UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

THE UNITED STATES OF AMERICA

Plaintiff,

v.

JOHAUN LAMONT HOWLAND,

Defendant.

Case No. 1:18-CR-140

Hon. Janet T. Neff
U.S. District Court Judge

DEFENDANT'S MOTION FOR RECONSIDERATION

Defendant Johaun Howland, through counsel, moves this Court for partial relief from the Court's June 7, 2019 Order (RE: 352, PageID #1511-13). This motion is captioned "Motion for Reconsideration" solely because the ECF system has no filing category for a motion seeking relief from an Order.

IN SUPPORT THEREOF, Defendant states:

1. On June 7, 2019, this Court set a deadline for filing a motion to suppress of August 5, 2019, and further set a page limit on a supporting memorandum of 30 pages.

2. Defendant has completed briefing on suppression issues.

3. Defendant raises 16 suppression issues in this case.

4. Briefing totals 71 pages.

5. Defendant believes that these pages are required in order to fully brief the issues.

6. Defendant has done everything possible to limit the length of his brief.

WHEREFORE, Defendant moves this Court for relief from the page limit identified in the Court's Order of June 7, 2019, and requests the Court for permission to file the attached memorandum in support of his motion to suppress.

Date: August 5, 2019

SCOTT GRAHAM PLLC

By: /s/ Scott Graham
Scott Graham, Attorney for Defendant

Business Address:
1911 West Centre Avenue, Suite C
Portage, Michigan 49024
(269) 327.0585

THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

THE UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHAUN LAMONT HOWLAND,

Defendant.
_____/

Case No. 1:18-CR-140

Hon. Janet T. Neff
U.S. District Court Judge

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS

I. The application for the wiretap of phone 9351 was deficient and the evidence derived under it should be suppressed: the application failed to establish that authorities had tried normal investigative procedures and that these procedures had failed or that such procedures reasonably appeared unlikely to succeed or would be too dangerous. The application thus failed to establish the necessity of the wiretaps and resulted in insufficient orders and unlawful interceptions.

The Fourth Amendment protects against unreasonable searches and seizures and can provide a means for attacking illegal wiretaps. *See, e.g.*, *United States v. Renzi*, 722 F. Supp. 2d 1100, 1104 (D. Az. 2010) (noting a magistrate's finding of Title III and Fourth Amendment violations). Congress has also enacted a statutory rubric to govern wiretaps. Mr. Howland now challenges the wiretap of phone 9351 on both statutory and constitutional grounds. In drug investigations, the government may apply for judicial authorization to intercept wire and oral communications. 18 U.S.C. § 2516(1)(e). Section 2518, in turn, lays out the procedure for the government to obtain authorization for such wiretapping. *See* 18 U.S.C. § 2518(1). The government must provide, among other things, a statement regarding the necessity of the wiretap, of why "other investigative procedures" have failed or would not succeed if tried or would be too dangerous. *See* 18 U.S.C. § 2518(1)(c). Under this rubric, to issue the authorization, a judge must find probable cause to believe that an individual is committing an offense,

that the interception will produce communications about that offense, that normal investigative procedures will not succeed, and (in some circumstances) that the facilities involved are being used in connection with the offense. 18 U.S.C. § 2518(3). The government may not present evidence, in any proceeding, derived from intercepted communications unless disclosure of the communication, or other evidence, comes in accordance with the provisions of these statutes. 18 U.S.C. § 2515; *see also United States v. Giordano*, 416 U.S. 505, 508 (1974).

If the target of an interception (or any "aggrieved person") believes an interception was unlawful, they may move the court to suppress the interception and evidence derived from it. 18 U.S.C. § 2518(10). In the case at hand, Mr. Howland qualifies as an aggrieved person and may challenge the interception. *See* 18 U.S.C. § 2510(11) (defining "aggrieved person" as "a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed"); *see also* Case No. 1:18-MC-28, RE. 3, PageID # 29 (alleging "JOHAUN HOWLAND's ongoing use of wire and electronic communications to and from Target Phone I . . . with certain Target Subjects . . . (collectively, the 'Interceptees of Target Phone I' or 'Interceptees')).

An aggrieved person, like Mr. Howland, may argue that authorities unlawfully intercepted communications and that the order authorizing the interception was insufficient on its face. 18 U.S.C. § 2518(10)(a)(i) & (ii); *see also United States v. Gray*, 372 F. Supp. 2d 1025, 1035 n.5 (N.D. Ohio 2005) (discussing parallel interpretation of these two prongs of the suppression analysis in a case involving a challenge based on the insufficient identification of the authorizer of an application). In considering such challenges, courts generally cannot go beyond "the information that the United States submitted to the judge who issued the wiretap order." *See United States v. Roybal*, 46 F. Supp. 3d 1127, 1149 (D.N.M. 2014). Four-corners review thus varies a bit in this context. *Id.* An issuing judge may require that the government produce additional testimonial or documentary evidence in support of a wiretap application. So "the information before the issuing judge includes the Applications, Affidavits and

Orders authorizing the wiretaps and also the 'testimonial or documentary evidence' introduced at the *in camera* proceedings before the issuing judge." *Id.* at 1149-50. The defense may obtain all these materials in the context of seeking suppression of wiretap evidence. *See id.* at 1168; *see also id.* at 1169 n.7 (suggesting the breadth of discovery in this context may include wiretap progress reports in some circumstances, including situations in which the government sought an extension to a wiretap). Mr. Howland currently has the application materials the government filed in this matter. If additional testimonial or documentary evidence related to the application exists, Mr. Howland asks the Court to order its disclosure, so he can address such evidence in this suppression context.

The government has failed to present the required complete statement, with specific allegations, regarding why tradition investigative procedures could not suffice in these circumstances. In judging the sufficiency of a wiretap application, courts "require a full and complete statement of specific allegations indicating why normal investigative procedures failed or would fail in the particular case." *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001). In *Blackmon*, the Ninth Circuit granted suppression in the wiretap context because "the application contain[ed] only generalized statements that would be true of any narcotics investigation." *Id.* at 1208. The application lacked the "specific facts necessary to satisfy the requirements of § 2518(1)(c)." *Id.* It also failed to go much beyond "boilerplate conclusions that merely describe inherent limitations of normal investigative procedures." *Id.* at 1210.

Regarding this "necessity requirement," the Sixth Circuit has explored the requirement that a wiretap application contain a statement related to the use of "normal" investigative procedures and why such procedures will not work in the case; the circuit has emphasized that the necessity requirement aims at ensuring that authorities do not resort to wiretaps in situations where traditional investigative techniques would suffice to expose an offense. *United States v. Rice*, 478 F.3d 704, 710 (6th Cir. 2007). The requirement protects against the impermissible use of wiretaps as first steps in

investigations. *Id.* The statutory rubric asks investigators to "give serious consideration" to non-wiretap techniques before they apply for wiretap authority. *Id.* The requirements ask authorities to inform courts of the reasons for the investigators' beliefs that non-wiretap techniques have not or will not succeed. *Id.* While an officer's prior experience may be relevant in analyzing whether other investigative procedures are likely to succeed if tried, "a purely conclusory affidavit unrelated to the instant case and not showing any factual relations to the circumstances at hand" will not suffice to comply with the statute. *Id.*

Because the necessity requirement sits as a statutory requirement to obtain wiretapping authorization, "and because suppression is the appropriate remedy for a violation under Title III," when "a warrant application does not meet the necessity requirement, the fruits of any evidence obtained through that warrant must be suppressed." *Id.* Mr. Howland's case merits such suppression, and the Sixth Circuit's decision in *Rice* provides support for this conclusion. In *Rice*, the court boiled the matter down to the wiretap application containing assertions that the confidential informant had been unable to make contact with the defendant and was thus of no use; "that pen registers and telephone tolls revealed possible connections to other people with histories of drug-related arrests"; and "generalized and uncorroborated information about why grand jury subpoenas, witness interviewing and search warrants, and trash pulls would not be useful." *Id.* at 711. The court affirmed the district court's suppression of the evidence derived from the wiretap. *Id.* Problems similar to those found in *Blackmon* and *Rice* appear in the wiretap application for phone 9351. Mr. Howland will discuss individually—and explore the deficiencies of—each of the sections of the application related to alternative investigatory methods.

Physical Surveillance

The application described an alleged incident, on March 14, 2018, with Mr. Howland supposedly stopping at three different gas stations, parking near pumps, and then moving on,

ostensibly demonstrating his consciousness of surveillance. *See* Case No. 1:18-MC-28, RE. 3, PageID # 53-54. The incident supposedly demonstrated that physical surveillance would not provide an effective investigation technique. *See* Case No. 1:18-MC-28, RE. 3, PageID # 53 (alleging that "members of the DTO [drug-trafficking organization] have effectively thwarted law enforcement attempts at surveillance, as noted below," and citing the March 14 surveillance in the next paragraph). The affiant explicitly disclaimed seeing Mr. Howland exit his vehicle: "During these stops, investigators did not observe HOWLAND get out of the vehicle, obtain gas or meet with anyone." *See* Case No. 1:18-MC-28, RE. 3, PageID # 54. The affiant then alleged that investigators saw Mr. Howland engage in a drug transaction at the Pita House. *See* Case No. 1:18-MC-28, RE. 3, PageID # 54.

As will become a crucial issue for Mr. Howland's motion for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), however, and in a way that deeply undermines the affiant's assertions of necessity because the assertions are less than credible as presented, this description of the March 14 investigation does not parallel other investigator accounts of that day. In the applications for the warrants for the Lantana Drive and Neland Avenue residences (which share extremely similar affidavits), the affiant (who happened to be the same affiant who filed the wiretap application) described March 14, 2018, under a heading reading "March 14, 2018, Surveillance of HOWLAND Conducting a Suspected Drug Transaction."[1] *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 19.

The affiant discussed investigators conducting surveillance on March 14, 2018, and using phone pings (authorized under a separate warrant) to place Mr. Howland on Kinnrow Avenue in Grand Rapids. Case No. 1:18-MJ-135, RE. 1-1, PageID # 19. Around 3:30 p.m., investigators saw a

[1] The Lantana Drive and Neland Avenue warrants constitute the fruit of the poisonous tree of the wiretaps and thus cannot stand; all evidence seized under them should be suppressed. These warrants relied on the phone-ping warrants that represent constitutional infirmities, and they relied on this infirm wiretap of phone 9351. In a separate motion, Mr. Howland will argue for suppression of all evidence discovered through these problematic warrants.

white Infiniti SUV, with Pennsylvania plates (a Hertz rental vehicle) parked in the driveway of the Kinnrow Avenue residence at which the phone pings placed Mr. Howland. Case No. 1:18-MJ-135, RE. 1-1, PageID # 19. (Investigators had earlier seen the vehicle outside the Lantana Drive residence, Mr. Howland's assumed residence. Case No. 1:18-MJ-135, RE. 1-1, PageID # 19.) About twenty minutes later, investigators watched the Infiniti leave the Kinnrow Avenue driveway and make its way to a Marathon gas station (at an intersection of Franklin Street). Case No. 1:18-MJ-135, RE. 1-1, PageID # 19. GPS data for Mr. Howland (from two cell phones) showed Mr. Howland moving with the vehicle. Case No. 1:18-MJ-135, RE. 1-1, PageID # 19. Investigators saw Mr. Howland exit the vehicle and enter the Marathon station, where he supposedly stayed for approximately five minutes. Case No. 1:18-MJ-135, RE. 1-1, PageID # 19.

Investigators then watched the SUV leave the Marathon and head directly to a BP gas station (at the corner of Franklin Street and Eastern Avenue). Case No. 1:18-MJ-135, RE. 1-1, PageID # 19-20. The affiant claimed investigators saw Mr. Howland exit the Infiniti and go into the BP, staying for about five minutes. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. He then returned to the vehicle. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. The SUV then supposedly headed to the Pita House (on Wealthy Street). Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. The Infiniti allegedly parked next to a gold Chevy Equinox. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. The affiant alleged investigators claimed they observed a man approach the Infiniti and get in the passenger-side door. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. About seven minutes later, investigators claim to have seen Mr. Howland and the other man leave the SUV and "talk outside of the vehicle for a couple of seconds." Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. The unknown male than got into the Chevy Equinox, which sat beside the Infiniti. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. Mr. Howland, the affiant said, appeared "to be speaking to someone in the rear passenger's side of the gold Chevy

Equinox for a minute before returning to his vehicle." Case No. 1:18-MJ-135, RE. 1-1, PageID # 20. Both vehicles then left the Pita House parking lot. Case No. 1:18-MJ-135, RE. 1-1, PageID # 20.

This description of the afternoon's surveillance of Mr. Howland on March 14, 2018, is a far cry from the description in the wiretap application for phone 9351. In this description, Mr. Howland goes into the "mini-marts" at the gas stations. He does not try to "clean" any possible surveillance. He goes into the stores to conduct business, purchase the things people buy at such shops, use the restroom, or whatever else people do at those convenience stores. This situation can hardly be described—truthfully—by saying, "During these stops, investigators did not observe HOWLAND get out of the vehicle, obtain gas or meet with anyone." *Cf.* Case No. 1:18-MC-28, RE. 3, PageID # 54.

