IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
[redacted] DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CASE NUMBER:** [redacted]
	)	
[redacted]	)	

DEFENDANT'S MOTION TO SUPPRESS CONTENTS OF ELECTRONIC DEVICES AND BRIEF IN SUPPORT

Comes now the defendant, [redacted] by and through his attorney, [redacted] Assistant Federal Public Defender, and does hereby respectfully move for an Order from this Court suppressing from use at trial, the contents of an Apple iPhone SE, assigned IMEI (IMEI) [redacted], a Lenovo Laptop bearing serial number [redacted], and an Apple iPhone 12 assigned IMEI [redacted], that was taken in violation of the Fourth Amendment to the United States Constitution, and for his motion states:

Background

Mr. [redacted] is charged in a two-count indictment and forfeiture allegation with one count of transportation of child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) & (b)(1) and one count of possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) & (b)(2). ([redacted] This matter is currently set for jury trial [redacted] ([redacted] A federal arrest warrant for Mr. [redacted] was issued on [redacted] 2022, and executed on or about [redacted] 2022. [redacted] At the time of his federal arrest, Mr. [redacted] was being held on pending state charges; he is currently incarcerated at the [redacted] Arkansas, and has been since on or about [redacted] 2021.

Facts

On [redacted] 2021, [redacted] police officers sought a warrant to search Room [redacted] at the Super 8 Motel in [redacted] Arkansas, which is in the Western District, for alleged drug activity. Upon entry, law enforcement seized among other things, a Lenovo Laptop (hereinafter SUBJECT COMPUTER) from the room and seized an Apple iPhone 12 (hereinafter SUBJECT PHONE) from Mr. [redacted]'s person as he was arrested and taken into custody. He was subsequently released.

On [redacted] 2021, Investigator [redacted] of the [redacted] Police Department made contact with Mr. [redacted] during a routine traffic stop, in which [redacted] was a passenger of a vehicle driven by an acquaintance. [redacted] was taken into custody for the alleged possession of a controlled substance and drug paraphernalia and was questioned by officers at the [redacted] Police Department. He was *Mirandized* and began speaking with officers about the alleged drug possession. Approximately forty-five minutes later, [redacted] was told that he was being investigated by local law enforcement concerning alleged child abuse and child pornography. Mr. [redacted] signed a consent form, consenting to a single manual search of his iPhone by a distinct officer within the [redacted] Police department and his partner. However, over two months after that search was over, the FBI, without further consent, conducted an offsite forensic search.

On [redacted] 2022, FBI Task Force Officer [redacted] sought a search warrant ("electronics warrant") for the contents of Mr. [redacted]'s Lenovo Laptop (referred to in the electronics warrant affidavit as the SUBJECT COMPUTER) and Apple iPhone 12 (referred to in the electronics warrant affidavit as the SUBJECT PHONE) that was seized from the Super 8 Motel on [redacted] 2021. In efforts to establish probable cause to search the SUBJECT COMPUTER and SUBJECT PHONE seized during Mr. [redacted]'s arrest at the Super 8 Motel, in her affidavit,

Officer [redacted] refers to contents found during an extraction of the Apple iPhone SE, which is referred to as "another phone." This electronics warrant sought to search the entirety of the SUBJECT COMPUTER and SUBJECT PHONE. Thus, 400 days after state agents seized the SUBJECT PHONE and SUBJECT COMPUTER from Mr. [redacted], an affidavit for a federal search warrant was filed. The affidavit provides in paragraph 27 that:

> At all times since their initial seizure by DTF agents on [redacted] 2021, the SUBJECT COMPUTER and SUBJECT PHONE have remained secure, unaltered, and in the custody of law enforcement. The SUBJECT DEVICES are currently in the custody of the Federal Bureau of Investigation, in the Western District of Arkansas.

Officer [redacted] provides no explanation as to the 400-day delay in requesting the search warrant. Mr. [redacted] moves this Honorable Court to suppress all the contents of the three electronic devices.

