", which was Daugherty's ham radio call sign. The affidavit also stated that his "profile picture" and the post included the same photos of Daugherty holding a handgun. No other explanation was provided about how they knew that was his profile. No explanation was provided about the website, how one could set up a profile, make posts, or about its user base, or its contents. No IP address was provided linking Daugherty to the post. Furthermore, the affidavit did not explain that the tipster intentionally obscured their identity through the Tor network. Nor did the affidavit explain that multiple people indicated that Daugherty had been set up. Significantly, the affidavit did not even include that posts continued to appear under his name while he was in custody and had no access to electronic devices. Instead, the Device Warrant affidavit contained conclusory assertions that it was Todd Daugherty's account that made the post.

On March 29, 2018, officer Christian Nelson obtained warrant for NFSN inc., the company hosting the website www.hateandflame.com (hereinafter the "Hateandflame Warrant"). *Search Warrant*, 18-MR-45 (Exhibit G). In response to that warrant, police learned that neither Daugherty's IP address nor his MAC address had been used to post on hateandflame.com during the time of the threatening post. *Warrant Return*, 18-MR-45 at p. 6-7 (Exhibit G). Instead, they learned that the IP address responsible for the threatening post was associated with the TOR network and was therefore anonymous. *Id.* Further police learned that "90% [of people posting on the website] use tor or proxy sites…No registration is required. No email address is checked. Impersonation is part of the status quo for the board… anybody can post as anybody else." *Id.* at p. 5.

On April 4, 2018, despite knowing that they definitively lacked probable cause to search the devices they seized from Mr. Daugherty's home, the Taylorville Police Department enlisted the FBI to conduct search of the devices that remained in their custody. *See SA Arnold* 1057, 4/6/18. On April 11, 2018, Arnold seized the devices from the Taylorville Police Department and placed them in an FBI storage facility. *Chain of Custody Form*, 343G-SI-2610873, pg. 1-5. On April 16, 2018, the State's Attorney filed a motion to dismiss the charges against Daugherty. *See Motion to Dismiss*, 18-CF-62 (April 16, 2018) (Exhibit H). The motion was based on the following facts: (1) the website used to disseminate the threat did not require any login credentials, (2) while Daugherty was in custody more messages appeared under his name, (3) posts on the website were made by people impersonating "judges, the president, and other such individuals" (4) Daugherty's internet activity have shown nothing to implicate him in the case. *Id.* The court granted the motion and specifically stated "[a]ny warrants or summonses previously issued are hereby quashed *Order of Dismissal* (April 16, 2018) (Exhibit I). The case was officially dismissed on the record and all warrants quashed by 11:32 a.m. *See People v. Daugherty* 18-CF-62, Tr. (April 16, 2018) (Exhibit J). Daugherty was released the same day. Upon his release from jail on April 16, 2018 and within the following weeks, Daugherty and his father both demanded return of his devices from the Taylorville Police Department and the State's Attorney. However, none of the devices were returned, nor were they given any formal denial of their request or a justification for the police retaining the devices.

Meanwhile, on April 16, 2018, as the case against Daugherty was being dismissed and the warrants quashed, FBI agent William O'Sullivan removed the devices from evidence and conducted an inventory. S*ee CART Examination Notes* 343G-SI-2610873 pg. 1 (Exhibit K). Three days after the warrant was quashed he began the process of extracting the devices pursuant to the invalid Device

Warrant. *See Id.; see also Chain of Custody Form*, 343G-SI-2610873, pg. 1-5 (Exhibit L). On April 23, 2018, a week after the warrant had been quashed and therefore was no longer valid, O'Sullivan began to search the device. *See CART Examination Notes* 343G-SI-2610873 pg. 3 (Exhibit K). During that warrantless search, O'Sullivan found what he noted what appeared to be a computer-generated image of a minor child with an adult male penis in his mouth. *Id.* Approximately two years later, despite no additional evidence against Daughtery emerging, the evidence seen during this warrantless search would be used as the basis for a federal search warrant. *See Warrant Application*, 20-MJ-3023 (Exhibit M).

On March 2, 2020, Special Agent Anthony Wright applied for a warrant (hereinafter the "Federal Warrant") to search the following eight devices: a black and blue Seagate hard drive, serial number NA7DWTK4; a Cyperton computer tower, serial number GA-789MT-USB3[8]; a Compaq computer, serial number CNH4520P00; a Gateway 7320 laptop, serial number N3451-710-03782; and four assorted USB drives. The affidavit for the Federal Warrant stated only that the devices were in the "lawful possession of the FBI" because they were seized from Daugherty based on a search warrant that allowed for a "search and seizure of any and all computers…" *Id.* at ¶ 6. The affidavit then stated that "Examiner William O'Sullivan found suspected child pornography on the black and blue Seagate desktop hard drive bearing serial number NA7DWTK4…" specifically, a "visual depiction of a three to five-year-old with an adult male's penis in his mouth." *Id.* at ¶ 9. The affidavit did not explain that O'Sullivan recognized it to be a computer-generated image. *See id.* Nor did the affidavit provide any other relevant information about the state case. Specifically, the affidavit omitted: (1) that the case against Daugherty had been dismissed for a lack of probable cause, (2) that the search by O'Sullivan had been conducted after the dismissal of the case and the quashing of the warrant, and (3) a copy of the allegedly valid Device Warrant upon which that search was conducted.

ARGUMENT

Suppression of suspected evidence gathered during the search of Daugherty's property stemming from the Federal Warrant is required by Fourth Amendment to the US Constitution, Article I Section 6 of the Illinois Constitution, and 725 ILCS 5/114-12(a)(2). Suppression is required because: (1) the device warrant was patently unconstitutional, (2) Agent O'Sullivan conducted a warrantless search of the devices in question, (3) the federal warrant contains material misstatements and omissions regarding the device warrant and the case against Daugherty, (4) Daugherty is entitled to a hearing on the

[8] Note that this appears to be the same computer that is listed in Warrant return 18-MR-40 under serial number GA-78LMT-USB3.

execution of the search, and (5) the federal warrant was not sought within a reasonable time period of the FBI's warrantless search. Accordingly, all suspected evidence obtained against Daugherty as the result of the Federal Warrant must be suppressed as the fruits of the multiple constitutional violations.