These blatant discrepancies between the affidavits' descriptions of the same incidents deeply undermine the veracity of all the warrants citing the incidents and undercut any sense of a necessity for the wiretap of phone 9351. And one cannot attribute these discrepancies to the affiant's lack of awareness, as though investigators provided her with mismatched accounts of their investigations. In the tracking-warrant application for the white 2017 Ford pickup truck[2] (signed by Magistrate Judge Kent on April 6, 2018), the affiant (the same affiant for the wiretap application and the Lantana and Neland residences) describes herself as having conducted the surveillance of Mr. Howland on March 14, 2018, with another officer (DEA TFO Schafer). *See* Case No. 1:18-MJ-97, Continuation of Application for Tracking Warrant, at 5 (defense counsel does not have ECF-stamped copies of these sealed records). No excuse exists for these flagrant misstatements.

While distinctions exist, *Blackmon* provides a helpful comparison here. In that case, the court rejected the idea "that we can extrapolate from this single example that surveillance against Blackmon

[2] As with the Lantana Drive and Neland warrants, this warrant constitutes fruit of the poisonous tree. For example, it relies heavily on the wiretap warrant at issue in this memorandum. All evidence derived under the tracking warrant should be suppressed, as Mr. Howland will discuss in his motion to suppress derivative evidence.

would be unsuccessful or dangerous," finding instead that such a position was "belied by the record which shows that government informants had established observation posts within the [housing project] and were providing agents with daily surveillance of the individuals entering Blackmon's apartment." *Blackmon*, 273 F.3d at 1209. The court concluded "that the surveillance section of the Blackmon wiretap application contained material misstatements and omissions that worked to conceal the fact that necessity had not been established." *Id.*

While Mr. Howland will dig into the material misstatements and omission in his separate motion (and supporting memorandum) seeking a hearing under *Franks*, he would point out here that agents were conducting surveillance and effectively gathering evidence through that surveillance. While the material misstatements make it impossible to know exactly what that surveillance had revealed, all the versions of the recitations of the March 14 surveillance reveal that surveillance was effective and could have remained effective if authorities had pursued it further.

Confidential Informants and Undercover Agents

After detailing a "falling out" a confidential informant had with Mr. Howland, the affiant made general statements about drug dealers being "reticent" with people they do not know. Case No. 1:18-MC-28, RE. 3, PageID # 58-59. She went on to explain general hurdles to gaining information through informants and undercover agents. Case No. 1:18-MC-28, RE. 3, PageID # 59-60. Finally, the affiant made sweeping, unscientific assertions about the dangers of fentanyl exposure. *See* Case No. 1:18-MC-28, RE. 3, PageID # 60.

These hyperbolic assertions about the risks of fentanyl exposure cannot withstand scientific scrutiny. As Mr. Howland will explain in his separate motion for a *Franks* hearing, medical doctors and researchers have debunked the idea that fentanyl exposure precludes effective first-responder and law-enforcement reactions to fentanyl overdoses and dealing. As to the other general assertions about the impracticality of using informants and undercover agents, this affidavit suffers from the same

infirmities as the affidavit in *Blackmon*, where the court pointed out that "[t]hese statements would be true of most or all drug conspiracy investigations, and the limitations on the usefulness of informants, no matter how successful or potentially successful to the particular operation, would support the necessity of a wiretap." *Blackmon*, 273 F.3d at 1210. The generic nature of statements such as "drug dealers know it is in their best interest to reveal as little as possible" and "witnesses cannot lead to the prosecution of an entire drug organization" will "not dissipate simply because the government claims a vast investigative purpose." *Id.* at 1211.

Witness Interviews and Grand Jury Subpoenas

All of the affiant's statements regarding questioning witnesses fall into this troubling class of generic assertions. The affiant's insistence that interviewing witnesses would not aid the investigation also comes up short because of circular reasoning. In paragraph 78 of the affidavit in support of the wiretap application, the affiant stated: "For example, additional subject interviews may alert the Target Subjects to the existence of the investigation, particularly if law enforcement officers questioned a Target Subject regarding events that law enforcement has learned about based on calls or text messages intercepted from Target Phone 1 during the course of this investigation." Case No. 1:18-MC-28, RE. 3, PageID # 61. The affiant essentially asserts that the wiretap is necessary because if authorities were to discuss with witnesses evidence discovered through the wiretap these witnesses would warn the targets of the investigation. Defense counsel fails to see how a finding of necessity for a wiretap can rest on the potential for exposure of an investigation based on revealing communications discovered through that wiretap.

The affidavit's disclaiming of the potential utility of target-subject interviews again just devolved into boilerplate, lacking case-specific claims of difficulty (beyond a broad statement that the alleged drug organization supposedly involved associations with people who would likely be loyal to the alleged organization). *See* Case No. 1:18-MC-28, RE. 3, PageID # 61. The affidavit failed to allege

unsuccessful or fruitless attempts at interviews. *See* Case No. 1:18-MC-28, RE. 3, PageID # 60-62. The affiant simply fell back on *experience*, rather than case circumstances, to explain the supposed necessity for the wiretap she sought. Interestingly, the affidavit discounted the value of historical call data by saying that "subpoenas for historical call contact between the **Target Offenses** [sic] would provide only limited—and in the case of some service providers, no—information about electronic text message contact between the targets of the investigation." *See* Case No. 1:18-MC-28, RE. 3, PageID # 62. Not only does this statement represent a conclusory assertion that fails to establish investigative *necessity*, it is almost verbatim the same statement affiants habitually use in these applications, a fact that demonstrates the complete lack of specificity and particularized effort common to these wiretap applications. *Compare United States v. Stovall*, No. 1:18-CR-251 (W.D. Mich. Nov. 21, 2018) (RE. 206, PageID # 279 (quoting almost identical language in the same context)). This statement also demonstrates that agents did not even try to pursue these subpoenas and did not know conclusively what such an investigation would produce.

Searches

Regarding searches, the affiant rejected the idea on generic grounds. Case No. 1:18-MC-28, RE. 3, PageID # 62. She also made statements that defense counsel finds incongruent. For example, the affiant claimed that, "due to the presence, historical quantity, and dangerous qualities of fentanyl, investigators are limited to the addresses that have been identified." Case No. 1:18-MC-28, RE. 3, PageID # 63. She pointed out as an example the idea that, "as these parcels are seized by law enforcement, the DTO may continue to utilize the United States Postal Service. However, they likely will not again ship a package to an address tied to a previous seizure." Case No. 1:18-MC-28, RE. 3, PageID # 63. As already touched on, Mr. Howland will discuss in his *Franks* motion medical and scientific literature related to the overstatement of the dangers of fentanyl. Regardless, these supposed

"dangers" hardly seem like they would affect the addresses to which traffickers would send drugs or somehow limit officers' identification of other addresses.

In *Rice*, the Sixth Circuit emphasized that the statements in the affidavit, related to the use of search warrants, amounted to generic assertions. *See Rice*, 478 F.3d at 708. The district court there had found that the explanations the authorities offered for not attempting to use searches, grand-jury investigation, subject interviews, and trash pulls all suffered from the same problem: The explanations centered around *typical problems* with the techniques in *typical drug cases* but failed to refer to any facts specifically about the defendant. *Id.* While the district court, and the later-reviewing Sixth Circuit, mentioned the credibility issues related to the affidavit, the generic nature of the assertions led the discussion on this particular point. *See id.* at 708, 711. The *Rice* court made this point clear: "After reviewing the record, we find that the district court was not in error in concluding that what was left of the Wenther Affidavit did not provide 'a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.'" *Id.* at 711. On these grounds, the court affirmed "the district court's decision to suppress the fruits of the wiretap." *Id.* The *Rice* decision carries significant guiding weight for the current analysis.

Pen Register, Trap and Trace, and Telephone Analyses

The affiant conceded effective use of these investigatory methods. *See* Case No. 1:18-MC-28, RE. 3, PageID # 65. In discussing the limits of these methods, the affiant merely pointed out their limits in general—falling back on that approach rejected by the *Blackmon* (and *Rice*) court. *See, e.g.*, *Blackmon*, 273 F.3d at 1211. In upholding suppression of wiretap evidence, the Sixth Circuit in *Rice* discussed that district court's finding that the pen-register section of the affidavit focused on "general language" regarding the usefulness of pen registers. *Rice*, 478 F.3d at 708. The only case-specific information in *Rice* related to a statement that "within the limitations of the technology, the pen

register has been as useful as it possibly can be—linking [the defendant] with other individuals with known drug histories." *Id.* The affidavit lacked specifics as to the calls traced. *Id.* The affidavit here in Mr. Howland's case is similarly deficient. *See* Case No. 1:18-MC-28, RE. 3, PageID # 65-66.

Trash Pulls

In speaking of trash pulls, the affiant again made blanket, generic statements about the limits of the investigatory method. *See* Case No. 1:18-MC-28, RE. 3, PageID # 66-67. She also raised the specter of the "dangers" of fentanyl again and the possibility that officers "may inadvertently come into direct contact with fentanyl residue, and/or contaminated narcotics paraphernalia containing fentanyl." Case No. 1:18-MC-28, RE. 3, PageID # 67. Another problem with these assertions arises because the investigation itself would reveal their insubstantial support just two weeks after the affiant filed the wiretap application.[3] In the warrant applications for the Lantana Drive and Neland Avenue residences, the same affiant described a very successful trash pull. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 26; Case No. 1:18-MJ-139, RE. 1-1, PageID # 26.

As the affiant recounted the trash pull, "[a]n employee of Valleywood Apartments informed investigators that he had seen HOWLAND rip the label off the box before placing it in the dumpster." Case No. 1:18-MJ-135, RE. 1-1, PageID # 26; Case No. 1:18-MJ-139, RE. 1-1, PageID # 26. Investigators retrieved "the box from the dumpster that HOWLAND had utilized to throw away the box" and "[t]he box was a FedEx shipping parcel with a partial label attached." Case No. 1:18-MJ-135, RE. 1-1, PageID # 26; Case No. 1:18-MJ-139, RE. 1-1, PageID # 26. This "label read: ORIGIN ID: Shanika Yvette DAUGHTRY" and gave an address on Walnut Avenue in Las Vegas, Nevada. Case No. 1:18-MJ-135, RE. 1-1, PageID # 26; Case No. 1:18-MJ-139, RE. 1-1, PageID # 26. A cooperating informant had told authorities with ATF in California that "DAUGHTRY is a girlfriend

[3] This successful trash pull also undermines the idea that physical surveillance and the use of informants would remain inadequate or unfruitful.

of COLBERT," who "is a source of supply for the HOWLAND DTO." Case No. 1:18-MJ-135, RE. 1-1, PageID # 26; Case No. 1:18-MJ-139, RE. 1-1, PageID # 26.

A different affiant described this trash pull in his application for a warrant to seize and search a Priority Mail Express package (with a tracking number ending 8863US) (Mr. Howland challenges this search and seizure later in this memo). *See* May 9, 2018 Application for Search Warrant for Priority Mail Express Parcel, at 3-4, ¶ 13; 6-7, ¶ 19. Given this success with trash pulls, one is likely to feel incredulous toward the affiant's assertions, in the wiretap application, related to the supposed futility of using trash-pull investigation methods.

Mobile Tracking Devices

This section of the affidavit concedes the usefulness of vehicle trackers—and the effectiveness of physical surveillance in identifying vehicles for which to apply for tracking warrants. *See* Case No. 1:18-MC-28, RE. 3, PageID # 67-68. The discussion of the limits of tracking for gathering information on the scope of the alleged drug organization devolved into those generic assertions related to the limits of the method—tracking—in general. And the assertion that the tracking data would not yield bases "to obtain warrants to search any particular locations" cannot stand up under the reality that tracking data regularly, and effectively, appears in search-warrant applications for premises.

Video Surveillance

In this section, the affiant stated, "[b]y their nature, surveillance cameras suffer the same limitations as physical surveillance: they provide limited direct evidence of the significance of the meetings." Case No. 1:18-MC-28, RE. 3, PageID # 69. Yet she went on to say, "[w]hen used in conjunction with wire and electronic communication interception, however, physical surveillance has proved to be a useful investigative technique." This thought process evidences exactly the willingness to skip to the traditional investigative methods, mandated by statute, and jump right to wiretapping

that courts like those in *United States v. Aileman*, 986 F. Supp. 1228, 1240 (N.D. Cal. 1997), discussed below, have condemned.

Mail Covers

The affiant argued the ineffectiveness of mail covers because packages may not display real names. *See* Case No. 1:18-MC-28, RE. 3, PageID # 69. But the affiant also explained that mail covers involve a postal carrier reporting on all packages delivered to a given *address*, so a lack of knowledge of specific names would not excessively hinder the effectiveness of using a mail cover. *See* Case No. 1:18-MC-28, RE. 3, PageID # 69. While not knowing all relevant addresses could limit the effectiveness of using mail covers, it would not obviate that effectiveness completely. As with other sections on investigative techniques, the affiant returned to the generic and jumped directly to the need for a wiretap: "Therefore, a mail cover by itself is unlikely to identify all of the members or activities of the enterprise and conspiracy, and would not allow law enforcement officers to reach the goals of the investigation." Case No. 1:18-MC-28, RE. 3, PageID # 70. Mail covers should not, alone, answer all investigatory needs. They provide one arrow in the many-arrowed investigatory quiver. To act as though this shortcoming of being a single tool gives rise to the necessity for the extreme measure of tapping a phone mocks traditional investigation skills.