Law, Analysis and Argument

The Fourth Amendment guarantees, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. When a search is conducted in violation of the Fourth Amendment, the exclusionary rule prohibits evidence seized during the search from being introduced into evidence, along with any derivative evidence acquired as an indirect result of the unlawful search. *Murray v. United States*, 487 U.S. 533, 536-37 (1988); *Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963). All evidence obtained as a result of these Fourth Amendment violations must be suppressed as "fruit of the poisonous tree." See *Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *United States v. Washington*, 490 F.3d 765, 775 (9th Cir. 2007) ("[E]vidence obtained subsequent to a violation of the Fourth Amendment is tainted by the illegality and is inadmissible . . . unless the evidence obtained was 'purged of the primary taint.'" (quoting *Wong Sun*, 371 U.S. at 488)); *United States*

v. Davis, 332 F.3d 1163, 1170-71 (9th Cir. 2003) ("[T]he standard articulated in *Wong Sun* remains the relevant test.").

In the instant case, Mr. [redacted]'s Fourth and Fifth Amendment rights were violated in several different ways, some of which are addressed in separate motions[1]. For the purposes of this motion, Mr. [redacted]'s rights were violated because 1) the Lenovo laptop and Apple iPhone 12 are the fruits of the invalid Super 8 Warrant, 2) the Apple iPhone SE was searched beyond the scope of consent 3) the Government did not obtain the electronics warrant in a reasonable period of time; and 4) the electronics warrant is the fruit of unlawful Dropbox and Google warrants, as well as an unlawful extraction. Each violation requires suppression of all evidence seized from his electronic devices.

I. The SUBJECT COMPUTER and SUBJECT PHONE Are the Fruits of the Invalid Super 8 Warrant.

The SUBJECT COMPUTER and SUBJECT PHONE were both seized pursuant to the Super 8 Warrant. However, the Super 8 Warrant Affidavit failed to establish probable cause to seize those items because it did not even attempt to establish the reliability of the informant on which the purported probable cause was based. *See Affidavit for Search Warrant*, dated [redacted] 2021, attached as Exhibit A (hereinafter the Super 8 Affidavit). Investigator [redacted] of the [redacted] County Sheriff Office sought to search the hotel room based on a bare-bones affidavit that did not establish probable cause. In his affidavit, dated [redacted] 2021, Inv. [redacted] averred the following:

> "On [redacted] 2021, a reliable confidential informant made contact with Investigator [redacted] and advised that he/she just left the Super 8 Hotel, located at [redacted] Room #[redacted]. While inside the room, the informant observed what he/she described as a large amount of crystal methamphetamine in a plastic

[1] Mr. [redacted] has filed separately: Motion to Suppress Statements; Motion to Suppress Google Contents, and a Motion to Suppress Dropbox Contents.

> baggie and a handgun inside the room. The informant stated that the room belongs to [redacted] and he was present in the room."

The reliability of the informant is not sufficiently established, and the warrant is based on conclusory claims that the confidential informant was reliable. The reliability of this informant is camouflaged in the information that two days prior to the date in question, that "a" confidential informant participated in a controlled buy that was surveilled by law enforcement. Nothing in the affidavit establishes that this was the same informant from the previously surveilled controlled buy, or that the informant on the date in question had worked with law enforcement on a number of prior occasions to provide accurate and truthful information. "The statements of a reliable confidential informant are themselves sufficient to support probable cause for a search warrant. The reliability of a confidential informant can be established if the person has a history of providing law enforcement officials with truthful information." *United States v. Mayweather*, 993 F.3d 1035, 1044 (8th Cir. 2021), reh'g denied (May 19, 2021) (quoting *United States v. Wright*, 145 F.3d 972, 975 (8th Cir. 1988) (holding that evidence obtained pursuant to a search warrant would not be suppressed because the affiant adequately established the CRI's reliability when the affiant stated that the CRI had proven his "reliability in the past by making controlled purchases[s] of crack cocaine" under the direct supervision of affiant officers)).

Even if the government asserts in the instant case that the confidential informant's identity would be revealed by stating that he/she was the same person from the [redacted] 2021, incident, that has no bearing on the necessity to establish how the "reliable" informant was in fact reliable. "[I]n the absence of any indicia of the informants' reliability, courts insist that the affidavit contain substantial independent police corroboration." *United States v. Waide*, 60 F.4th 327, 336 (6th Cir. 2023) (quoting *United States v. Frazier*, 423 F.3d at 532). Inv. [redacted] added that he contacted probation and parole to verify whether Mr. [redacted] was a convicted felon; however, that in no way

corroborates the information provided by the informant that Mr. [redacted] was at the Super 8 Motel at that time. No other corroborating information was presented in the affidavit, neither was there any additional investigation about Mr. [redacted] or his whereabouts.