I. The Device Warrant Was Patently Unconstitutional

The Device Warrant was invalid because it lacked probable cause and was an unconstitutional general warrant. Moreover, in obtaining that warrant, the government intentionally omitted material facts that demonstrated that they lacked probable cause.

a. The Device Warrant Lacked Probable Cause

The Device Warrant lacked probable cause because it was based on the statement of an anonymous informant whose credibility was completely uncorroborated by subsequent investigation. Instead, the warrant affidavit rests on the fact that a threatening online post contained publicly available information—Daugherty's name, ham radio signal, and a photograph.

The Fourth Amendment to the United States Constitution protects the right of the people against unreasonable searches. Illinois adopted the same protections for its people in Article I, Section 6 of the Illinois Constitution. Evidence obtained as the result of an illegal search or seizure is inadmissible and must be suppressed. 725 ILCS 5/114-12(a)(2).

The Supreme Court of Illinois adopted the "totality of the circumstances" test to determine the sufficiency of probable cause to issue a warrant under the Illinois Constitution's Article I, Section 6. *People v. Tisler*, 103 Ill. 2d 226, 245 (1984). However, the court still employs the prongs of the *Aguilar-Spinelli* test as a useful tool in determining whether an informant's statement gives rise to probable cause. *See id.* This is consistent with the Supreme Court's decision in *Gates* which explained that "an informant's "veracity," "reliability" and "basis of knowledge" are all highly relevant… and "should be understood simply as closely intertwined issues that may usefully…" be used by courts to determine probable cause. *Illinois v. Gates*, 462 U.S. 213, 230 (1983). *Aguilar-Spinelli* requires a finding that: (1) the informant was reliable; and (2) that the informant had a sufficient basis of knowledge. *See Spinelli v. United States*, 393 U.S. 410 (1969); *Aguilar v Texas*, 378 U.S. 108 (1964).

The affidavit in this case fails both prongs of *Aguilar-Spinelli*. Although the affidavit explained that the FBI received a tip, it did not establish that the individual who made that tip was a known or reliable informant. Instead, it merely stated that the "FBI Springfield office received a tip…" that it was Todd E. Daugherty. Furthermore, it did not establish the individual's basis of knowledge that the post was made by Todd Daugherty as opposed to someone using his name and information to impersonate

him. For example, it did not state that the tipster was a website administrator who had access to log files showing the user's connection to Todd Daugherty. Nor did it state the tipster was a friend or acquaintance who overheard him discussing the post. Therefore, neither prong of *Aguilar-Spinnelli* was met.

For similar reasons the Device Warrant fails the Gates "totality of circumstances" test. *See Gates*, 462 U.S. at 230. Neither probable cause nor reasonable suspicion can be based solely on an anonymous tip that merely provides the static details of a suspect's life along with an allegation of criminal conduct. *See People v. Yarber*, 279 Ill.App.3d 519, 529 (1996). This is true even when target has a prior criminal conviction. *See id.* at 523 (police confirmed Yarber's race, height, and weight through a criminal background check); *see also United States v. Johnson*, 427 F.3d 1053, 1057 (7th Cir. 2005).

In *Florida v. J.L.*, an anonymous caller reported that a young black male was standing at a bus stop wearing a plaid shirt and carrying a gun. *Florida v. J.L.*, 529 U.S. 266, 268 (2000). This anonymous tip was held to be insufficient even where police corroborated the location of the defendant and the type of clothing he was wearing. *Id.* at 272. This is because "[s]uch a tip …does not show that the tipster has knowledge of concealed criminal activity." *Id.* In *Yarber*, the fifth district extended that logic to a case where the anonymous tipster claimed that her best friends regularly bought cannabis from a man named Samuel Yarber and provided a physical description of Yarber, his address, and his place of employment. *Yarber*, 279 Ill.App.3d at 522. Police confirmed this information and stopped Yarber as he was leaving a train station. *Id.* at 521-522. However, the court found "reasonable and articulable suspicion requires more than corroboration of innocent details. Without verification of any other portion of the informant's tip, for all the police knew, Samuel Yarber was the victim of a malicious prank." *Id.* at 529. This holding is consistent with both federal and Illinois precedent. *See e.g. United States v. Lopez*, 907 F.3d 472, 482 (7th Cir. 2018) (when a tipster is unknown officers "must conduct and rely upon independent investigation to corroborate a tip before seizing a person."); *People v. Lopez*, 2018 IL App (1st) 153331 (App. Ct. 1st Dist. 2018) (insufficient corroboration of an anonymous tip).

The *Yarber* decision is controlling here. Here, Daugherty was linked to the account posting the threat by an anonymous tipster. The affidavit did not establish that the tipster was known to police or in any way reliable. To the contrary, they utilized a computer network designed by the U.S. Naval Research Laboratory to ensure they could not be traced. Although police confirmed that the user posting the threat used Daugherty's name, likeness and call sign, this was all publicly available static

information. As the court pointed out in *Yarber*, "[w]ithout verification of any other portion of the informant's tip, for all the police knew, [Todd Daugherty] was the victim of a malicious prank." *Yarber*, 279 Ill.App.3d at at 529. The questionable value of the publicly available information in linking him to the account was further diminished by the affidavit's references to the fact that Daugherty told police he did not post on the site and was being "set up" by someone who was trying to have his ham radio license suspended by the FCC. The other information in the affidavit was merely gratuitous information about Daugherty's past conviction, for an unrelated threat on law enforcement and does nothing to establish a reliable link between him and the threatening post.