Other Investigations

This section detailed what sounded like effective investigation efforts by multiple agencies in California and Michigan. *See* Case No. 1:18-MC-28, RE. 3, PageID # 70-71. The affiant discussed the evidence discovered being "limited" but provided no details of what "limited" meant—no details for a court to judge the effectiveness of these investigation efforts and whether a wiretap truly was necessary. Statements like this one provide no basis for a reviewing court to make an informed determination: "However, the USPS has developed limited evidence regarding real time evidence relating to the DTO outside of the 'known' addresses utilized for destinations for narcotics related

parcels, and/or the organizational structure of the DTO." *See* Case No. 1:18-MC-28, RE. 3, PageID # 71. Such statements thus contribute essentially nothing to a real "necessity analysis."

Financial Investigations

This section again presented the idea that these investigatory methods "alone" would not uncover all information necessary to result in convictions. *See* Case No. 1:18-MC-28, RE. 3, PageID # 72. But as already discussed, this myopic approach to each investigatory method ignores the obvious need for a multi-pronged investigation. No one is asking investigators to obtain convictions using a single investigation technique. But Congress does ask investigators to make a real effort to engage in their work using a multi-pronged approach before investigators can resort to wiretaps. After falling back on generic training-and-experience comments, the affiant even acknowledged the need for a "combination of investigative techniques." *See* Case No. 1:18-MC-28, RE. 3, PageID # 72. The affiant stated that "most" of the subpoenas issued remained pending at the time of the wiretap application. *See* Case No. 1:18-MC-28, RE. 3, PageID # 73. With these subpoenas still pending at the time, one struggles to see how a wiretap could be "necessary"—the use of financial-investigation techniques had not been completed. Indeed, the affidavit described a successful-sounding financial investigation, one that included a confidential source making disclosures (and thus further eroding the idea of confidential sources being futile). *See* Case No. 1:18-MC-28, RE. 3, PageID # 72.

Having considered each of these sections on investigatory options, one can consider the affidavit as a whole. Much of what the affiant said regarding "traditional" investigatory techniques echoes statements made in other wiretap applications. *See, e.g.*, *United States v. Stovall*, No. 1:18-CR-251 (W.D. Mich. Nov. 21, 2018) (RE. 206, PageID # 278-83 (discussing generic and boilerplate assertions in wiretap application)). This general, generic plea of necessity for a wiretap rings insincere in light of its regular appearance in most wiretap cases. As the Sixth Circuit has admonished, the government and issuing courts should use the statutory authority granted for wiretapping "with restraint" and only

when circumstances warrant such surreptitious interception. *See United States v. Gray*, 521 F.3d 514, 521 (6th Cir. 2008). The *Gray* court clarified that one may challenge a wiretap for not just constitutional violations but also for violations of the statutory authority. *Id.* at 522. In delineating the statutory violations warranting suppression, the court said that technical defects may not require suppression, but investigators, prosecutors, and courts must honor the statutory protections required, such as that requiring that "[t]he mature judgment of a particular, responsible Department of Justice official [be] interposed as a critical precondition to any judicial order." *See id.* at 522, 524. In considering a challenge to a wiretap application, courts will consider whether Title III's "essential safeguards" have been undermined. *See id.* at 527. As in *Rice* and *Blackmon*, the affidavit in support of the wiretap of phone 9351 indeed failed to honor these Title III statutory safeguards.

While district courts wrestling with these issues must apply the varied rules of their circuits, one can see general trends and themes in their decisions. In *United States v. Ailemen*, 986 F. Supp. 1228, 1244 (N.D. Cal. 1997) (this citation produces the magistrate's report and recommendation at 1242 to 1314 and the district court's adoption of that recommendation at 1230 to 1242), the magistrate judge recommended suppression of the challenged wiretap evidence. The judge felt that the government had failed to make the required "good faith effort" to generate the evidence it sought through "normal investigative techniques." *Id.* at 1245. Relative to the alleged magnitude of the case and the alleged high priority of the investigation to the government, the government had failed to devote "reasonable resources over a reasonable period of time to normal investigative methods." *Id.* The *Aileman* district court considered boilerplate, generic assertions about the insufficiency of traditional methods to uncover evidence related to the drug conspiracy. It found that "[s]uch generic language is far from specific about the inability of traditional methods to uncover specific information." *Id.* at 1240. The Ninth Circuit, the court explained, "explicitly prohibited such 'sidestepping' of the necessity requirement with general allegations about 'drug conspiracies.'" *Id.* The court found "that the three

main categories of information, as well as the smaller details, sought by the wiretap could have been discovered by traditional means." *Id.* The generic nature "of the necessity section coupled with its one-sided account of the defects in the ongoing investigation effectively misled the issuing judge about the promise of traditional investigative methods." *Id.* at 1242.

The *Ailemen* district court and magistrate judge recognized that wiretaps threaten "core values in our society" and constitute a "highly intrusive" investigatory technique. *Id.* at 1231 (in opinion of district court adopting magistrate's report and recommendation), 1246 (in magistrate's opinion). The magistrate judge pointed out the government had devoted "less than two months of serious undercover and surveillance work to this investigation before it decided to shift the investigatorial center of gravity to the wiretap." *Id.* at 1247. The government failed to pursue "many potentially significant investigatory leads that it had developed, or with reasonable competence should have developed," before seeking the wiretap, and it failed to develop the promising leads it had. *Id.* Some of those "leads clearly would have yielded valuable information about the sources of the drugs" at issue, and "the decision to rely on the wiretap as the principal investigatory tool was made no later than the first week in March of 1993," which was almost five months before authorities submitted the application. *Id.* After that point, "the only investigatory efforts of any consequence were directed toward analysis of telephone communications." *Id.*

In a related vein and as present in Mr. Howland's case, the affidavit obscured many of these shortcomings, making implications regarding the extent of the investigation. *Id.* And while the timing of the investigation in Mr. Howland's case diverged somewhat from that in *Ailemen*, the difference is not great. Investigation in Mr. Howland's case began in December 2017 (or January 2018 for ATF in Michigan), with the affidavit filed only four to five months later, on April 5, 2018. *See* Case No. 1:18-MC-28, RE. 3, PageID # 34, 71. As in *Ailemen*, the investigation in Mr. Howland's case likely involved "traditional" investigatory methods that could have produced information on multiple additional

participants in the alleged trafficking—as Mr. Howland pointed out above in the trash-pull section, which described the efficacy of traditional methods. *Compare Aileman*, 986 F. Supp. at 1275 (pointing out that traditional investigation had turned up seven additional participants). In the application for the wiretap of phone 9351, the affiant identified half a dozen "target subjects" by name—participants who had come to the attention of law enforcement through traditional investigative means. *See* Case No. 1:18-MC-28, RE. 3, PageID # 32-34.

As discussed above, in Mr. Howland's case as in *Ailemen*, the government failed to pursue viable traditional investigation. *Compare Ailemen*, 986 F. Supp. at 1276. The affiant here conceded that investigators did not pursue avenues such as interviewing suspects or executing search warrants (despite plans for such searches once the government brought charges). *See* Case No. 1:18-MC-28, RE. 3, PageID # 60-64. The discussion of using search warrants *later* flies in the face of the statutory requirements for wiretaps: Turning to tools like search warrants *after* applying for wiretap authorization represents exactly the approach condemned in 18 U.S.C. § 2518(1)(c). Section 2518 requires that "other investigative procedures have been tried" (and failed) or that other techniques "reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c). Given their plan to use search warrants, and the alleged probable cause they implied they had to support such warrants, the authorities here should have executed search warrants *before* resorting to wiretaps. *Cf.* Case No. 1:18-MC-28, RE. 3, PageID # 63-64.

The affidavit essentially involves "ritualistically repeating" strains of, or themes from, statutory language (e.g., language about the potential risks of pursuing "traditional" investigatory methods). *See Ailemen*, 986 F. Supp. at 1285. The assertions about the supposed ineffectiveness of traditional investigatory methods did not fulfill the statutory requirement, a requirement that implies specificity, and they did not ring true given the success linked to using such "traditional" techniques in this and other cases. *See Ailemen*, 986 F. Supp. at 1286. Courts have charged the government "with knowing

that this kind of merely generic knowledge is not sufficient to support a finding of necessity." *Id.* at 1285-86. In discussing investigatory leads in a related Canadian case in *Ailemen*, the magistrate judge pointed out that information from that related investigation "virtually compelled" the conclusion that the defendant was involved in heroin purchasing and in smuggling. *Id.* at 1314. In *Ailemen*, the magistrate concluded that information like this information, learned through "traditional" investigation, obviated the *need* for the wiretap. *Id.* The same can be said of Mr. Howland's case: The affidavit alleged information and potential leads that did away with any possible finding that a wiretap was *necessary*. Given all the wiretap application's deficiencies, the evidence derived from the tap of phone 9351 should be suppressed. "While the necessity requirement demands something considerably less than perfection, it must have some real meaning, and a responsible court has no choice but to order suppression when, as here, the affidavit clearly fails to meet the standards that derive from that requirement." *Id.* at 1246.

II. The wiretap application for the phone ending in 9351 included material omissions and misstatements, requiring a *Franks* hearing and ultimately a finding that the application cannot withstand scrutiny and that the evidence derived from the wiretap must be suppressed.

Courts recognize the analysis under *Franks v. Delaware*, 438 U.S. 154 (1978), in this wiretap context. *See, e.g.*, *United States v. Roybal*, 46 F. Supp. 3d 1127, 1149-50 (D.N.M. 2014) (citing cases), 1159; *see also United States v. Green*, 175 F.3d 822, 828 (10th Cir. 1999); *United States v. McDowell*, 520 F. App`x 755, 758-59 & n.1 (10th Cir. 2013). Under *Franks*, courts have said, a person can challenge a facially sufficient affidavit. *See, e.g.*, *Roybal*, 46 F. Supp. 3d at 1150. Courts have spoken of conducting *Franks* hearings, in this wiretap context, when a defendant makes a substantial preliminary showing that the warrant affidavit included a false statement/material omission; the affiant made the statement knowingly and intentionally or with reckless disregard for the truth; and the allegedly false statement necessarily contributed to a finding of probable cause. *See id.* at 1150, 1161. To obtain a *Franks* hearing, a defendant should make an offer of proof. *Id.* at 1150. If the defendant makes the required showing

under *Franks*, a reviewing court should consider the sufficiency of the affidavit with the offending passages excised. *See id.* at 1151.

This required showing involves the defendant showing falsity or reckless disregard for the truth by a preponderance of the evidence. *See, e.g.*, *id.* at 1161. An officer's negligence or inadvertence will not suffice. *See id.* All statements in an affidavit need not be true, but a defendant should receive a *Franks* hearing if he or she can show that the affiant did not believe, or appropriately accept, certain statements as true. *See id.* "If a wiretap affidavit omits material information that would vitiate either the necessity or the probable cause requirements had it been included, the resultant evidence must be suppressed." *Green*, 175 F.3d at 828. Mr. Howland can show that the affiant in this case did not and could not accept as true certain statements in the wiretap application for phone 9351. Thus, the Court must determine the facts, relying on credible evidence produced at a hearing, to determine whether a "reasonable issuing judge" should have denied the wiretap application based on a lack of necessity. *United States v. Blackmon*, 273 F.3d 1204, 1208 (9th Cir. 2001).

The false statements in Mr. Howland's case undermine any possible finding of necessity to support issuing the authorization for the wiretap of the phone ending in 9351. *Cf.* RE. 308, PageID # 1192-1212 (discussing lack of necessity demonstrated in the affidavit supporting the wiretap application). While the application for the wiretap authorization failed to establish necessity as discussed in Mr. Howland's earlier motion—the government simply failed to show the necessity of engaging in the serious intrusion into privacy involved in wiretapping—the false statements explored in this motion provide the final nails for the wiretap's figurative coffin. These deficiencies mean all evidence derived from the wiretap of phone 9351 should be suppressed. *See* 18 U.S.C. § 2518(10)(a) (allowing for suppression of derivative evidence); *see also United States v. Giordano*, 416 U.S. 505, 533 (1974). Regardless of the affidavit's length in this case, the government has come up short here. The Sixth Circuit has consistently emphasized that length does not make an affidavit valid. *See, e.g.*, *United*

States v. Helton, 314 F.3d 812, 816, 825 (6th Cir. 2003) (court found lack of probable cause to support the search warrant, despite the affidavit spanning 27 pages and 64 paragraphs). The government cannot satisfy the necessity requirement, as discussed in Mr. Howland's earlier motion, and the *Franks* issues presented here further undercut a finding of necessity and even of probable cause itself.

A. The application's discussion of the "dangers" of fentanyl precluding use of traditional investigation methods constitutes material misstatement.