In her application for a federal warrant to search [redacted]'s electronic devices, Officer [redacted] relies on the invalid state search warrant, so the SUBJECT COMPUTER and SUBJECT PHONE never should have been searched. (*See Electronics Warrant Affidavit* attached, Exhibit B). Officer [redacted] states in paragraph four her affidavit that:

> …I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(1) [transportation of child pornography]; Title 18, United States Code, Section 2252A(a)(2) [receipt/distribution of child pornography] and Title 18, United States Code, Section 2252A(a)(5)(B) [possession of child pornography/access with intent to view] are now concealed on the SUBJECT COMPUTER and SUBJECT PHONE.

Interestingly, only three paragraphs later in paragraph seven of the Probable Cause section of the affidavit, Officer [redacted] provides a direct contradiction and avers incriminating information, but not for the purpose of establishing probable cause.

> Although your affiant is not providing the following information to establish probable cause, your affiant believes the court should be made aware that during the search warrant execution, DTF Agents observed what they believed may have been child pornography on the SUBJECT COMPUTER, which was powered on, unlocked, and open at the time.

It must be noted that Officer [redacted] does not lay out the reason for including this prejudicial information if it is not included for the purpose of establishing probable cause. This information was provided for the purpose of bolstering sufficient information for probable cause to search the electronics that had been in the custody and control of law enforcement for 400 days. Such illegally obtained evidence provided in the Electronics Warrant Affidavit included Mr. [redacted]'s

statements to law enforcement, incriminating information contained in Mr. [redacted]'s Apple iPhone SE, and photos and videos in his Google and Dropbox accounts.

II. The Apple iPhone SE Was Searched Beyond the Scope of Consent.

On [redacted] 2021, Mr. [redacted] was taken into custody and questioned for alleged possession of drugs and drug paraphernalia. At the outset of the interview, Captain [redacted] provided a form to Mr. [redacted] and explained to him his *Miranda* rights. Investigator [redacted], who made the traffic stop, was also present. [redacted] was questioned about the alleged drugs found in the vehicle in which he was a passenger. After further dialogue officers established that [redacted] drove a chip truck for work. At approximately the 39:00 mark of the recording of the interview, Cpt. [redacted] asks [redacted] "So would you be willing to give us consent to look in your truck?" [redacted] responds, "My chip truck?—Uh, yeah, (unintelligible) I would." The officers then prepare and present to [redacted] a consent to search form for a Freightliner 90s model truck, which he signs. Officers later begin to shift the conversation to discuss allegations of child abuse and child pornography. At approximately the 50:13 mark of the recording of the interview, Inv. [redacted] asks [redacted], "Is there anything on that phone?" —referring to the Apple iPhone SE that [redacted] had in his possession during the traffic stop and interview. [redacted] replies, "No, sir." Inv. [redacted] then asks, "Would you mind giving consent for us to look at that phone? After some unintelligible dialogue, starting at the 50:58 mark of the interview, Inv. [redacted] then goes on to say:

> I mean, if you're worried about these allegations of the pornography and stuff like that, and you want to clear your name—I mean, I know if I was in your spot and I didn't have anything on my phone, I would by all means tell anybody in the world to look at my phone. Now, granted, you still have your expectation of privacy if you don't want us to go through it because you're scared we might see something else—well then that's fine. But, understand if it was me and I was being—you know, if I had somebody file allegations against me I would be transparent and say, "—

At that point, [redacted] interjects and states that he just wants to go home. Cpt. [redacted] then asks [redacted] the phone number to the Apple iPhone SE and the password. It sounds like [redacted] says he does not know [the passcode]. Cpt. [redacted] states, "You gonna put your thumb on it and let me look through it?" [redacted] replies, "Yes, sir." At approximately the 52:29 mark of the interview, Cpt. [redacted] prepares a consent to search form for the Apple iPhone SE and places it in front of [redacted]. He then places the consent to search form for the Freightliner 90s model truck, that [redacted] had signed earlier in the interview, next to the consent to search form for the Apple iPhone SE, and states, "That's the same thing as this one." [redacted] acknowledges the consent to search form for the truck and states what sounds like, "I know." [redacted] then states, "—yall gonna search the truck—the truck, yall gonna do that there, but I wanna keep my phone." To which Cpt. [redacted] replies, "I'm gonna keep your phone no matter what if you don't let me search it." [redacted] then states that he can open the phone and let the officers look. Cpt. [redacted] replies, "[redacted], you gotta sign the form in order for me to look in your phone." Based on this dialogue, [redacted] was led to believe that by giving the officers permission to look at the contents of the phone right then and there, that he would be able to maintain possession of it after they finished looking through it.