There are many ways in which an online post can be linked to a suspect. First, and by far the most common first step in any investigation is to connect someone through an IP address. To be sure, using an IP address to establish probable cause is not without problems. *See e.g.* Aaron Mackey et. Al. *Unreliable Informants: IP Addresses, Digital Tips and Police Raids*, pg. 6 (September 2016). However, courts have almost universally held that IP addresses are sufficient to establish probable cause to search the residence they are connected to. *See e.g. United States v. Featherly*, 846 F.3d 237, 240 (7th Cir. 2017); *United States v. Vosburgh*, 602 F.3d 512, 526–27 (3d Cir. 2010) (collecting cases from the Fifth, Sixth, Eighth, Ninth, and Tenth Circuits); *United States v. Thomas*, No. 5:12–CR–37 (CR), 2013 WL 6000484, at *24 (D.Vt. Nov. 8, 2013), aff'd, 788 F.3d 345 (2d Cir.2015); *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007); *United States v. Morel*, 922 F.3d 1 (1st Cir. 2019). Here, police obtained the Device Warrant before engaging in this critical first step.

Police can also link people to online accounts through circumstantial evidence, however, that evidence must not consist solely of a few pieces of publicly available information. *See e.g. United States v. Vayner*, 769 F.3d 125 (2d Cir. 2014). In *Vayner*, the Second Circuit, while acknowledging that, "[t]he bar for authentication of evidence is not particularly high," held that a social media profile was not properly authenticated. *Id.* There the government introduced a printout of a "VK" profile (described as the Russian equivalent of Facebook) that a special agent printed off the internet the day of his testimony. *Id.* The Second Circuit overturned the Eastern District Court, finding that although "information about [the defendant] appeared on the VK page: his name, photograph, and some details about his life consistent with [the cooperating witness'] testimony about him… there was no evidence that [the defendant] himself had created the page or was responsible for its contents." *Id.* at 132. "Other than the page itself, moreover, no evidence in the record suggested that [the defendant] even had a VK profile page, much less that the page in question was that page. Nor was there any evidence that identity

verification is necessary to create such a page with VK, which might also have helped render more than speculative the conclusion that the page in question belonged to [the defendant]." *Id.* at 133. The court hinted that the government's witness had both the motive and ability to create the page himself. Specifically, the court stated, "all the information contained on the VK page allegedly tying the page to [the defendant] was also known by [the cooperating witness] and likely others, some of whom may have had reasons to create a profile page falsely attributed to the defendant." *Id.* at 132.

Here, similarly, while the post had Daugherty's name, call sign, and photograph, all that information was publicly available. A simple check of the website logs could (and in fact later did) confirm whether there was a possibility that someone else was behind the post—especially given the statement by Daugherty that he was being set up. Similarly, while probable cause, like authentication, is not a high bar; it does impose some requirements of due diligence on the part of the government before they obtain a warrant to conduct a search of every electronic device in someone's home. Simply restating information posted on a website, like www.hateandflame.com, and asserting they were done by someone who denies posting them is not enough. This is especially true where the affidavit contains no information about what credentials an individual must supply in order to access the website, what the policies on impersonating others are, or how they are enforced.

Because the Device Warrant relied on an uncorroborated tip by an anonymous informant and static, publicly available information, it was not supported by probable cause and must be suppressed.

b. The Device Warrant Was an Unlawful General Warrant

The Device Warrant was an unconstitutional general warrant because it was completely lacking in particularity and as a result an overbroad[9] general warrant of the type "abhorred by the colonists" that lead to the creation of the Fourth Amendment and the particularity clause. *Coolidge v. New Hampshire,* 467, 91 S.Ct. 2022, 2038 (1971); *see also Carpenter v. United States*, 138 S.Ct. 2206, 2239-2240 (2018). Specifically, the warrant here failed to identify the data to be seized from the electronic devices or even the crime for which the police were required to restrict its search.

The amount of particularity required in a warrant can fluctuate depending on the nature of the case, evidence sought, and information known to police. *See Andresen v. Maryland,* 427 U.S. 463, 481 n. 10 & 11 (1976); *United States v. Strand*, 761 F.2d 449, 453 (8th Cir. 1985); *United States v. Regan*, 706 F.Supp. 1102, 1113 (S.D.N.Y.1989). However, one thing is clear—warrants must, at a bare

[9] While breadth and particularity are two distinct legal issues ordinarily analyzed separately, see *United States v. Zemlyansky*, 945 F.Supp.2d 438 (2013), the Device Warrant is completely devoid of any particularity thereby making this a distinction without a difference in this matter.

minimum, state the crimes for which evidence is being sought. *United States v. Cioffi,* 668 F.Supp.2d 385, 390 (E.D.N.Y 2009); *United States v. Otero,* 563 F.3d 1127, 1132 (10th Cir. 2009); *United States v. Rosa*, 626 F.3d 56 (2d Cir. 2010); *United States v. Zemlyansky,* 945 F.Supp.2d 438 (2d Cir. 2013); *United States v. Riccardi*, 405 F.3d 852 (10th Cir. 2005); *United States v. Clough*, 246 F.Supp.2d 84 (D.M.E. 2003); *United States v. Mink*, 613 F.3d 995 (10th Cir. 2010); *United States v. Hunter,* 13 F.Supp.2d 574 (D. V.T. 1998); *cf. United States v. Christie*, 717 F.3d 1156 (10th Cir. 2013); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992); *United States v. Romain,* 678 Fed.Appx. 23 (2d Cir 2017). This means the specific crime for which probable cause is found and not just a category of crime, as "[a]n unadorned reference to a broad federal statute does not sufficiently limit the scope of a search warrant." *United States v. Leary*, 846 F.2d 592, 602 (10th Cir.1988); *see also United States v. Spilotro*, 800 F.2d 959, 965 (9th Cir.1986) (finding that search warrant violated particularity requirement where only limitation on scope of search was items to be seized had to be evidence of violation of one of thirteen statutes); *United States v. Roche*, 614 F.2d 6, 8 (1st Cir.1980) (finding that search warrant violated particularity requirement where only limitation was reference to the mail fraud statute); *Cassady v. Goering*, 567 F.3d 628, 636 (10th Cir.2009); *United States v. Clark*, 31 F.3d 831, 836 (9th Cir.1994). This is especially true where the statute is broad or language like "any or all data" accompanies the restriction. *United States v. Winn*, 79 F. Supp. 3d 904, 919 (S.D. Ill . 2015). This rule applies because, "whatever new challenges computer searches pose in terms of particularity, it is always necessary – and hardly onerous – to confine any search to evidence of particular crimes." *Cioffi*, 668 F. Supp. 2d at 392.