Multiple times in the wiretap application, the affiant made assertions regarding the alleged dangers of possible fentanyl exposure. *See, e.g.*, RE. 308, PageID # 1200 (supposed dangers to confidential informants and undercover agents), 1202 (supposed limits on searches because of dangers of fentanyl), 1204 ("dangers" of fentanyl limiting trash-pull potential). As the court found in *United States v. Aileman*, "[t]hese incantations of the danger factor were fundamentally misleading." *United States v. Aileman*, 986 F. Supp. 1228, 1285 (N.D. Cal. 1997). In *Aileman*, "the government knew . . . there was no basis, at the time the affidavit was submitted, for a belief that [certain individuals], or any of their white female couriers ever had committed an act of violence, ever had threatened anyone with an act of violence, or ever had carried a weapon." *Id.* The absence of such evidence was especially noteworthy because the defendant "and his alleged co-conspirators had been investigated twice by the government—and those investigations had subjected the suspects' conduct and criminal histories to scrutiny over a period that spanned some five years, between late 1987 and mid-1993." *Id.* The magistrate judge in *Aileman* found that the unfounded assertions about danger constituted material assertions. *Id.* at 1286. In Mr. Howland's case, the affiant took similar liberties, making unfounded, unscientific assertions about the dangers of fentanyl exposure.

In the section on trash pulls, the affiant commented on "the significant presence of fentanyl associated with the HOWLAND DTO," which supposedly enhanced "the risk that law enforcement m[ight] inadvertently come into direct contact with fentanyl residue, and/or contaminated narcotics paraphernalia containing fentanyl." *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 67, ¶ 93. In the

section on cooperating informants and undercover agents, the affiant suggested that "due to the significant presence of fentanyl within the HOWLAND DTO, the benefit does not outweigh the risk that utilizing a CS or UC would provide by potentially coming into direct contact with fentanyl or heroin heavily laced with fentanyl." *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 60, ¶ 76.

The affiant asserted that "the seizure of 945 grams of fentanyl from the February 28, 2018 parcel makes the controlled purchase of heroin or fentanyl extremely dangerous to not only the confidential source or UC but to any law enforcement officer responsible for handling evidence containing fentanyl." *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 60, ¶ 75. She also made much of the "dangers" of a "large quantity of fentanyl" that "necessitated the seizure of all parcels related to the DTO due to the potentially dangerous nature of their contents." *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 55, ¶ 60. This seizure of parcels supposedly made the alleged drug-trafficking organization more aware of law enforcement's presence. *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 55, ¶ 60. This assumed wariness allegedly reduced law enforcement's ability to identify and intercept subsequent parcels. *See* RE. Case No. 1:18-MC-28, RE. 5, PageID # 55-60, ¶ 60.

The affiant's assertions related to the supposed dangers of fentanyl, however, rest on no empirical support. Medical doctors have debunked the hyperbole surrounding fentanyl. As three doctor-scholars have expressed it, "Reports in lay media have sensationalized accounts of exposure and harm" related to exposure to opioids and those who overdose on them. Michael J. Lynch, Joe Suyama, Francis X. Guyette, *Scene Safety and Force Protection in the Era of Ultra-Potent Opioids*, 22 Prehospital Emergency Care 157, 157 (2018). Popular media have described law-enforcement exposures to synthetic opioids and the potential for toxicity that could require treatment for responders. *Id.* Medical experts, however, have shown that "[t]he likelihood of prehospital providers suffering ill effects from opioid exposure during routine emergency medical services (EMS) operations is extremely low." *Id.*

The reality is that users typically inject fentanyl and its analogues, or ingest these substances through contact with mucous membranes—snorting. The "[t]ransdermal delivery of fentanyl has been described and developed for decades, however, crystallized or powdered fentanyl has markedly diminished absorption and systemic availability. While fentanyl "has demonstrated relatively favorable skin permeation characteristics," it "requires pharmaceutical delivery mechanisms to achieve meaningful systemic levels." *Id.* at 158. Fentanyl patches promote diffusion across skin layers typically through an alcohol-based solution that is gelled with hydroxyethyl cellulose. *Id.* Studies of occupational exposure in pharmaceutical production workers who load, filter, dry, and package significant amounts of powdered fentanyl "have shown dermal absorption of clinically insignificant levels of fentanyl following prolonged exposure." *Id.* While industrial production and pharmacokinetics of fentanyl would indicate that there is a theoretical risk of skin absorption, it is unlikely that rapid absorption of crystallized or powdered fentanyl, or fentanyl derivative, outside of solution, would occur. *Id.* Water and mild detergents can remove fentanyl contamination. *Id.*

Though it did not constitute a focus of this article, the authors of this piece explicitly considered the law-enforcement context, including the "confiscation of drug evidence" context. *See id.* 159. Of course, they advise first responders to refrain from tasting or touching powdered or packaged drug substances. *Id.* They emphasize that "visible powder without evidence of disruption or airborne dust should not preclude identification, removal, and standard treatment of a victim." *Id.* Scenarios in which "powder has clearly been disrupted and dust particles are identified are rare," and these circumstances, of course, should prompt an evaluation of the premises and possible "danger to personnel." *Id.* But time, distance, and shielding can minimize exposure. *Id.* Shielding includes using gloves, long sleeves, and pants. *Id.* Responders do not need masks to treat a patient suffering from fentanyl toxicity. *Id.* This position reflects the fact that these scenarios seldom involve airborne materials, but regardless, even if a scene hosts powder, responders can treat inadvertent contact with

such powder by washing with water. *Id.* at 159-60. While carfentanil has been implicated in gas attacks, these scenarios involved "a weaponized preparation, not the street level drug." *Id.* at 160.

Specifically in the law-enforcement context, "[p]opular media reports of possible law enforcement exposure and toxicity have included removal of dust from clothing." *Id.* Yet "[c]lothing should act as an appropriate barrier to direct skin contact," though "secondary exposure through hand contact or production of dust is unlikely but possible." *Id.* If officers identify powder or dust "on clothing, a disinfectant wet wipe should be used with a gloved hand to remove it," since "[u]sing a wetted wipe will prevent significant aerosol of dust and disinfectant wet wipes have been shown to remove approximately three times more dust from skin than waterbased ones." *Id.* After this "dust removal, clothing should be carefully removed and laundered at the first opportunity." *Id.* A wet wipe and a run through the laundry could potentially address issues. And "[i]f there is any concern for external contamination the provider should shower as soon as is practicable." *Id.*

Regarding treating overdose victims, these experts advise that, "if there is visible drug on a patient's face, it is appropriate to remove the powder with a gloved hand prior to initiation of ventilation." *Id.* They do advise law-enforcement officers to engage in "appropriate forensic collection" of drug evidence, and they recognize a lack of data on these topics. *Id.* at 161.

From a logic standpoint, the key lies in the fact that even large-scale drug dealers are not suffering injury. As the doctor-authors of this article point out, "[w]hile published data regarding first responder safety with the advent of highly potent opioid derivatives do not exist, the widespread national availability of these drugs combined with the infrequent of [sic] reports of emergency medical responder, drug dealer, and illicit drug lab exposure incidents are encouraging that routine performance of these activities is unlikely to result in toxicity." *Id.* at 159. Essentially, routine performance of drug dealing is unlikely to result in toxicity. *See id.* The idea that fentanyl presents some

extreme risk that impedes the use of informants and undercover agents, and things like trash pulls, simply does not enjoy empirical support.

The affiant herself purchased narcotics that field tested positive for fentanyl, within the confines of a vehicle, without (one assumes from her account in the warrant applications for the Lantana and Neland residences) negative health effects to herself (or even observed in the seller Jacarr Cox). *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 48; Case No. 1:18-MJ-139, RE. 1-1, PageID # 48. The wiretap affidavit's falling back on the unsubstantiated "fentanyl-is-too-dangerous" reasoning raises a *Franks* issue and undermines the reliability of any statements about the "necessity" of the wiretap.

B. Inconsistencies between warrant applications demonstrate the inclusion of false statements or statements for which authorities recklessly disregarded the truth.

As Mr. Howland discussed in his motion to suppress the evidence derived from the wiretap of phone 9351, the affidavit in support of the wiretap authorization contained points regarding things like the utility of physical surveillance—points that brought to the forefront issues of veracity because the affiant described events and incidents in multiple, divergent ways over the course of multiple warrant applications. RE. 308, PageID # 1196-1200 (discrepancies in accounts of physical surveillance), 1204-05 (discrepancy issues related to description of potential for trash pulls).

This divergence of renditions appears *within* warrants as well. For example, in the warrant applications for the residences on Lanatan Drive and Neland Avenue, the affiant described an alleged incident in the parking lot of a Boost Mobile store on April 7, 2018. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 28, 46; Case No. 1:18-MJ-139, RE. 1-1, PageID # 28, 46. The affiant described how "HOWLAND's white F150 exited the driveway" of the Neland Avenue residence and "drove to a Boost Mobile store" on Madison Avenue in Grand Rapids. Case No. 1:18-MJ-135, RE. 1-1, PageID # 28; Case No. 1:18-MJ-139, RE. 1-1, PageID # 28. Mr. "HOWLAND's white F150 parked in the parking lot of the closed Boost Mobile store," and "[a]t approximately 7:41 p.m., investigators

observed an unknown individual walk up to the rear driver's side door and enter the white F150." Case No. 1:18-MJ-135, RE. 1-1, PageID # 28; Case No. 1:18-MJ-139, RE. 1-1, PageID # 28. The "F150 then exited the parking lot and continue[d] south on Madison." Case No. 1:18-MJ-135, RE. 1-1, PageID # 28; Case No. 1:18-MJ-139, RE. 1-1, PageID # 28. The investigators opined that this incident evidenced a narcotics transaction. Case No. 1:18-MJ-135, RE. 1-1, PageID # 28; Case No. 1:18-MJ-139, RE. 1-1, PageID # 28.

Later in the warrant applications, however, the affiant described the incident as involving Mr. Howland's truck driving to a Boost Mobile store on Madison Avenue in Grand Rapids and investigators observing "an unknown male approach[ing] the vehicle for a very short period of time," with "[t]his incident [being] consistent with drug trafficking." Case No. 1:18-MJ-135, RE. 1-1, PageID # 46; Case No. 1:18-MJ-139, RE. 1-1, PageID # 46. In this rendition, the individual does not enter the truck; rather, he stays only a "very short period of time" and then seems to move on. These numerous inconsistencies further undermine the wiretap affidavit's credibility and demonstrate the systemic nature of the misstatements, giving rising to the need for a *Franks* hearing and ultimately to excision of these statements from the wiretap, and warrant, applications.

As Mr. Howland has already discussed in his motion to suppress the wiretap evidence, the government cannot establish necessity for the wiretap of phone 9351. This deficiency only grows when one considers the misstatements in the wiretap-application affidavit. These misstatements vitiate any potential necessity and give rise to the need for a *Franks* hearing. For these reasons, and those in his motion to suppress, Mr. Howland asks the Court to grant a *Franks* hearing and then suppress all evidence (including all evidence derived from the execution of search warrants that relied on the wiretap and intercepted communications) derived from the wiretap of phone 9351/Target Phone 1.

III. No good-faith exception exists in the wiretap context to save the intercepted communications and evidence at issue from suppression.

Courts have considered, and rejected, the idea of a good-faith exception in the wiretap arena. No good-faith exception exists in this context to save from suppression the evidence Mr. Howland challenges here. *See Rice*, 478 F.3d at 711. In cases such as this one—cases in which the government may have engaged in extensive investigation, invested massive quantities of resources and hundreds of hours—it bears returning to certain fundamentals. As Justice Brandeis reminded the nation in his dissent in *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting), one of the Supreme Court's fundamental wiretapping cases, "[e]xperience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent." People "born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers," but "[t]he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding." *Id.* The statutory scheme governing wiretapping simply asks investigators to use "traditional" investigatory tools and resort to wiretapping only when truly necessary. This approach honors this country's tradition that "it is better that a few criminals escape than that the privacies of life of all the people be exposed to the agents of the government, who will act at their own discretion, the honest and the dishonest, unauthorized and unrestrained by the courts." *See id.* at 479 n.12 (Brandeis, J., dissenting).

Phones are different, which *Olmstead* even noted in the '20s. *See Olmstead*, 277 U.S. at 465 ("By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place."). Five years ago, in *Riley v. California*, 134 S. Ct. 2473, 2489 (2014), the Supreme Court affirmed that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." As the Supreme Court explained it, "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."

Riley, 134 S. Ct. at 2489. Modern phones can "just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." We turn to them because they make many tasks faster, easier, more efficient. Law enforcement, of course, sees value in turning to these telephonic resources to investigate crime. Our system of criminal justice, however, does not countenance tapping phones as a first resort. Case law like *Riley* and *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (requiring a warrant for historical cell-site data), affirm the privileged place of phone data and the fact that cell-phone data is not to be taken for granted as a law-enforcement tool. Title III simply requires more. Mr. Howland asks the Court to suppress all evidence derived from the wiretap of phone 9351/Target Phone 1. Such evidence includes all evidence derived from the execution of search warrants that relied on the wiretap and intercepted communications.