At approximately the 55:00 mark of the recording, Inv. [redacted] states, "You have the right to stop the search at any time. This consent—you can withdraw your consent at any time." [redacted] replies, "But where does it say that at?" —while looking at the consent to search form for phone. Cpt. [redacted] responds, "You have that right—that's a—that's—a consent to search can be withdrawn at any time." [redacted] then asks, "But how am I gonna take the consent back?" Cpt. [redacted] answers, "Because we're gonna sit here and look at it right in front of you." [redacted] states, "Do I need to write a note on here that you told me that—I can stop the search?" Both officers responded that [redacted] did not have to write a note because that was a federal law that if he says

stop, they have to stop. [redacted] then proceeds to sign the consent to search form. *See iPhone Consent Form* attached as Exhibit C. Inv. [redacted] can then be seen on the recording looking through the phone for approximately 23 minutes before handing the phone to Cpt. [redacted], who looks through the phone for an additional 15 minutes. No child pornography was discovered on the phone during this consensual manual search.

There are several ways an examiner can search the contents of a phone. First, they can conduct a manual examination (like the one Cpt. [redacted] and Inv. [redacted] conducted on [redacted] 2021). This simply includes looking at information on the device as your average user would–by unlocking it and examining individual applications and data therein. These types of examinations do not allow the examiner to see metadata, deleted data, or access applications protected by internal passcodes. These searches can also incidentally alter or destroy data on the phone. Second, an examiner could conduct an "on site" forensic search using tools that allow them to examine some of the evidence on a device without doing a full extraction or "image" of the device. Finally, they can conduct a full forensic extraction by copying or "imaging" the device in order to later conduct a full "analysis" or search of a device.

On [redacted] 2021, the FBI utilized the Grayshift GrayKey tool v1.6.17 to conduct a full file system extraction of Mr. [redacted]'s iPhone SE. The data from that extraction was then uploaded to the Little Rock storage area network (SAN) shared drive. This means that the FBI created a forensic copy or "image" of the device that allowed them to examine everything a user of a device would see as well as metadata and even some deleted data that a user does not ordinarily have access to. This method also allows the government to repeatedly parse and search the data using analysis tools like Grayshift's ArtifiactIQ, Cellebrite's Physical Analyzer or Magnet Axiom. In other words, the forensic extraction and subsequent searches conducted in this case are the most

intrusive and thorough search that the government could have conducted and do not resemble a manual search. This second search far exceeded the reasonable understanding of Mr. [redacted]'s limited written consent. *See* [redacted] *Affidavit* attached as Exhibit D.

The second search fell outside the scope of consent because it was unconnected to the initial consent in time, place, or the agency conducting the search. Furthermore, the search conducted was inconsistent with the consent [redacted] provided in its level of invasiveness and the evidence sought. At no time during the interview was [redacted] advised that the FBI was conducting or would conduct its own investigation or that his phone would be transferred to a different agency for a separate investigation, neither was [redacted] advised that he was consenting to a forensic extraction of all cell phone data. He was advised that the officers would "look at" his phone while "sitting right in front of" him. Based on the FBI Process Report, on or about [redacted] 2021, approximately 60 days later, Agent [redacted] requested the forensic extraction based solely on the consent form signed by [redacted] on [redacted] 2021. *See FBI Process Report* attached as Exhibit E. Thus, on or about [redacted] 2021, a forensic examiner in the office of the FBI conducted a file system extraction of the phone. Thereafter, deleted incriminating file links were extracted from the phone and downloaded to a CD for storage.