The search here was unlimited in that it allowed a search of any computer or computer storage device for the following:

> ***any and all*** evidence of dominion and control over the computer, specifically, ***but not limited to***, a computer possessing MAC address "EC:4F:82:29:84:03" or IP address "72.9.123.215"; peer to peer file trading software; any and all information pertaining to dates and times of access to the computer; any and all information pertaining to internet searches pertaining to posts regarding threats of violence directed towards schools or public officials; records and other items which evidence ownership or use of computer equipment found in the above residence; including but not limited to sales receipts, bills for internet access and handwritten notes, records evidencing occupancy or ownership of the premises described above including but not limited to utility and telephone bills, mail envelopes or address correspondence.

Search Warrant, 18-MR-40 (emphasis added) (Exhibit F).

This does not limit the search to evidence of the threatening post. The language specifically "includes but is not limited to" the subsequent clauses which provide an illustrative but non-exclusive list of what the government may search for and seize. *See In Matter of Black iPhone 4*, 27 F.Supp.3d 74 (E.D.D.C. 2014) (Lists are illustrative rather than exclusionary where they include precursors like "[a]ll records…including" and then list different types of data). Lists of evidence that are illustrative rather than exclusionary or exhaustive should be heavily scrutinized. *United States v. Wey*, 2017 WL 257402 at *21-22 (S.D.N.Y. 2017). This is because those phrases "make the seizure list broader than the categories specifically listed." *In Matter of Black iPhone 4*, 27 F.Supp.3d at 78. Where such lists "merely identify generic classes of items and permit the seizure of virtually all conceivable documents" they cannot render an otherwise un-particularized warrant sufficiently particular. *People v. Melamed*, 178 A.D.3d 1079 (2d Dept. 2019).

The warrant did not limit the searches of any of the devices to any particular category(s) of information for example: web browser history, cookies, photographs, emails, etc. *See e.g. Winn*, 79 F. Supp. 3d at 919; *United States v. Hunter*, 13 F.Supp.2d 574, 581 (D. V.T. 1998). It did not provide temporal limitations on the search. *See e.g. United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("'Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad.'"); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (warrant "not sufficiently particular" in part because the "government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *United States v. Abrams*, 615 F.2d 541, 545 (1st Cir. 1980) (deeming warrant insufficiently particularized and noting, among other things, that "[a] time frame should also have been incorporated into the warrant"). Instead, the Device Warrant authorized an unfettered search of every device in the household "not limited to" an illustrative list of categories of information.

Warrants for "any and all files" that "include[] but [are] not limited to" an illustrative list of various types of data found on a phone are patently unconstitutional. *Winn*, 79 F. Supp. 3d at 919. In *Winn* the Southern District Court of Illinois noted "[t]he major, overriding problem with the description of the object of the search—"any or all files"—is that the police did not have probable cause to believe that everything on the phone was evidence of the crime of public indecency. *Id.* Instead there "was probable cause to believe that only two categories of data could possibly be evidence of the crime: photos and videos." *Id.* Furthermore even "[w]ith respect to the categories of data for which the police

did have probable cause—the photos and the videos—the warrant was not as particular as could be reasonably expected given the nature of the crime and the information the police possessed. The warrant merely described the category of data, rather than specific items, which allowed the police to seize all of the photos and videos on Winn's phone, as opposed to specific photos and videos…" but "Detective Lambert knew the precise identity and content of the photos/videos sought. However, he failed to mention the characteristics that made those photos/videos easily identifiable and distinguished them from others that were irrelevant. For example, the warrant could have described the location of the incident as well as the subjects of the images—children at a swimming pool, or more specifically young girls in swimsuits at the Mascoutah Public Pool." *Id.* at 920. The court further noted that there were no temporal limitations and the only limit implied by the warrant was an unadorned reference to a criminal statute. *Id.* at 921.

Here the Device Warrant uses the same "any and all" language as *Winn,* the additional broad phrase "including but not limited to," followed by an illustrative list of various types of data. This illustrative list includes types of data for which there is not probable cause. It imposes no temporal limitations and fails to even impose the minimal restriction from *Winn* limiting the search to evidence of a specific criminal statute. The Device Warrant, at one point, makes an oblique reference to something resembling the facts in the case when it states "any and all information pertaining to internet searches pertaining to posts regarding threats of violence directed towards schools or public officials." However, that clause is in and of itself both overbroad and insufficiently particular. The affidavit did not contain any information establishing threats to public officials or towards schools in general. Had they actually connected Daugherty to that post (which they did not) the only possible thing they could investigate him for was the March 16, 2018, threat "FUCK YOU YOU STALKING MOTHER FUCKERS. I'LL SHOW YOU WHO IS AUSTIC. I'LL GO TO FUCKING MEMORIAL ELEMENTARY SCHOOL AND MAKE SANDY HOOK LOOK LIKE A SUNDAY SCHOOL PICNIC" posted on hateandflame.com. This is a basic tenant of probable cause and particularity—a search for evidence of one crime does not allow a search for evidence of other crimes. *United States v. Wey*, 2017 WL 257402 at *18 (S.D.N.Y. 2017). Furthermore, there is no reason to believe they would find information relevant to their investigation in the form of an "internet search" as there were no facts that established any reason to believe an "internet search" was done for public officials or schools. Therefore, this clause (if it could be considered a clause at all) was both overly broad and lacking in particularity.