IV. The application for the wiretaps of Target Phones 2 and 3 failed to establish necessity for those wiretaps; it failed to show that authorities had tried normal investigative procedures and that these procedures had failed, or that such procedures reasonably appeared unlikely to succeed or would be too dangerous, and these application deficiencies mean the wiretap orders were insufficient and resulted in unlawful interceptions.

Mr. Howland also moves this Court to suppress all evidence derived from the wiretaps of two phones, with numbers ending 2295 (what the government calls Target Phone 2) and 3996 (what the government calls Target Phone 3). The wiretaps of Target Phones 2 and 3 fail under the necessity requirements of 18 U.S.C. § 2518(1)(c). All evidence derived from these wiretaps should be suppressed. *See* 18 U.S.C. § 2515. A more fundamental question regarding the necessity of tapping Phones 2 and 3 arises because, as discussed in Section III below, the affidavit in support of the taps of Phone 2 and 3 leans *very* heavily on evidence derived from the tap of the first phone. This reliance creates the issue of the subsequent taps qualifying as evidence derived from the first (illegal) tap (making it subject to suppression), but it also creates a situation where one can ask: if authorities supposedly obtained so much evidence from tapping the first phone, wouldn't they have enough to

proceed with an indictment? Regardless of the reasoning—a lack of necessity, derivation from the first illegal tap, or both—the wiretaps of Phones 2 and 3 contravened the law.

On the necessity issue, Mr. Howland will look at separate sections of the subject wiretap application individually, starting with physical surveillance.

Physical Surveillance

The affiant attempted to argue the inefficacy of physical surveillance by saying Mr. Howland used fake names to contact the Post Office and would use others to make calls and receive packages. *See* Case No. 1:18-MC-28, RE. 10, PageID # 375, ¶ 65. She made these assertions in the face of her own discussion of Mr. Howland supposedly calling Indiana authorities about a lost package and *using his own name* and Target Phone 2's number. *Cf. id.* at 353-54, ¶ 42. This frankness in the use of a real name undercuts the affiant's later assertions about Mr. Howland's supposedly clandestine behavior thwarting surveillance efforts.

Likewise, the affiant's assertions about physical surveillance failing to indicate the nature and significance of meetings must topple in the face of the myriad of warrant applications that cite physical surveillance and a recognition of drug sales to establish probable cause. *See id.* 376, ¶ 69. Courts routinely believe that authorities can and do recognize the significance of meetings like those of drug transactions. Of course, physical surveillance will seldom, if ever, firmly establish all the elements of an offense, especially when one considers the issues surrounding mens rea. *Cf. id.* at 377, ¶ 72. But no one expects it to. This limit does not, however, mean every case warrants a resort to wiretapping. Such a limit to a single investigatory technique hardly establishes *necessity* for such tapping.

Confidential Informants and Undercover Agents

In arguing that using confidential informants and undercover agents would not work to further the investigation, the affiant ignored her own statements about the successful use of informants. For example, the affidavit described a controlled buy on March 19, 2018. *See* Case No. 1:18-MC-28, RE.

10, PageID # 344, ¶ 25. The affiant stated, "The confidential informant then successfully obtained two grams of heroin from [Justin] MARTIN, which field tested positive." *Id.* Likewise, on April 3, 2018, Justin Martin allegedly led authorities to conclude Mr. Howland acted as his supplier. *Id.* at 379, ¶ 77. The fact Mr. Martin supposedly had no additional information to share does not mean agents could not have continued on this trajectory of arresting suspects and interviewing them, a trajectory that ostensibly produced the information from Martin and moved the investigation forward and could have been similarly efficacious with other suspects.

This section also suffers in the way the application for the wiretap of Target Phone 1 suffered: it includes at least reckless misstatements. In this section, these misstatements related to (as with Phone 1) the supposed dangers of fentanyl. The affiant alleged that it would be "extremely dangerous" to conduct controlled buys. *See id.* at 380, ¶ 83. As Mr. Howland has already discussed, science and logic simply do not bear out such assertions. These claims also appear especially disingenuous in light of the controlled buys the affiant and others conducted in the case. *See, e.g.*, Case No. 1:18-MJ-135, RE. 1-1, PageID # 48; Case No. 1:18-MJ-139, RE. 1-1, PageID # 48.

Witness Interviews and Grand Jury Subpoenas

This section suffers as generic boilerplate. It relies on speculation and conclusory assertions based on "experience." *See* Case No. 1:18-MC-28, RE. 10, PageID # 381, ¶¶ 85-86. This section also demonstrates the affiant's premature attempt to resort to wiretapping. She rejected the idea that historical cell-phone records obtained through a warrant or subpoena would yield helpful information, but in citing this option and rejecting it out of hand, she proved the authorities' lack of commitment to trying less intrusive methods of investigation before resorting to wiretaps. *See id.* at 383, ¶ 88. She should have at least obtained and reviewed the records before applying for a wiretap. Whether historical or not, such records very well could have revealed much of the information the affiant professed to seek: information on the extent and methods of the distribution organization, the

identities and roles of those involved, the distribution of proceeds, the location of related records, the location and source of supply for controlled substances and financing, and the location of relevant items used in furtherance of the illegal activity. *See id.* at 334-35, ¶ 7(d).

One does not need real-time phone interceptions to discover this kind of information—historical records could present much of this information, especially given the timing would not have made the records stale. These historical records could still be recent. Contrary to the assertions in the affidavit, these records could have provided leads for further traditional investigation. Officers could have used recent historical records to facilitate further surveillance, use of CIs, procuring of records through warrants and subpoenas, and other such traditional investigations, just as they said they would do with phone interceptions. It defies logic to think that *only* real-time interceptions could yield investigatory leads.

Searches

Regarding searches, the affiant rejected the idea on generic grounds. Case No. 1:18-MC-28, RE. 10, PageID # 383, ¶ 89. This section also suffers from logical discrepancies. The same unscientific misstatements about the dangers of fentanyl appear. *See id.* at 384, ¶ 91.

The boilerplate included then falls flat given the timing of the application and the use of the wiretap of Target Phone 1. For example, the affiant states, "However, the execution of search warrants at this time—well in advance of the achievement of the investigation's most critical goals—likely would lead to the detection of the investigation and the destruction of evidence, thwarting law enforcement goals." *Id.* at 385, ¶ 92. It seems disingenuous to cry that executing warrants at that time would have been "well in advance" of achieving the investigation's goals when the traditional investigation and the first wiretap had already identified everyone named in the fifth superseding indictment. *Compare id.* at 333, ¶ 7(a), & 336-39, ¶ 11, *and* Case No. 1:18-MC-28, RE. 6, PageID # 108, ¶ 15 (identifying Christian Newbern), *with* RE. 260, PageID # 972.

The investigation at that point had actually produced more than those suspects. *See, e.g.*, Case No. 1:18-MC-28, RE. 10, PageID # 333, ¶ 7(a). The wiretap application for Target Phone 1 used the same generic pleas about the timing of the investigation and the application coming well in advance of achieving the investigation's goals, boilerplate assertions that just drive home the cut-and-paste nature of the application. *Cf.* RE. 6, PageID # 64, ¶ 84.

The insincerity of these cries comes to the forefront when one compares the second wiretap application to the applications for residential warrants and the execution of arrests. Authorities submitted the second wiretap application on May 2, 2018. Less than two weeks later, the same affiant was submitting residential warrants; she filed the Neland Avenue, Lantana Drive, and other residential-warrant applications on May 15, 2018. A DEA agent arrested Mr. Howland a day later, on May 16, 2018. One cannot help but see a lack of necessity for these additional wiretaps when one compares the application for them to the applications for the residential warrants. Taking the Lantana Drive application as an example, the first several pages are boilerplate citing training and experience. Case No. 1:18-MJ-135, RE. 1-1, PageID # 6-11. Then the application lists suspects. *See id.* at 11-15. To try to establish probable cause, the application cites the first wiretap application and incidents from December 2017 through May 12, 2018. *Id.* at 17-34, 38 ¶ 84. Most of the material predates the second wiretap application: the application cites intercepted communications from Target Phones 2 or 3 at PageID # 44 (¶¶ 107, 109). And again, an agent arrested Mr. Howland just one day after the affiant signed the applications for the residences.

Given this timing, counsel is left scratching his head and asking how the second wiretap was *necessary*, how it *had* to occur, before execution of residential search warrants. It strains credibility to think officers truly "believe[d] that executing search warrants at this time [the May 2 filing of the wiretap application] (assuming it were even possible for all identified locations) would likely compromise the investigation of the DTO [drug-trafficking organization] and its associates." RE. 10,

PageID # 386, ¶ 96. Was the time really so wrong for searches if authorities executed the residential warrants and effected the arrest of Mr. Howland so soon after applying for the additional wiretaps?

Pen Register, Trap and Trace, and Telephone Analyses

As with the application for the wiretap of Target Phone 1, the affiant conceded in this section that law enforcement used these investigation tool effectively. *See* RE. 10, PageID # 386, ¶ 97. The section suffers the same issues of generic information and blanket assertions as presented in the Target Phone 1 application.

Trash Pulls

This section acknowledges the use of trash pulls in the investigation but claims they did not yield contraband. *See id.* at 387, ¶ 99. The section conveniently omits discussion of the April 19, 2018 trash pull at the Valleywood Drive residence, which yielded a shipping label identifying Shanika Yvette Daughtry, a girlfriend of Calvin Colbert. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 26, ¶ 47. This successful trash pull suggests that the affiant could not have truly believed that trash searches are not effective in identifying a drug conspiracy's participants and scope. *Cf.* RE. 10, PageID # 388, ¶ 100. Perhaps trash pulls will not identify *fully* all participants and details, but no one expects such *full* identification from them. *Cf. id.* Used with other methods, however, they may contribute to obviating the need to eavesdrop on people's private phone conversations. And as discussed above, this pull was successful enough to appear in an application for a warrant to seize and search the Priority Mail Express package with the tracking number ending 8863US. *See* May 9, 2018 Application for Search Warrant for Priority Mail Express Parcel, at 3-4, ¶ 13; 6-7, ¶ 19.

The affiant also resorts to the hyperbole about fentanyl again. *See id.* at 388, ¶ 101. The section simply shapes itself to suit the affiant's end goal of tapping two additional phones. It omits essential details, details that undermine a finding of *necessity*.

Mobile Tracking Devices

Similar to the situation with the application for the wiretap of Target Phone 1, this section of the affidavit conceded the usefulness of vehicle trackers, especially for identifying locations frequented by suspects. *See* RE. 10, PageID # 388, ¶ 102. The discussion of the limits of tracking again, as with Phone 1's application, devolved into generic assertions related to the limits of tracking in general, and while bemoaning these ostensible limits, the affiant glossed over the fact that tracking data is useful enough to show up in warrants in many cases in general (and in this case specifically).

Video Surveillance

The affiant speaks of the usefulness of this option when used "in conjunction with" wiretaps. *See id.* at 390, ¶ 106; *see also id.* at 393, ¶ 116 (recognizing need for multiple investigatory approaches). All of these techniques, of course, have their limits in isolation, but history belies the idea that authorities use these techniques in isolation. For decades, this district operated—quite effectively—without any sign of wiretaps. The implication in this wiretap application—that traditional investigative techniques require wiretap augmentation—flies in the face of history and experience. Nor can one simply say that technology has changed the game. In the end, a wiretap is simply a means of listening in on a phone conversation, even if that conversation occurs in writing (texting). These taps have been around for a century. *See, e.g.*, *Olmstead v. United States*, 277 U.S. 438 (1928). And authorities have not always resorted to them out of hand.

Mail Covers

This section of the affidavit presented the same sort of issues Mr. Howland pointed out when discussing the wiretap application for Target Phone 1. It contains generic assertions applicable in just about any drug case.

Other Investigations

As with the application for the tap of Phone 1, this section detailed what sounded like effective investigation efforts by multiple agencies in California and Michigan.

Financial Investigations

The affiant recognized the value of subpoenas for things like financial records. *See id.* at 393-94, ¶ 117. She also acknowledged that close to 15 subpoenas remained outstanding when she applied for the wiretap of Target Phones 2 and 3. *See id.* 394, ¶ 118. She offered no explanation for her refusal to review the results of these subpoenas before engaging in the extreme privacy intrusion of wiretapping the additional phones.

From a practical standpoint, these wiretaps revealed very little to law enforcement. In a ten-day progress report for the Court, the U.S. Attorney's Office pointed out that only 6 of 124 calls intercepted on Phone 2 were relevant. *See* RE. 14, PageID # 431-32, ¶ 5. Of the total 124 calls, only 1 ran longer than 2 minutes. *See id.* at 432, ¶ 5. While counsel is not suggesting an overly broad, after-the-fact analysis, the idea that fewer than 5% of the calls resulted in relevant information makes these wiretaps appear less than necessary. Phone 3 fared perhaps slightly better, but it still yielded only a small percentage of relevant interceptions. Of 452 interceptions, authorities deemed 82 relevant; 60 of these calls lasted 2 minutes or more. *See id.* at 432-33, ¶ 7.