Consent to a single search is not consent to multiple searches. *See United States v. McMullin*, 576 F.3d 810 (8th Cir.2009) (where defendant consented to entry of his home by U.S. Marshals seeking one Crowder, for whom they had an arrest warrant, and they then apprehended Crowder in back yard, where they now also detained defendant, "a new consent was required for the second entry" of the home; given that "the marshals had already completed their task of arresting Crowder," the "re-entry exceeded the scope of [defendant's] consent"); *United States v. Rahman*, 805 F.3d 822, 834 (7th Cir. 2015) ("the presumption is that once the basement was ruled

out as the origin of the fire, the search that Hankins conducted in the basement after he reached his conclusion was done for the purpose of searching for criminal activity".); *See also State v. Brochu*, 237 A.2d 418 (Me.1967); *State v. Lopez*, 78 Haw. 433, 896 P.2d 889 (1995) (fact defendants called police to report a robbery was a consent to initial police entry, but did not give "enforcement officials an implied license to enter their home" on subsequent occasions to seek evidence related to the robbery); *State v. Douglas*, 123 Wis.2d 13, 365 N.W.2d 580 (1985) (implied consent to enter to render emergency assistance is not "boundless" and did not cover second entry two days later). *State v. Marino*, 259 Or. App. 608, 314 P.3d 984 (2013); *People v. Cohen*, 87 A.D.2d 77 (2d Dep't 1982), aff'd, 58 N.Y.2d 844 (1983); *People v. Khativ*, 147 Misc. 2d 838 (Sup. Ct. Monroe Co. 1990). Nor is consent to search a single item permission to remove items for offsite search. *People v. Schmoll*, 383 Ill. 280, 48 N.E.2d 933 (1943); *United States v. Ibarra*, 955 F.2d 1405 (10th Cir.1992) ("The government asserts that defendant's consent to search his vehicle carried over to the second search of his car conducted at the lot to which the vehicle was towed. We hold that because an illegal seizure occurred following the initial consent, that consent does not 'continue' to justify the second search"); *Pinizzotto v. Superior Court for Los Angeles County*, 257 Cal. App. 2d 582, 65 Cal. Rptr. 74 (2d Dist. 1968); *State v. Brochu*, 237 A.2d 418 (Me. 1967); *State v. Jones*, 22 Wash. App. 447, 591 P.2d 796 (Div. 2 1979); *State v. Douglas*, 123 Wis. 2d 13, 365 N.W.2d 580 (1985).

It is unreasonable to suggest that [redacted] understood that the scope of his consent expanded beyond a manual search of his phone while in the presence of the two officers questioning him. He specifically inquired as to how to withdraw his consent and whether he should write a note on the consent form that he could withdraw his consent. The officers then told him that he did not need to write a note on the form because it was his right to withdraw consent at any time and that

they would conduct the search in front of him. The scope of [redacted]'s consent ends here and does not expand to a forensic extraction by the FBI over 60 days later. "The length of time a consent lasts depends upon the reasonableness of the lapse of time between the consent and the search in relation to the scope and breadth of the consent given. If the consent to search is voluntarily and knowingly given, and if the search takes place within a reasonable time of the consent and is limited to the scope and breadth thereof, a mere [uncommunicated] change of mind will not render the search violative of a defendant's Fourth Amendment rights." *Gray v. State,* 441 A.2d 209, 221 (Del. 1981). In that case the passage of time, 20 hours, was deemed reasonable, as defendant was in custody that entire time and the consent was to search his belongings in police custody, as to which there had been no change in that interval. *See also Shamaeizadeh v. Cunigan*, 338 F.3d 535 (6th Cir. 2003) (occupant of house who requested police to search house for intruder consented to first search in which no intruder found, but not second and third searches conducted with assistance of other officers prompted by suspicion of narcotics present).

A general or specific consent is not implied to include permission to look in areas not designed to be routinely opened or accessed. *See, e.g., Jimeno*, 500 U.S. at 251–52, 111 S.Ct. at 1804 (consent to search trunk for drugs is reasonably understood to permit opening of paper bag, but probably not "breaking open of locked briefcase within the trunk"); *United States v. Patacchia*, 602 F.2d 218, 219 (9th Cir.) (consent to search did not authorize officers to pry open car trunk), amended, 610 F.2d 648 (9th Cir. 1979); *United States v. Washington*, 739 F. Supp. 546, 550 (D. Or. 1990) (consent given to search trunk did not authorize removal of car seats to conduct search when proper key could not be located); S*tate v. Arroyo–Sotelo*, 131 Or.App. 290, 884 P.2d 901, 905 (1994) (broad consent given by defendant to search for narcotics and cash did not authorize officers to remove screws and pry panel from sidewall of car). *In Arroyo–Sotelo*, the Oregon court

of appeals asserted that "a general consent to search a car does not authorize an officer to search areas of a car that are not designed to be routinely opened or accessed." 884 P.2d at 905.