Similarly, the warrant mentions "peer to peer file trading software" this is both overbroad and insufficiently particularized. There is no mention of peer-to-peer file sharing in the affidavit for the device warrant. Therefore, it is overbroad. Similarly, it places no limits on what kind of peer-to-peer file sharing evidence the government may collect. Therefore, it is insufficiently particularized.

Finally, the warrant includes an "indicia of ownership" clause that allows for "records and other items which evidence ownership or use of computer equipment found in the above residence." Warrants allowing for searches of "indicia of ownership" have been rejected by courts across the country because they turn an otherwise valid warrant into a general warrant. *See State v. Bock*, 310 Or.App. 329 (Ct. Ap. Or. 2021); *People v. Coke*, 461 P.3d 508 (Colo. Sup. Ct. 2020); *State v. Hamilton,* No. 6:18-CR-57-REW-10, 2019 WL 4455997 (E.D. Ky. August 30, 2019); *see also People v Herrera*, 357 P.3d 1227 (Colo. Sup. Ct. 2015) (rejecting the use of such clauses to justify broad searches); *United States v. Ford*, 184 F.3d 566, 586 (6th Cir. 1999) (rejecting the use of similar clauses that would potentially allow limitless seizures of financial information).

In *Bock*, the Oregon Court of Appeals suppressed evidence recovered from a cell phone in part because of a clause allowing the government to search for "[a]ny evidence identifying the owner/user of the device." *Bock*, 310 Or.App. at 332. The court held that "[r]egardless of whether the command to search for evidence of the owner or user of the device included a temporal limitation on the material subject to seizure… the search command violates the particularity requirement." *Id.* at 334. This is because "there is little information on the device that the state could not use to identify the defendant given the right circumstances and background information. Under such circumstances, the officer performing the search has the discretion to rummage freely throughout the device and seize nearly everything—the exact practice that the particularity requirement was adopted to prohibit." *Id.* at 335.

Similarly, in *Hamilton*, the District Court rejected the government's argument that broad warrants are lawful because, "anything and everything in the Facebook account could be used to prove identity of the Facebook user and control of the account…" *Hamilton*, 2019 WL 4455997 at *5. The court reasoned that "[t]aken to its logical conclusion, this argument nearly obviates the particularity requirement altogether; almost anything in someone's social media data can be used to show they did (or did not) own and control that account." *Id.* The court elaborated, explaining that the government was "certainly entitled to search for this information to a reasonable extent; for example, the registered user, email addresses, birth date, telephone number, physical address, and IP addresses associated with the account are likely to show ownership and control of the account. The breadth of information the search

warrant required Facebook to disclose, however, amounted to "a general, exploratory rummaging" in [the defendant's] digital life that did not comport with the particularity requirement of the Fourth Amendment." *Id.*

The same logic from *Bock* and *Hamilton* applies to, and invalidates, the indicia of ownership "clause" here. One can only begin to imagine what might constitute "records and other items which evidence ownership or use of computer equipment found in the above residence." Nude photographs of the defendant, communications regarding his political affiliations, sexual orientation, medical history etc. could all demonstrate ownership of the computer equipment. As could IP addresses, web browser history, cookies, and text files. However, the warrant provides no explanation as to what the government may seize. Thus, the boundaries of this clause are left only to the imagination of the executing officer as they come across previously unidentified evidence during their unrestrained search. This is "the exact practice that the particularity requirement was adopted to prohibit." *Bock*, 310 Or.App. at 335.

The Device Warrant was a hopelessly unparticular and overbroad general warrant. Therefore, it violates the Fourth Amendment and Article I, Section 6 of the Illinois Constitution and any evidence obtained as a result of the warrant must be suppressed.

c. The Government Intentionally Omitted Material Facts from the Device Warrant Affidavit that If Known to The Judge Would Have Demonstrated an Affirmative Lack of Probable Cause

Officer Christian Nelson intentionally omitted material facts demonstrating that police affirmatively lacked probable cause to execute the Device Warrant. Specifically, he intentionally withheld information regarding the nature of the website itself, the likelihood that individuals there regularly impersonated one another and attempted to harm one another's reputations, and that there was a very real possibility that this had happened in Daugherty's case.

Under *Franks*, evidence seized under a warrant must be suppressed when the defendant shows that "(1) the affidavit in support of the warrant contains false statements or misleading omissions, (2) the false statements or omissions were made deliberately or with reckless disregard for the truth, and (3) probable cause would not have existed without the false statements and/or omissions." *United States v. Williams*, 718 F.3d 644, 647 (7th Cir. 2013); *see Franks*, 438 U.S. at 155–56.

Here, officer Nelson made numerous intentional omissions which if they had been known to the judge would have informed them that the threatening post likely came from a third party (potentially the tipster themselves) rather than Todd Daugherty.

First, officer Nelson, intentionally omitted that the initial tip itself was suspect because the tipster used the Tor network as a means of obscuring their location and identity. Although the person claimed to be from the United States, their IP address resolved in France to a node identified with the Tor network. This information would have demonstrated to the issuing judge that the tipster had an above average knowledge of computer networks and was utilizing them in this case to mask their identity from the FBI in making accusations against Daugherty. Furthermore, this information would also have demonstrated they were either lying about their actual location or taking steps to conceal it, further undermining their credibility.