In this progress report, the U.S. Attorney's Office asked the Court to continue the wiretap authorization, citing a need for more time to achieve all the objectives of the investigation. *See id.* at 441-42 & ¶ 21. The office, however, filed this report on May 14, 2018. Authorities sought the residential warrants a day later and arrested Mr. Howland a mere two days later. Certain assertions by the affiant demonstrate the backwardness of the government's approach to necessity in this case. Regarding electronic surveillance, the affiant asserted: "The location information from Target Phone 1 and Target Phone 2 corroborated information obtained through the interceptions of Target Phone

1, and confirmed the locations associated with the meet locations for narcotics transactions broadcasted by HOWLAND during the interceptions of Target Phone 1." *See id.* at 371, ¶ 56. *Necessity* does not equate with providing information the authorities can otherwise corroborate. The government may not use the unique intrusion of a wiretap to obtain information it can so handily corroborate through other investigatory means.

In a similar vein, the affiant argued that authorities only obtained "half of the narcotics trafficking information" available from monitoring Target Phone 1 because Mr. Howland was supposedly using Target Phone 2 at the same time. *See id.* at 374, ¶ 62. This reasoning relies on convenience, not necessity. If Target Phone 1 was providing the information the authorities needed, there was no *need* to tap an additional phone. The application simply shows, time and again, that authorities were looking for a convenient, rather than truly *necessary*, investigatory tool.

V. The application for the wiretaps of Phones 2 and 3 contained misstatements that give rise to the need for a *Franks* hearing and excision.

Along with the misstatements discussed above, this wiretap application contains misstatements similar to those found in the earlier application for the wiretap of Target Phone 1. It contains a similar rendition of the alleged surveillance of March 14, 2018—a rendition that varies in material ways from the versions given in the residential warrants. *See* Case No. 1:18-MC-28, RE. 10, PageID # 372-73, ¶ 60. It contains an even more convoluted discussion of the April incident in the Boost Mobile parking lot. *See id.* at 373, ¶ 61. This incident appears—with different renditions—multiple times within the residential warrants. In those warrants, the affiant gives a date of April 7, 2018. *See, e.g.*, Case No. 1:18-MJ-135, RE. 1-1, PageID # 26, ¶ 49. In the wiretap application for Phone 2 and 3, the affiant gives a date of April 6, 2018. *See* Case No. 1:18-MC-28, RE. 10, PageID # 373, ¶ 61. As with the discussion in the materials related to the first wiretap application (for Target Phone 1), the version of this incident in the wiretap application for Target Phones 2 and 3 varies from a version in the residential-warrant materials. *Compare id. with* Case No. 1:18-MJ-135, RE. 1-1, PageID

28, ¶ 54, & PageID # 46, ¶ 115. All the versions present a timing discrepancy, though counsel recognizes that this discrepancy may represent a typographical error (yet the repetition of it and later omission of it seem to militate against finding it to be a mere typo): each version describes an incident at 7:41 p.m. occurring after the description of 8:25 p.m. *See* Case No. 1:18-MC-28, RE. 10, PageID # 373, ¶ 61; *see also* Case No. 1:18-MJ-135, RE. 1-1, PageID # 28, ¶ 54, & PageID # 46, ¶ 115 (not giving a time).

As with the application for the wiretap of Target Phone 1, the affiant makes sweeping, unscientific assertions about the dangers of fentanyl, as touched on above. These assertions appear in various places, cited above and at places like PageID # 375, ¶ 67.

VI. The wiretaps of Phones 2 and 3 also warrant suppression as derivative evidence from the first wiretap (of Target Phone 1, with a number ending in 9351).

Not only does the wiretap application for Phones 2 and 3 fail on its own, it fails as derivative evidence stemming from the illegal wiretap of Phone 1. As already discussed, courts should suppress evidence derived from an illegal wiretap. *See* 18 U.S.C. § 2518(10)(a). Here, much of the affidavit offered in support of the application for the wiretaps of Phones 2 and 3 relied on information obtained through the tap of Phone 1. *See, e.g.*, Case No. 1:18-MC-28, RE. 10, PageID # 330, ¶ 3; 333, ¶ 6(i); 340-42, ¶¶ 16-18; 342, ¶¶ 20-21; 349-52, ¶¶ 35-37 & nn.4-5; 357-58, ¶ 50 n.6; 359-64, ¶¶ 52-62 & nn.8-9; 365 n.10; 366, ¶ 66; 370, ¶ 54; 375-76, ¶ 67.

If one excises from the warrant application all of the material related to the interceptions of Target Phone 1, one is left with the discussion of seized money from the Indiana authorities, various toll records, mention of controlled buys, and information from Justin Martin. *See, e.g.*, *id.* at 354-56, ¶¶ 43-47 (paragraphs related to Indiana authorities' seizure of package).

VII. Authorities failed to minimize their wiretap intrusions, and this failure rises to a level that supports suppression of the evidence derived from the interception of privileged communications.

Under 18 U.S.C. § 2518(5), wiretaps "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days." This minimization requirement addresses things like protecting attorney-client calls. *See, e.g.*, *United States v. Renzi*, 722 F. Supp. 2d 1100, 1111 (D. Az. 2010). Indeed, minimization gains special importance when a target of communication interception enjoys representation by counsel. While not directly addressing minimization issues, the magistrate judge in *United States v. Aileman*, 986 F. Supp. 1228, 1297-98 (N.D. Cal. 1997), pointed out the gravity of misstatements related to a subject's lack of counsel in the minimization context. (The *Aileman* citation produces the magistrate's report and recommendation at 1242 to 1314 and the district court's adoption of that recommendation at 1230 to 1242.)

The defense here understands that "the percentage of privileged conversations is not a sure guide to the answer in a suppression case." *See Renzi*, 722 F. Supp. 2d at 1110. Numbers simply do not answer the critical questions when minimization is an issue. Rather, the focus must be on the circumstances of the interceptions. Here, the government admits that authorities intercepted attorney-client calls during the tapping of phone 9351. *See* Case No. 1:18-MC-28, RE. 7, PageID # 295-98. And the government recognizes the issues these interceptions raise. *See* Case No. 1:18-MC-28, RE. 7, PageID # 298-99 (detailing the actions the government took regarding these interceptions and the issues of privilege). A key problem, however, is the power given to monitoring officers to determine privilege. *See* RE. Case No. 1:18-MC-28, RE. 3, PageID #74 (giving "monitoring officers" the task of minimizing "all privileged communications"); *see also* Case No. 1:18-MC-28, RE. 7, PageID # 295-97 (evidencing reliance on law-enforcement officers to determine if call interception raised an issue of privilege).

In analogous contexts, courts have pointed out the problems with the "liberal use of taint teams," finding that such use "should be discouraged" because the teams present an "inevitable and reasonably foreseeable" risk that privileged information could be leaked to prosecutors. *See Renzi*, 722 F. Supp. 2d at 1112. Government "taint teams" may have an interest in preserving privilege, but they also possess a conflicting interest in pursuing and furthering the investigation, and, "human nature being what it is," taint-team participants may make mistakes or violate their ethical obligations. *Id.* In *Renzi*, where the court expressed these concerns, the team included *attorneys*, a situation that should actually have mitigated the tension between minimization duties and law-enforcement zeal. *See id.* In Mr. Howland's case, in contrast, the Assistant U.S. Attorneys were the only attorneys involved (and, of course, have a prosecutorial bias), and that involvement arose only *after* the initial decision to point out potential privilege—which a law-enforcement officer made. *See* Case No. 1:18-MC-28, RE. 7, PageID # 295-98.

Those monitoring the potential-privilege issues were invested in the law-enforcement aspect of the investigation, including the attorneys monitoring the situation, who were the prosecuting attorneys. No quasi-neutral team was reviewing these interceptions for proper minimization. In these circumstances, suppression provides an appropriate remedy. Suppression should extend to all evidence derived from these illegally intercepted communications. *See* 18 U.S.C. § 2515; *see also United States v. Giordano*, 416 U.S. 505, 508 (1974).

In discussing the significance of the attorney-client privilege, the Sixth Circuit has said that the privilege can give rise to dramatic remedies, things as extreme as mandamus relief. *See, e.g.*, In re *Perrigo Co.*, 128 F.3d 430, 437 (6th Cir. 1997). The "forced disclosure of privileged material may bring about irreparable harm." *Id.* Privileged communications enjoy special protections in our system of justice, including in the wiretap context. *See, e.g.*, 18 U.S.C. § 2518(5) (directing minimization of interception

"of communications not otherwise subject to interception"). The wiretap here failed to respect the attorney-client privilege and Congress's direction on minimization.

For all these reasons, and those Mr. Howland has raised in his motion to suppress the wiretap evidence based on a lack of necessity for it and his motion for a *Franks* hearing, Mr. Howland asks the Court to suppress all evidence derived from the wiretap of phone 9351/Target Phone 1 that involved improper or inadequate minimization of calls and communications.

VIII. The warrants for cell-phone data from the targeted phones, especially for Target Phone 2, failed to establish probable cause to justify the searches.

To obtain location or other data from a cellular phone, the government must obtain a warrant. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI [cell-site location information]. The location information obtained from Carpenter's wireless carriers was the product of a search."). Of course, issuance of such a warrant requires probable cause. *See id.* at 2221.

This kind of data implicates unique privacy concerns, concerns even graver than those of tracking a vehicle or something similar. *See id.* at 2218. Cell phones have virtually become an aspect of human anatomy, and as such, can reveal extreme amounts of information about a person. *Id.* While *Carpenter* did not address real-time cell-site location information or "tower dumps" (downloading information on all devices that connected to a particular cell site during a particular interval), the case's holding logically extends to real-time data, historical message data like that sought in this case, and similar phone information. *See also Riley v. California*, 573 U.S. 373, 386 (2014) ("Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in

[*United States v.*] *Robinson*[, 414 U.S. 218 (1973)]. . . . [O]fficers must generally secure a warrant before conducting such a search.")

A. Phone and location data require a unique probable-cause inquiry because of the privacy interests involved.

Here, an agent did seek a warrant. The problem arises in that the affidavit in support of the warrant failed to establish probable cause. In looking at the issue, though, another, more fundamental, question arises in this technological context: what constitutes probable cause in the realm of ping warrants and phone data? In the post-*Carpenter* world, one cannot avoid a sense that the probable-cause equation may have shifted.[4] And actually, it was shifting before *Carpenter*. In *United States v. Powell*, 847 F.3d 760, 768-69 (6th Cir. 2017), the court cited *Illinois v. Gates*, 462 U.S. 213 (1983), and looked to the traditional standard, even though it was considering warrants for real-time cell-site location data and GPS tracking. The court simply reiterated that "[p]robable cause supports a search warrant when the affidavit demonstrates 'a fair probability that contraband or evidence of a crime will be found in a particular place.'" *Powell*, 847 F.3d at 769.

In looking to the old standard, the *Powell* court did acknowledge the district court's efforts to craft a new standard in this tracking-technology context. *See id.* In dicta, the *Powell* court noted that "the warrant [had] issued on a finding of probable cause to believe that evidence of drug trafficking would be found by tracking the location of [the defendant's] cell phone." *Id.* 770. The district court, however, had gone to much greater lengths to consider the issue. *See United State v. Powell*, 943 F. Supp. 2d 759, 770-84 (E.D. Mich. 2013). It pointed out the possibility of a "super-warrant" requirement (one based on more than traditional probable cause). *See id.* at 770. In looking at the minority of courts that did not protect this kind of data with some recognition of privacy rights, the *Powell* district court

[4] It bears noting that *Carpenter* addressed the *need* for a warrant. The Court did not take on the issue of what, exactly, constitutes probable cause in this realm. *Cf. Carpenter*, 138 S. Ct. 2217 (addressing only the search aspect).

noted those courts' reliance on the third-party doctrine, which of course, *Carpenter* abrogated. *See id.* at 772.

The *Powell* district court concluded that, "In the absence of a definitive statutory niche for prospective cell-phone tracking, and in light of the considerable, and distinctive, privacy concerns raised by long-term, real-time cell-site tracking discussed above, scrutiny of the appropriate probable-cause showing in these cases is called for." *Id.* at 778. The court ended up finding "that a specific showing is required to establish probable cause when the government seeks a warrant for long-term real-time tracking of an individual via a cell phone." While the court's ultimate framing of the standard may not be the exact standard applicable post-*Carpenter*, the court's efforts represent important ones. Jurisprudence in this area must evolve to address what, exactly, probable cause means in the context of phones and location data. Among other things, the *Powell* district court emphasized that "in a sense, a person's location is in some way *always* relevant to his potential participation in a crime" (and it noted that "a person does not have a general privacy interest in his location"). *Id.* But it found that, before agents may use a person's cell phone to track him or her into places "in which an individual *does* have a reasonable expectation of privacy, the government should show more than that the person is suspected of a crime; the government should show that the person's location in the protected area is in some way relevant to the ongoing investigation of criminal activity." *Id.*

The court also suggested that the government would need to prove "a nexus between the cell phone, the suspect, and the information sought." *Id.* In the end, courts should recognize the nature of the privacy interests at stake with these searches. As the *Powell* district court put it, "[t]he showing described here does not require exhaustion of other investigative techniques; it simply calls for the government to provide additional facts in its warrant application to justify tracking an individual via his personal cell phone, over an extended period of time, into protected spaces." *Id.* at 779. The

analysis results in "a showing that is not necessarily *heightened,* rather it is simply responsive to the full range of recognized privacy interests at stake in long-term cell-phone tracking." *Id.*

The government's ability to intrude into private spheres has only gotten easier and cheaper over time and with new technology. *See id.* at 780. As the *Powell* district court acknowledged, courts must respond to the encroachments on privacy that new technology facilitates.