Consent to onsite search did not allow later offsite search. Even assuming arguendo the consent to search had been broadened to encompass an offsite search, the scope of the enlarged consent did not unambiguously extend in time beyond a few days. *United States v. Chopra*, No. 3:08-CR-16-J-32HTS, 2008 WL 2090671, at 4 (M.D. Fla. Apr. 10, 2008); *United States v. Escamilla*, 852 F.3d 474 (5th Cir. 2017) (where incident to vehicle stop defendant consented officer's request that he be allowed to "look through" defendant's phone, after which phone returned to defendant, that consent did not also cover post-arrest manual search of that phone, as officer's return of phone ended that search, and search at station was "a second, distinct search").

In the instant case, even though [redacted]'s phone was not returned to him at the conclusion of the interview, he was told that the search would take place in front of him. Therefore, when Inv. [redacted] and Cpt. [redacted] stopped looking through [redacted]'s phone while in front of him, the search to which [redacted] consented had ended. Inv. [redacted] told [redacted] that if he was in the same spot as [redacted], that he would tell "anybody in the world" to look in his phone. He said this to convince [redacted] to provide consent for he and Cpt. [redacted] to view the contents of [redacted]'s phone in his presence. The conversation led [redacted] to believe that he was consenting to a manual search of his phone during the interview in which both officers would view the phone as a normal user, not that they would transfer the device to the FBI to extract any data, deleted data, or metadata from the phone days after the interview.

III. The Contents of the SUBJECT COMPUTER and SUBJECT PHONE Must Be Suppressed Because the Government Waited 400 Days to Obtain a Search Warrant.

Here, the government, without a valid warrant, seized and retained Mr. [redacted]'s devices for an unreasonable period before seeking a warrant to search those devices. This is a constitutional violation that requires suppression. "[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.

The length of the delay: Where the government fails 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)).

In the instant case, the affidavit seeking to search the electronic devices was filed 400 days after the seizure of the devices, and the affidavit further relies upon a plethora of unconstitutionally obtained evidence in order to establish probable cause. Local law enforcement took possession of the SUBJECT COMPUTER and SUBJECT PHONE on [redacted] 2021, when it executed a search warrant at the Super 8 Motel based on a bare-bones affidavit. The items were then transferred to the FBI on or about [redacted] 2021, approximately 142 days later. [redacted] was indicted by a grand jury on [redacted] 2022, 222 days after the FBI took possession of the SUBJECT COMPUTER and SUBJECT PHONE. Still, no search warrant was sought for the items held in the FBI's possession until another 36 days. "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 far beyond one month to seek a search warrant for the property seized. The court in *Smith* gave independent weight to the length of delay and concluded that a month-long well exceeds what is ordinarily reasonable.

The importance of the seized property to the defendant: "[O]ur 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* 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. Granias*, 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." *Smith* at 207. 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)). "The upshot is that the search and seizure of personal electronic devices like a modern cell phone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person's ordinary effects." *Id.*

In the case at bar, law enforcement sought a warrant to search [redacted]'s motel room and seized [redacted]'s Lenovo laptop and his Apple iPhone 12 that he had on his person. [redacted] was released from the [redacted] 2021, arrest, and remained on state bond. While on bond for the alleged drug charges, he requested the return of his laptop and iPhone. It is expected that he may have had personal tax or banking information, medical records or personal diaries on the laptop interspersed among the evidentiary material. In addition, his smartphone would be used in a similar manner, to house important contact information, electronic banking data, and other private information. It is widely known and accepted that laptop and smartphone users place high priority and value on their

electronic devices because of their capabilities, storage capacities, camera functions, and ease of use in accessing personal information while on the go.