Second, Officer Nelson intentionally omitted an explanation of the contents of the website the post was made, www.hateandflame.com. He did not explain that the site was a virtual cesspool of individuals impersonating, antagonizing, threatening, and doxing one another. Other than the post attributed to Daugherty, none of the individuals used their real names to post. Instead, they used obviously fake names like "Ernist Hemingay", "Buddy Che Hinton", "Harry Tard Snortz" "Loyd Davies, Timelord" "THE PINKLE WHEEZLE", "STAINLESS STEEL FUCKBOT" or just "." Nor did any of them use real photographs of themselves as their profile photos with the exception being the post allegedly made by Todd Daugherty. Nor did he explain that Thomason recognized the photographs on the post of Daugherty holding a gun from a previous incident or that Daugherty explained he had previously posted them on a blog making them available to anyone on the internet to use. Further, he did not reveal that during the days leading to the threatening post, many of these individuals were accusing one another of posting under multiple account names. This would have greatly undermined the value of paragraphs two and five which attach the account to Daugherty through an image of him and his ham radio call sign. It also would have provided credence to Daugherty's statement in paragraph four that he was being set up by a member of the online community.

Third, he did not reveal that he had no technical means of identifying Todd Daugherty as the person who posted the threat. When he submitted the affidavit, while he had obtained Todd Daugherty's IP and MAC address from Daugherty's internet service provider, he had not obtained or executed a search warrant for the web logs from www.heatandflame.com and he therefore could not confirm that the posting was linked to an account or computer owned by Daugherty. Nor did he explain to the judge that he had no idea what credentials an individual must supply in order to access the website, what the policies on impersonating others are, or how they are enforced. Had he fully explained that he had

methods of verifying the informant's claims but had yet to employ any of them, the judge likely would not have signed off on the warrant until those investigations were completed.

Finally, officer Nelson hid the fact that prior to his application, multiple individuals had provided information to law enforcement that supported Daugherty's claims that he was being "set up" by someone online. Specifically, he omitted that on March 18, 2018, Todd Daugherty's brother, Jeremy Daugherty, contacted the Taylorville police department and provided links to the hateandflame website demonstrating that individuals were making posts purporting to be Todd Daugherty while he was in police custody. He also omitted mention that a Canadian man named Karl Madera contacted the State's Attorney Mike Havera to tell him that Todd Daugherty was being set up by someone named Bryan Crow. Again, these facts both undermined the value of paragraphs two and five and demonstrated the potential truth of Daugherty's claims in paragraph 4.

Had the judge been aware of all the circumstances surrounding the investigation and the possibility that Daugherty was being set up by a member of a toxic online community known for impersonating people, they never would have signed a warrant to seize and search every device in his home. Therefore, Daugherty is entitled to suppression of all materials recovered pursuant to the Device Warrant or a hearing pursuant to *Franks*.

II. Agent O'Sullivan Conducted a Warrantless Search of the Devices

FBI agent William O'Sullivan executed a warrantless search of the devices after the Device Warrant was quashed and the charges against Daugherty were dismissed for a lack of probable cause. Therefore, all fruits of that search must be suppressed.

Warrantless searches are *per se* unreasonable, absent limited exceptions. *Katz v. United States,* 389 U.S.- 347, 357 (1967). Furthermore, probable cause must exist not only at the time law enforcement obtains a warrant, but also at the time the warrant is executed. Where a search warrant is issued on probable cause, changed circumstances or new information can negate a prior determination of probable cause. *See United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993) (finding new information can negate prior determination of probable cause). When new circumstances call into question an original finding of probable cause, the officer must bring the new information to the issuing magistrate's attention. *United States v. Bowling*, 900 F.2d 926, 933 (6th Cir. 1990). "Thus, when a definite and material change has occurred in the facts underlying the magistrate's determination of probable cause, it is the magistrate, not the executing officers, who must determine whether probable cause still exists.

Therefore, the magistrate must be made aware of any material new or correcting information." *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984)

Here, although the government initially obtained a warrant for the device in question on March 21, 2018, by, March 29, 2018, the government knew they no longer had probable cause to prosecute Daugherty. That is when police learned that neither Daugherty's IP address, nor his MAC address had been used to post on hateandflame.com during the time of the threatening post. Instead, they learned that the IP address responsible for the threatening post was associated with the TOR network and was therefore anonymous. Further, police learned that 90% of people posting on the website were using Tor or proxy sites; no registration was required; no email addresses were checked; as a result of all this anybody could post as anybody else and impersonation is part of the status quo for the board. All of this simply confirmed what police had been told by multiple witnesses and what was readily apparent from the fact that someone continued to post as Daugherty while he was incarcerated and lacked access to the internet—that Todd Daugherty was being set up by someone posting on hateandflame.com using his name and likeness. Despite confirming that Daugherty could not be connected to the threat and that they lacked probable cause, police gave all of the devices to the FBI on April 11, 2018, and requested that they conduct a search.

Furthermore, on April 16, 2018, the government filed motion to dismiss the case based on the following facts: (1) the website used to disseminate the threat did not require any login credentials, (2) while Daugherty was in custody more messages appeared under his name, (3) posts on the website were made by people impersonating "judges, the president, and other such individuals" (4) Daugherty's internet activity showed nothing to implicate him in the case. At 11:32 a.m. on April 16, 2018, the court granted the motion which specifically stated that any warrants or summonses previously issued were ***quashed***.

Despite the lack of a warrant or probable cause, Agent O'Sullivan withdrew the devices from storage at 8:20 p.m. on that same day, April 16, 2018 and created an inventory. It was not until three days after the warrant had been quashed that he began the process of extracting the contents pursuant to the invalid (and at that point non-existent) Device Warrant. Then, on April 23, 2018, a week after the warrant had been quashed, O'Sullivan began to search the device. During that warrantless search O'Sullivan found what he noted what appeared to be a computer-generated image of a minor child with an adult male penis in his mouth.

Thus, the evidence discovered here was discovered after the Device Warrant was quashed and was therefore a warrantless search. Furthermore, the probable cause on which the Device Warrant was had dissipated prior to the Taylorville police department providing the devices to the FBI to conduct the searches. For those reasons, all evidence discovered pursuant to that search and the fruits thereof must be suppressed. This includes the subsequently issued Federal Warrant.