B. The affidavit failed to establish probable cause here because it relied on inaccurate, incomplete information related to the IP address (supposedly used to track the seized package) and related to the phone at issue.

Regardless of the probable-cause standard employed, this warrant fails. The affiant included in her affidavit the statements that "[i]nvestigators served an administrative subpoena on a Comcast IP address that tracked the parcel that was seized on December 29, 2017," and that this subpoena supposedly "revealed the IP address registered to Johaun HOWLAND," with an address on Lantana Drive in Kentwood, Michigan. *See* Attachment, Continuation of Warrant Application, at 3, ¶ 9. Registration of an IP address, however, adds very little to any probable-cause calculus.

One can liken an IP address to a phone number: "it is a number that identifies a computer or computer network and so enables a person operating another computer to communicate with it." *Milan v. Bolin*, 795 F.3d 726, 727 (7th Cir. 2015). An unsecured WiFi network means "that a person in the vicinity of the home—standing in the street in front of the house, for example—could access the network and send messages from it without needing to know a password." *Id.* Or with a secured network, anyone with the password could be using it. *See id.* at 727-28. Some writers use the term "joyriding" to describe the practice of using someone else's WiFi network to access the internet (without paying for access). *See, e.g.*, Ned Snow, *Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality*, 84 Nebraska L.R. 1226, 1227 (2006). Counsel has also heard the term "wardriving," meaning to drive around an area looking for unsecured networks to exploit. Scholars recognize the dangers to legitimate WiFi-network operators presented by these

practices. Joyriding neighbors can bring disrepute to innocent WiFi-network operators. *See id.* at 1227 n.8. If a joyriding neighbor or a wardriver commits a criminal act online, authorities will likely trace that act back to the innocent WiFi-network operator. *Id.* at 1227 n.8, 1245 n.144. This tracing back occurs because each online connection produces that unique IP address, that numerical combination that police can trace to the physical place where the Internet connection is set up. *Id.* at 1227 n.8. A joyriding neighbor's or wardriver's online activities will lead back to the unoffending WiFi-network operator. *Id.*

An IP address represents nothing more than an origin for WiFi "radio signals." *Id.* at 1231. The router transmits data between computers within the network, and between an internet-connected modem and a computer within the network. *Id.* Essentially, a router serves as an information hub for exchanges between computers within the network and between any network computer and the internet. *Id.* Tech companies have described routers as bridges that allow interconnectivity among computers and facilitate the sharing of an internet connection. *See id.* at 1231 n.37. Routers can often transmit a signal to multiple buildings. *Id.* at 1232. With the proper amplifying antenna, a receiver could "poach" an internet signal miles away. *See id.* at 1232 n.45.

A victim of joyriding or wardriving (or other forms of internet-access poaching) usually does not know of the invasion of their internet access. *See id.* at 1233. And unauthorized or illegitimate access can occur even when a WiFi-network operator uses password protections to try to keep their network private; people can still hack into a password-protected network. *See id.* (noting that *most*, though not all, joyriding occurs without hacking). Thus tracing an internet action (an action such as that of tracking a package) back to an IP address does nothing more than reveal who *may* be paying for the internet access used—licitly or illicitly—by any number of people, including those who know the network's password (if the network has password protection), those joyriding or wardriving, and those who may have hacked into the network.

One third of Americans admit they try to use WIFI networks not their own. *See, e.g.*, Carolyn Thompson, *N.Y. Case Underscores WI-FI Privacy Dangers*, U.S.A. Today (Apr. 25, 2011), *available at* http://usatoday30.usatoday.com/tech/news/2011-04-25-wifi-warning.htm. Police mistakes about who was using a wireless router have led to false accusations and, in some cases, civil suits by wronged civilians. *See id.*; *see also Milan*, 795 F.3d at 727. Given these threats to privacy and the potential for abuses (and the high human toll of law-enforcement mistakes), police must do more than simply note an IP address when trying to establish probable cause. The conclusory statement in the affidavit that Mr. Howland had the IP address and participated in the Gwopped Up drug-trafficking organization puts the cart before the horse: the point of the investigation and the warrants and the ultimate charges is to prove *whether or not* Mr. Howland trafficked in drugs.

Likewise, with the phone itself, Malik Matthis supposedly gave the phone number to staff at the Westwood Post Office in Kalamazoo. The affiant claimed to have identified the phone as belonging to Mr. Howland but did not go to any lengths to disentangle the phone's use from Matthis. Indeed, much of the affidavit focused on Mark Martin's phone ending in 2942. *See* Attachment, Continuation of Warrant Application, at 4-5, ¶ 12; 6, ¶ 14. This conflation occurs with the phone ending in 9351 as well. *See id.* at 7-8, ¶ 15. The affidavit throws out multiple phones hoping something will stick to Target Phone 2 (ending in 2295). This approach hardly reflects the "tailored showing" discussed by the *Powell* district court that "would help prevent the arbitrary or casual invasion of privacy rights that technological change facilitates." *See Powell*, 943 F. Supp. 2d at 779. Nor does it involve the government showing "that a criminal suspect under investigation is the likely user of the cell phone at issue and that he or she uses the cell phone in connection with criminal activity." *See id.* And in the end, this approach cannot establish that tracking one phone will lead to contraband or evidence of a crime.

IX. Authorities should have obtained a warrant to track the use of the cited IP address.

On a more fundamental level, this warrant must fail because, even if the Court finds probable cause to support the search, the key piece of the probable-cause inquiry is the IP address, and the government violated Mr. Howland's Fourth Amendment rights by obtaining a piece of his online "footprint" (namely, information related to his IP address) without first obtaining a warrant.[5] In considering Fourth Amendment and privacy issues, courts ask whether a person has "manifested a subjective expectation of privacy in the object of the challenged search" (here, the internet-browsing history) and whether society is "willing to recognize that expectation as reasonable." *See United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

In this case, Mr. Howland did harbor a subjective expectation of privacy in his internet-browsing history. It seems reasonable to say that most people harbor such an expectation, a state of affairs that helps answer the second prong of the inquiry. Society certainly recognizes such an expectation as reasonable. Generally, Ms. Jane Doe does not expect Big Brother to be lurking in her computer, recording her internet search history as she shops for sex toys, looks up the location of an abortion provider, researches grisly murder details for the novel she is writing (under a pen name), or orders prescriptions to alleviate the symptoms of her HIV.

Whether legal or not, internet wanderings often involve deeply personal, sometimes sensitive, potentially embarrassing, or even politically or professionally detrimental, explorations. According to the Pew Research Center, "Americans continue to express the belief that there should be greater limits on government surveillance programs" and "they say it is important to preserve the ability to be anonymous for certain online activities." *See* Mary Madden & Lee Rainee, *Americans' Attitudes About Privacy, Security and Surveillance* (May 20, 2015), *available at* https://www.pewinternet.org

[5] Whether or not Mr. Howland did indeed track the package seized on December 29, 2017, he had a reasonable expectation of privacy in the internet-search history of his IP address.

/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. While they remain skeptical about organizations' ability to keep their information secure, Americans engage "in some everyday obfuscation tactics and privacy-enhancing measures" to try to keep online information private. *See id.* Over half of America clears its cookies or browser history (59%); a majority refuses to provide information about themselves that isn't relevant to a transaction (57%); a quarter of America uses temporary usernames or email addresses (25%); about a quarter gives inaccurate or misleading information about themselves (24%); and almost a quarter of people in America will refuse to use a website when asked for a real name (23%). *See id.*

Almost 10% of America engages in the far more complex practice of using "a service that allows them to browse the Web anonymously, such as a proxy server, Tor software, or a virtual personal network" (9%). *Id.* Almost half of America (40%) believes "that their **search engine** provider shouldn't retain information about their activity." *Id.* And "65% of American adults believe there are not adequate limits on the telephone and internet data that the government collects." *Id.* Interestingly, and tellingly, "[t]he majority view that there are not sufficient limits on what data the government gathers is consistent across all demographic groups." *Id.* Given these thoughts, practices, and approaches, all of America (regardless of demographics) has expressed a feeling that online browsing *should* be private.

On the very issue of online anonymity, "the majority of adults (55%) said that people should have the ability to use the internet completely anonymously for certain kinds of online activities." *Id.* Another 16% said they did not think people should be able to remain anonymous when online. *Id.* And 27% said they didn't know what to think on the topic. *Id.* While "[m]en are more likely than women to think people should be able to engage in certain online activities anonymously (61% vs. 49%)," support for online anonymity does not vary by age. *Id.* Adults with "at least some" college

education are significantly more likely (compared to people who have not attended college) to believe that people should have the ability to use the internet anonymously (66% vs. 40%). *Id.*

These statistics rather seal the idea of an expectation of privacy in one's browser history—a majority of Americans recognize the reasonableness of expecting private browsing. Fourth Amendment jurisprudence must recognize this expectation: "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *Warshak*, 631 F.3d at 285. Here, jurisprudence must evolve to recognize the reasonable expectation people have in their online tracks.

A. The third-party doctrine cannot whittle away these Fourth Amendment protections for online browsing history and virtual "wanderings."

Just as the third-party doctrine did not undercut the need for a warrant in the cell-location-data context of *Carpenter*, it cannot undercut the need for a warrant here. As the *Carpenter* Court put it, "Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term." *Carpenter*, 138 S. Ct. at 2220. First, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* (citing *Riley*, 573 U.S. at ___, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 441). Second, cell phones log cell-site records by dint of their operation, "without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates." *Id.* As with browsing online, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.* Thus, "in no meaningful sense" does the user voluntarily assume the risk of turning over "a comprehensive dossier" of their virtual movements. *Cf. id.*

The *Warshak* court, exhibiting a sort of judicial ESP, prefigured the demise of third-party-doctrine justifications for intrusion into these realms of privacy. *Compare Warshak*, 631 F.3d at 288, *with Carpenter*, 138 S. Ct. at 2216-17 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."). In coming to its conclusions in *Warshak*, the Sixth Circuit examined the protections afforded telephone communications and letters. *See Warshak*, 631 F.3d at 285. One can now make similar comparisons with historic cell-site location information and IP addresses and browsing history, with *Carpenter* thus supporting the need for a warrant to obtain this latter information.

"Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age," the *Warshkak* court said. *Id.* at 286. Internet protocol addresses and browsing history, while perhaps not "scions" of cell-site location information, are at least first cousins to that information, if not sisters. As the *Warshak* court reasoned, "[i]f we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP [internet service provider] to turn over the contents of an email without triggering the Fourth Amendment." *Id.* An ISP is the intermediary that makes email communication possible: email must pass through an ISP's servers to reach its intended recipients, so an "ISP is the functional equivalent of a post office or a telephone company." *Id.* As police officers may not storm a post office and intercept a letter, "they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is." *Id.* It only stands to reason then that, "if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception." *Id.* The same can easily be said of compelling an ISP to turn over the records of a person's internet use and browsing—their movements in cyber space.

It does not matter that someone (Mr. Howland or someone else in his household) may have "voluntarily" granted Comcast (the ISP at issue here) permission to access this virtual location information. The *Warshak* court rejected the idea that contractual reservation of a right of access to emails (for certain purposes) would defeat an expectation of privacy. *See id.* A "mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.* In coming to this conclusion, the *Warshak* court analogized emails to hotel rooms: "Our conclusion finds additional support in the application of Fourth Amendment doctrine to rented space. Hotel guests, for example, have a reasonable expectation of privacy in their rooms" (which receive housekeeping and similar services). *Id.* at 287. The analogy compelled the conclusion that "some degree of routine access is hardly dispositive with respect to the privacy question." *Id.* The Sixth Circuit's analysis received affirmation in the Supreme Court's rejection of the third-party doctrine in *Carpenter*. *Cf. Carpenter*, 138 S. Ct. at 2220.

B. The internet-browsing information revealed by Comcast here (under an administrative subpoena) is at least as intimate as the location data at issue in Carpenter where the Court granted Fourth Amendment protections.

In considering *Carpenter* on remand, the Sixth Circuit discussed the need for courts to "carefully and incrementally adapt their Fourth Amendment jurisprudence to advancements in the digital era." *See United States v. Carpenter*, No. 14-1572, 2019 U.S. App. LEXIS 17383, at *12 (6th Cir. June 11, 2019) (on remand from U.S. Supreme Court) (*Carpenter II*). In the context of IP addresses, administrative subpoenas, and online tracking, the need to keep pace with technological developments becomes even more pronounced. As the Sixth Circuit recognized in *Carpenter II*, key to the Supreme Court's reasoning in *Carpenter* "was the inability of CSLI to distinguish between public and private life: because a cell phone 'faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales,' any collection of CSLI risks opening 'an intimate window into a person's life.'" *Id.* at *8 (citation omitted).

Such data can reveal not only particular movements, but (through those movements) familial, political, professional, religious, and sexual associations. *Id.* at *8-*9.