Whether [redacted] had a reduced property interest in the seized item: 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. In the alternative, one's property interest may be diminished because of the existence of probable cause. *Id.* at 208. 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, [redacted] did not consent to a seizure or search his Lenovo laptop, nor his Apple iPhone 12. Both were taken upon local law enforcement's execution of the Super 8 Warrant for alleged drug activity. As argued, the Super 8 Warrant was obtained by a bare-bones affidavit that failed to establish that the confidential informant was in fact reliable. [redacted]'s possessory interest in his property was not diminished by probable cause. Before obtaining the electronics search warrant for the SUBJECT COMPUTER and SUBJECT PHONE, Officer [redacted] was uncertain of what the search would reveal, stating in her affidavit that "…DTF Agents observed what they believed may have been child pornography on the SUBJECT COMPUTER, which was powered on, unlocked and open at the time." (See Electronics Warrant, p. 3). In *Smith*, officers also thought

that they may have seen child pornography on the defendant's tablet; however, no distinct descriptions were provided. "Similarly, Snickles' deposition statement on the day of the seizure described the female genitalia he saw on the tablet screen as 'bald' but without description of age, stating only that '[t]he electronic device was secured as it may pertain to a possible illegal sexual encounter with a female.'" 967 F.3d at 209. "The tablet's evidentiary value turned solely on what the police might find from a search of its contents." *Id.* The information concerning what *may* be present on [redacted]'s laptop was even more vague and ambiguous. Thus, throughout her affidavit, Officer [redacted] relied heavily on a plethora of contents gained from unlawful searches in order to establish probable cause to search the electronic items seized. Even if probable cause arguably existed to seize the items, law enforcement's interest was delimited by its obligation to seek a search warrant without unreasonable delay.

The strength of the government's justification for the delay: "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 [redacted]'s laptop and iPhone on [redacted] 2021, and then transferred such to the FBI on or about [redacted] 2021. The FBI held possession of [redacted]'s property for 159 days before providing an update concerning the electronics seized. Thus, on or about [redacted] 2022, an FBI electronic communication case status update was prepared. *See FBI Case Update* attached as Exhibit F. The update stated that TFO [redacted] had begun authoring a federal search warrant affidavit for [redacted]'s laptop and iPhone seized on or about [redacted] 2021, and that the affidavit was expected

to be submitted within one week of that electronic communication. The affidavit was not submitted until another 99 days, totaling 400 days after the initial seizure of the devices.

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* at 211. In the instant case, Officer [redacted]'s delay amounted to gross negligence. Therefore, the 400-day delay in seeking a valid warrant to search the SUBJECT COMPUTER and SUBJECT PHONE was a violation of the Fourth Amendment and suppression is required.

IV. The Electronics Warrant is the Fruits of Unlawful Dropbox and Google Warrants, As Well As a Search Beyond the Scope of Consent.

The Electronics Warrant is comprised of compounded information that should be suppressed and is such the fruit unlawful searches and seizures. The affidavit references the Dropbox Warrant, which gave the government access to search beyond the scope of the CSAM identified by Dropbox software[2]. Any incriminating evidence obtained because of the Google Warrant should be suppressed because the warrant was overbroad and insufficiently particular as to what the government could search for and seize and because Agent [redacted] deceived the magistrate as to the nature of Google's storage of the contraband in this case[3]. Additionally, the Electronics Warrant Affidavit relies on information illegally obtained from Mr. [redacted]'s iPhone SE, as a result of an unlawful extraction of the contents of such iPhone. For these reasons, any evidence obtained as a result of the Electronics Warrant is fruit of the poisonous tree and must be suppressed.

[2] *See* Defendant's Motion to Suppress Contents of Dropbox Account and Brief in Support.
[3] *See* Defendant's Motion to Suppress Contents of Google Contents and Brief in Support.

Conclusion

WHEREFORE, the Defendant, [redacted] respectfully requests that his Motion be granted; that all contents of the SUBJECT LAPTOP, SUBJECT PHONE, and the Apple iPhone SE be suppressed, along with any evidence or other statements obtained, directly or indirectly, as a result of the electronics warrant sought on [redacted] 2022; that he be granted a hearing on this matter if the Court should deem it necessary; that he be given the opportunity, if necessary, to file a post-hearing brief based on evidence that may be elicited at any hearing that is held; and for all other relief to which he may be entitled.

Respectfully submitted,

[redacted]
FEDERAL PUBLIC DEFENDER
WESTERN DISTRICT OF ARKANSAS

By: /s/ [redacted]

Counsel for Defendant

CERTIFICATE OF SERVICE

I hereby certify that I have electronically filed the foregoing with the Clerk of the Court using the CM/ECF System which will send notification of such filing to Mr. [redacted] Assistant United States Attorney, and a copy of this pleading was mailed by the United States Postal Service to: none.

/s/ [redacted]