III. The Federal Warrant Contains Material Misstatements and Omissions Regarding the Device Warrant and the Case Against Daugherty

The Federal Warrant application drafted by Special Agent Anthony Wright misrepresents the nature of the FBI's possession of the devices and the validity of the Device Warrant. If these misrepresentations and omissions were excised or corrected in the warrant application for the Federal Warrant, Magistrate Tom Schanzle-Haskins would not have signed Federal Warrant.

First, paragraph six of the Federal Warrant states that the Taylorville Police department seized the devices "based on a state search warrant related to threats of a mass shooting against Memorial Elementary School in Taylorville, Illinois made by Daugherty." It does not explain that the case against Daugherty had since been dismissed for a lack of probable cause and that the warrants on which they were seized was subsequently quashed for the same reasons.

Second, paragraphs seven and eight of the Federal Warrant imply that the search was conducted on April 6, 2018, before the warrant was quashed. However, the search was not conducted until after probable cause had dissipated and the warrant had been formally quashed by a judge at the request of the prosecution for a lack of probable cause.

The Federal Warrant essentially laundered all of the problems with the investigation into Daugherty, the Device Warrant, and the illegal execution, by merely claiming that they had a valid warrant and stumbled across contraband in plain view. With this whitewashed version of the events surrounding the investigation into the hateandflame incident and Daugherty's devices, there can be no wonder why the magistrate signed the Federal Warrant. They were under the impression that the FBI, acting on a valid state warrant, stumbled across contraband in plain view and acted according to the law to obtain a new warrant. Had the magistrate been aware of all the circumstances surrounding the investigation into Daugherty and the search and seizure of his devices he never would have signed the Federal Warrant. Therefore, Daugherty is entitled to suppression of all materials recovered pursuant to the Federal Warrant or a hearing pursuant to *Franks*.

IV. Daugherty is Entitled to a Hearing on the Execution of the Search

Should the court find that agent O'Sullivan was allowed to execute a search pursuant to the Federal Warrant, Daugherty is entitled to a hearing on the methodology used to conduct the search of the devices to examine whether it adhered to the constitutional strictures. *United States v. Christie*, 717 F.3d 1156, 1167 (10th Cir. 2013).

In the context of electronic device searches, the Fourth Amendment requires the courts to "assess the propriety of the government's search methods (the how) *ex post* in light of the specific circumstances of each case. So, even if courts do not specify particular search protocols up front in the warrant application process, they retain the flexibility to assess the reasonableness of the search protocols the government actually employed in its search after the fact, when the case comes to court, and in light of the totality of the circumstances." *Id.* at 1166-67 (citations omitted); *see also Winn*, 79 F. Supp. 3d at 921 & 924-926 (noting that a full hearing was conducted on the execution of the device search); *United States v. Graziano*, 558 F. Supp. 2d 304, 317 (E.D.N.Y. 2008) (evidentiary hearing conducted); *Wey*, 2017 WL 2574026 (in depth hearings conducted on the execution of the search warrants); *United States v. Bonner*, 2013 WL 3829404 (S.D.C.A. 2013) ("The search protocol employed must be reasonably directed to identify data within the scope of the warrant in order to meet the particularity requirement."). The *Christie* court required a hearing on the subject, finding that "[t]o undertake any meaningful assessment of the government's search techniques . . . we would need to understand what protocols the government used, what alternatives might have reasonably existed, and why the latter rather than the former might have been more appropriate." *Christie*, 717 F.3d at 1167. The court noted that such *ex post* reviews should include, "evidence and experts from both sides." *Id.*

To the extent the Court finds Device Warrant put some restrictions on the subsequent search, it is clear that it did not authorize a search for child pornography or child sexual abuse material. Therefore, the contraband in question was beyond the scope of the warrant and the government can only proceed by claiming that it was in "plain view." Thus, unless the State concede suppression is mandated, a hearing is required to "assess the government's search techniques" and test this claim. *See id.*

V. The Federal Warrant Was Not Sought Within a Reasonable Time Period of the FBI's Warrantless Seizure

Setting aside the problems with the initial Device Warrant, the evidence must be suppressed because the government waited almost two years to seek a Federal Warrant to re-search the devices.

This unreasonable delay in seeking a warrant was an additional violation of Daugherty's constitutional rights.

"[T]he Fourth Amendment imposes a time-sensitive duty to diligently apply for a search warrant if an item has been seized for that very purpose, and all the more so if the item has been warrantlessly seized." *United States v. Smith*, 967 F.3d 198, 210 (2d Cir. 2020). The Second Circuit has held that ordinarily a delay of 31 days or more in seeking a warrant is unreasonable. *See id.*; *see also United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) (21 days found unreasonable). In making the determination that 31 days was unreasonable in ordinary cases the court examined four factors: (1) the length of the delay, (2) the importance of the seized property to the defendant, (3) whether the defendant had a reduced property interest in the seized items, and (4) the strength of the state's justification for the delay. *Smith*, 967 F.3d at 203.

a) The length of the delay Weighs in Favor of Suppression

In *Smith*, the Second Circuit found a delay of 31 days or more in seeking a warrant is unreasonable. *Smith*, 967 F.3d 198. The 11th Circuit similarly found 21 days to be unreasonable. *See also United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009). The court in *Smith* gave independent weight to the length of delay and concluded that a month-long well exceeds what is ordinarily reasonable.

In the instant case, the affidavit seeking to search the electronic devices was filed **686 days or one year 10 months and 15 days *after the dismissal of the warrant*** in this case. "If the police have seized a person's property for the purpose of applying for a warrant to search its contents, it is reasonable to expect that they will not ordinarily delay a month or more before seeking a search warrant." *Smith*, 967 F.3d at 206–207. The officers in the instant case waited over 22 times longer than the 31 days in *Smith* to seek a search warrant for the property seized. Therefore, the delay weighs strongly in favor of suppression.

b) The Importance of the Seized Property Weighs in Favor of Suppression

In *Smith*, the Court noted "our starting point is to consider the nature of the property seized: a personal tablet computer that is typically used for communication and for the storage of immense amounts of personal data. The sheer volume of data that may be stored on an electronic device like a Nextbook (or similar tablet computer products like an Apple iPad) raises a significant likelihood of that much of the data on the device that has been seized will be deeply personal and have nothing to do with the investigation of criminal activity. For this reason, we have recognized the special concerns that apply when law enforcement seize and search people's personal electronic data and communication devices."

Smith 967 F.3d at 207. "While physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material, the reasonableness of seizure and subsequent retention by the government of such vast quantities of irrelevant private material was rarely if ever presented in cases prior to the age of digital storage." *Id.* at 207 (quoting *United States v. Ganias*, 824 F.3d 199, 218 (2d Cir. 2016) (*en banc*). "Indeed, this fundamental distinction between one's ordinary personal effects and one's personal electronic devices has persuaded the Supreme Court to accord broader constitutional protection when police seize a person's 'smart' cell phone." *Id.* The Supreme Court has observed that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 208 (quoting *Riley v. California*, 573 U.S. 373, 134 (2014)).

In the case at bar, law enforcement retained ***all fifteen items*** seized from Daugherty's home including: a black and blue Seagate hard drive, serial number NA7DWTK4; one Seagate 1TB hard drive, serial number 5vPG12DV, a Cyperton computer tower, serial number GA-78LMT-USB3; a Compaq computer, serial number CNH4520P00; a Gateway 7320 laptop, serial number N3451-710-03782; a Gateway computer, serial number PTE590XD01960595B2700; three DVD-Rs, one CDR, one CTI router, and four assorted USB drives. *Warrant Return*, 18-MR-40. This goes far beyond the single tablet seized in *Smith* and weighs strongly in favor of suppression.

c) Daugherty's Property Interests in His Devices Weighs in Favor of Neither Party

According to *Smith,* a defendant may have a reduced property interest because of a consent to a seizure or search or by voluntarily relinquishing property to a third party. *Id.* at 208. In the alternative, one's property interest may be diminished because of the existence of probable cause. *Id.* However, even in the event that probable cause rather reasonable suspicion existed, "…the police's interest was delimited by the obligation to seek a search warrant without unreasonable delay." *Id.* at 209. "That is because '[t]he longer the police take to seek a warrant, the greater the infringement on the person's possessory interest will be, for the obvious reason that a longer seizure is a greater infringement than a shorter one.'" *Id.* at 209 (quoting *United States v. Burgard,* 675 F.3d 1029, 1033 (7th Cir.2012)). The court opined in *Smith* that the existence of probable cause was relevant to Smith's possessory interest, but was far from dispositive to deciding the reasonableness of the delay in seeking the search warrant.

Here, Daugherty did not consent to a seizure or search the 15 items retained by the FBI. Instead, they were obtained through the use of a warrant that lacked probable cause, was obtained through the use of material misstatement and omissions, and was unconstitutionally unparticularized and overbroad.

Additionally, they were retained and searched by the FBI despite the fact that the warrant was quashed and Daugherty and his father requested their return. Also, here similarly to Smith the police had probable cause to believe that the devices contained child sexual abuse material. *Smith*, 967 F.3d at 209. However, the existence of probable cause—as opposed to reasonable suspicion—merely allows for a slightly greater delay in seeking the warrant. *Id.* Even if probable cause existed to seize the items, the police interest was delimited by its obligation to seek a search warrant without unreasonable delay.

d) The Lack of Justification for the Delay Weighs in Favor of Suppression

"The fact that a police officer has a generally heavy caseload or is responsible for a large geographical district does not without more entitle the officer to wait without limit before applying for a search warrant to search an item that the officer has seized. That is because the Fourth Amendment imposes a time-sensitive duty to diligently apply for a search warrant if an item has been seized for that very purpose…" *Id.* at 210.

There is no justification for the delay in this case. Local law enforcement seized Daugherty's devices on March 21, 2018, and then transferred such to the FBI on or April 11, 2018, after it became abundantly clear they lacked cause to retain or search them. The FBI then maintained possession of Daugherty's property for **686 days or one year 10 months and 15 days *after the dismissal of the warrant*** in this case.

Where the police fail to seek a warrant in a reasonable amount of time pursuant to *Smith*, no exceptions to the exclusionary rule apply and suppression is required. *Id.* at 213 ("[W]e have stated and clarified principles above that shall guide law enforcement officers with respect to what circumstances establish an unreasonable delay under the Fourth Amendment… These principles shall… inform the application of the exclusionary rule in future cases."). *Id*; *see also United States v. Tisdol*, 544 F. Supp. 3d 219, 228 (D. Conn. 2021) (finding the good faith doctrine inapplicable post *Smith*); *cf. United States v. Burgard*, 675 F.3d 1029 (7th Cir.2012) (stating in dicta that "removing this sort of police misconduct from the ambit of the exclusionary rule would have significant implications," and that "it would eliminate the rule's deterrent effect on unreasonably long seizures.") (citing *United States v. Song Ja Cha*, 597 F.3d 995, 1006 (9th Cir.2010)).

The exclusionary rule must be applied. Evidence must then be excluded when the police have violated Constitutional rights deliberately, recklessly, or with gross negligence. *Smith*, 967 F.3d at 211. In the instant case, Wright's delay amounted to gross negligence. Therefore, the 686-day delay in

seeking a valid warrant to search the devices was a violation of the Fourth Amendment and suppression is required.

CONCLUSION

For the above reasons, Daugherty respectfully requests that this Court suppress the evidence seized as a result of the illegal searches of his personal electronic devices.

TODD E. DAUGHERTY,

September 9, 2024

By: Tiffany Senger
Tiffany Senger, His Attorney

CERTIFICATE OF SERVICE

The undersigned hereby certifies that she served a true and correct copy of the foregoing instrument upon the Christian County State's Attorney by causing it to be emailed via efiling on September 9, 2024.

Tiffany Senger
Tiffany Senger, Attorney