Tracking someone's online movements, effected in the privacy of their own home while sitting in front of their own laptop, involves an even more intimate record. Decades ago, few could or would have imagined a society in which someone's phone goes everywhere with its them, comprehensively tracking all of their movements. *See id.* at *9. Nor could courts of a few decades ago have anticipated the "depth, breadth, and comprehensive reach" of the data used by law enforcement today. *Id.* How much less could society have anticipated the comprehensive picture of a person's life their internet browser history paints. To keep pace with technology, courts must begin to recognize privacy interests in this history, in this virtual location data. The Fourth Amendment requires a warrant to obtain such data.

C. An administrative subpoena cannot provide protections to satisfy the Fourth Amendment in this context, which involves extremely intimate details of a person's life, often sown completely within the private sphere of the home.

In Mr. Howland's case, "[i]nvestigators served an administrative subpoena on a Comcast IP address that tracked the parcel that was seized on December 29, 2017." *See* Attachment, Continuation of Warrant Application, at 3, ¶ 9. This subpoena supposedly "revealed the IP address registered to Johaun HOWLAND," with an address on Lantana Drive in Kentwood, Michigan. *Id.* An administrative subpoena does not require any judicial review. *See, e.g.*, U.S. Dept. Justice, Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities*, *available at* https://www.justice.gov/archive/olp/rpt_to_congress.htm#b8 (an "agency's exercise of administrative subpoena authority is not subject to prior judicial approval"; judicial review arises only "upon a recipient's motion to modify or quash the subpoena or upon an agency's initiation of a judicial enforcement action").

In *Carpenter*, at least, two magistrate judges had "issued court orders granting the Government's request to compel the production of Carpenter's CSLI." *Carpenter II*, 2019 U.S. App. LEXIS 17383, at *11-*12. No such judicial review occurred here with the subpoena, an especially troubling situation given the discussion of heightened privacy concerns included above. Not only was there no judicial review, this lack of review occurred in a sphere in which the privacy interests at stake militate in favor of a *heightened* standard for probable cause.

X. The warrant application here sought permission to search and seize data far beyond the scope of the investigation.

The warrant application here requested permission to search and seize data far beyond the scope of the investigation. The list of data and records to be searched and seized was overbroad and unparticularized, severely lacking specificity. For example, the affiant requested "[a]ll text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message." *See* Attachment, Continuation of Warrant Application—Attachment B, at 2, ¶ c. To allow the government access to these logs for phones completely unrelated to the investigation—simply because the user of a phone sent or received (even as a "wrong number") something to or from the target phone—constitutes an abuse of the Fourth Amendment. Likewise, with the request for "[a]ll voice mail [sic], text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier," one sees an end run around the strictures of the wiretap statutes. *See id.* at 2, ¶ a.

To intercept phone communications, of course, the government must satisfy the dictates of 18 U.S.C. § 2518. Obtaining historical (yet recent) data with a regular warrant, and to this broad extent, makes a mockery of the wiretap rules. Even from a more basic Fourth Amendment perspective, this warrant fails. A search warrant must describe property and items to be searched and seized with sufficient specificity. *See, e.g.*, *United States v. Embry*, 625 Fed. App`x 814, 817 (9th Cir. 2015). A warrant cannot pass muster if it authorizes "wholesale seizures of entire categories of items not generally

evidence of criminal activity," and if it provides insufficient guidelines to allow officers to distinguish items used lawfully from those the government had probable cause to seize. *See id.*

As in *Embry*, where the Ninth Circuit invalidated the warrant and refused to apply the good-faith exception, the warrant here simply let officers have virtually unfettered access to phone records, which in the modern age means unfettered access to *all* a person's records. *Cf. id.*; *see also Riley*, 573 U.S. at 386. As with the warrant in *Embry*, the warrant here cannot stand.

XI. The warrant application for cell-phone data from Target Phone 2 contained reckless misstatements that warrant a *Franks* hearing.

As Mr. Howland has argued regarding other warrants, and the wiretap applications, in this case, this warrant contains misstatements meriting a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978).

XII. The good-faith exception to the warrant requirement does not apply.

The exclusionary rule, and its concomitant remedy of suppression of illegally obtained evidence, under the Fourth Amendment encompasses the primary evidence obtained as a direct result of an illegal search or seizure and any evidence later derived from the original illegality: the fruit of the poisonous tree. *Powell*, 847 F.3d at 768. Here, that remedy applies, providing for suppression of all the data gathered under these ping warrants *and* all evidence gathered as a result of that data, including evidence gathered under warrants that relied on that data.

The good-faith exception to the warrant requirement does not apply to abrogate this position. Excluding evidence obtained in violation of the Fourth Amendment aims at deterring future Fourth Amendment violations. *Id.* at 772. In Mr. Howland's case, it would do just that. Courts have outlined four scenarios "when good-faith reliance on a warrant is not sufficient." *See Powell*, 943 F. Supp. 2d at 783. First, the exception does not apply "when the warrant is issued on the basis of an affidavit that the affiant knows (or is reckless in not knowing) contains false information." *Id.* Second, it does not apply "when the issuing magistrate abandons his neutral and detached role and serves as a rubber

stamp for police activities." *Id.* Third, it does not apply "when the affidavit is so lacking in indicia of probable cause that a belief in its existence is objectively unreasonable." *Id.* And fourth, it does not come into play "when the warrant is so facially deficient that it cannot reasonably be presumed to be valid." *Id.*

Here, authorities knew they were flirting with a problematic search. First, the *Franks* issues vitiated any possible application of the good-faith exception. Second, the affiant has served as a DEA special agent since August 2015. Given the rapid and volatile evolution of case law in this area, one can safely assume she would have received some training on these issues. This area of law was extremely fluid from the 2010s onward with cases like *Warshak*, *United States v. Jones*, 565 U.S. 400 (2012), the *Powell* decisions (both district and appellate), and those leading to *Carpenter* (including *United States v. Rios*, 830 F.3d 403, 427-29 (6th Cir. 2016), the Latin Kings case with which this Court is quite familiar, and which presented these issues to the point the Supreme Court ordered further briefing when the petition for a writ of certiorari was pending in the lead up to the *Carpenter* decision).

Regardless of *Carpenter* not being released until three months after the warrant application at issue, *Warshak* was out. *Jones* was out. The *Powell* district-court decision had taken a powerful position. *Carpenter* was pending in the Supreme Court. *Rios* had attracted the Supreme Court's attention. In *Warshak*, the Sixth Circuit declared unconstitutional segments of the Stored Communications Act. *Warshak*, 631 F.3d at 288 ("Moreover, to the extent that the SCA [Stored Communications Act, 18 U.S.C. § 2701 et seq.] purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.") The winds blowing around this area of law established that officers needed warrants for things like email, and they prefigured the decision in *Carpenter*.

Finally, the warrant here presented as facially deficient because of the overbreadth and particularity issues discussed above. *See Embry*, 625 Fed. App`x at 817 (finding that "the good faith exception cannot be used to rescue a search warrant that is facially overbroad, such as the one at issue here").

For all these reasons, a reasonable officer would not have relied on this warrant application to obtain the subject phone and location data. A reasonable officer especially would not have relied on the conclusory and truncated information related to the IP address. Any reasonable officer would have delved further into the issue of the IP address—perhaps researching who might have had access to the wireless router and whether the network was unsecured.

Mr. Howland asks the Court to suppress all evidence derived from the "ping" warrants obtained for Target Phone 2 and the other phones discussed in footnote 1 above. Such evidence includes all evidence derived from the execution of search warrants that relied on these "ping" warrants.

Defendant has moved this Court to suppress all evidence the government derived from the April 6, 2018 tracking warrant for the white 2017 Ford pickup truck (from case number 1:18-MJ-97); the May 15, 2018 search warrant for a residence on Lantana Drive in Kentwood (from case number 1:18-MJ-135); and the May 15, 2018 search warrant for a residence on Neland Avenue in Grand Rapids (from case number 1:18-MJ-139). The affidavits in support of these warrants relied significantly on evidence obtained through the illegal wiretap of the phone with a number ending in 9351 (referred to as Target Phone 1 by the government).

Mr. Howland has also moved the Court to suppress all evidence obtained through the wiretap of the phone. *See* RE. 296, PageID # 1130. And he has moved for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), and for suppression on minimization grounds.

XIII. The wiretap of phone 9351 led to issuance of multiple later warrants, which now constitute the fruit of the poisonous tree, and all evidence derived under these subsequent warrants must be suppressed.

As Mr. Howland has hit on very briefly in his other motions related to the wiretap of the phone with a number ending in 9351 (or Target Phone 1, as the government has called it), the wiretap of phone 9351 cascaded into multiple later warrants. These later warrants constitute fruit of the

poisonous tree, and all evidence derived under these warrants should be suppressed. The government may not present evidence, in any proceeding, derived from illegally intercepted communications. *See* 18 U.S.C. § 2515; *see also United States v. Giordano*, 416 U.S. 505, 508 (1974).

These warrants include, but are not limited to:[6]

- The April 6, 2018 tracking warrant for the white 2017 Ford pickup truck from case number 1:18-MJ-97;
- The May 15, 2018 search warrant for a residence on Lantana Drive in Kentwood, from case number 1:18-MJ-135;
- The May 15, 2018 search warrant for a residence on Neland Avenue in Grand Rapids, from case number 1:18-MJ-139.[7]

Each of these warrants relied heavily on the illegal wiretap for support.[8] For example, in the April 6, 2018 tracking warrant for the Ford pickup, the affiant stated: "During the course of the interception of Target Phone 1, investigators have intercepted HOWLAND using the phone in furtherance of drug trafficking and then surveilled him utilizing the Target Vehicle. The intercepted communications suggested that he would use the Target Vehicle to complete a transaction." Case No. 1:18-MJ-97, Continuation of Application for Tracking Warrant, at 6 (defense counsel does not have ECF-stamped copies of these sealed records). For the Lantana and Neland residential warrants, the affiant referred to "Title III phone intercepts, phone toll analysis, physical surveillance, administrative subpoena returns, and recorded phone calls," as establishing that "HOWLAND is responsible for coordinating narcotics shipments . . . and for coordinating payments for the narcotics to COLBERT." Case No. 1:18-MJ-135, RE. 1-1, PageID # 12; Case No. 1:18-MJ-139, RE. 1-1, PageID # 12.

---

[6] Mr. Howland believes additional warrants and evidence constitute derivative evidence meriting suppression. He will offer argument on other warrants derived from the wiretap, and other derivative evidence in general, under separate cover.

[7] Should the government raise a "standing"/reasonable-expectation-of-privacy issue related to the Neland Drive residence, Mr. Howland would respond with the fact that the governing statutes and case law call for the suppression of *all* evidence derived from an illegal wiretap, as Mr. Howland has already discussed. *See, e.g.*, 18 U.S.C. § 2515; *see also Giordano*, 416 U.S. at 508.

[8] The Lantana Drive and Neland Avenue warrants also relied on the phone-ping warrants that represent constitutional infirmities. Mr. Howland will move for all evidence derived under the problematic phone-ping warrants under separate cover.

The affiant also referred to Title III intercepts in alleging that Mark Martin was involved in narcotics shipping, that Robert DeGroot participated in heroin dealing with Mr. Howland, that Sterling Hickmon trafficked in cocaine and heroin, that Jamica Taylor aided Mr. Howland with narcotics dealing, and that Jacarr Cox participated in fentanyl and heroin trafficking. Case No. 1:18-MJ-135, RE. 1-1, PageID # 12-15; Case No. 1:18-MJ-139, RE. 1-1, PageID # 12-15 (the warrant applications do not always include the specifics of the wire interceptions, sometimes referring to a specific phone, and sometimes omitting that detail; Mr. Howland has not cited here the passages relying specifically on the tap of Target Phone 3).

The Lantana- and Neland-residence warrant applications also referred specifically to the wiretap application for phone 9351/Target Phone 1. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 16; Case No. 1:18-MJ-139, RE. 1-1, PageID # 16. They relied on a "toll analysis between JUSTIN MARTIN's phone number and HOWLAND's phone [that] revealed approximately 87 calls and 63 text messages between December 1, 2017, and April 2, 2018." *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 23; Case No. 1:18-MJ-139, RE. 1-1, PageID # 23. Later, the warrants relied on the wiretap specifically: "On April 6, 2018, investigators monitoring HOWLAND's phone intercepted a text message conversation between him and ROBERT DEGROOT. During that conversation, the two arranged a drug deal at approximately 9:40 a.m." Case No. 1:18-MJ-135, RE. 1-1, PageID # 24; Case No. 1:18-MJ-139, RE. 1-1, PageID # 24.

In relating the details of an alleged drug transaction, the Lantana and Neland warrant applications cited a supposed incident in which the wiretap allegedly resulted in evidence of narcotics trafficking. On April 6, 2018 (which fell within the monitoring period for phone 9351), around "11:48 a.m., HOWLAND received an incoming phone call from DEGROOT and HOWLAND instructed DEGROOT to meet him at the corner of 29th and Breton." Case No. 1:18-MJ-135, RE. 1-1, PageID # 24; Case No. 1:18-MJ-139, RE. 1-1, PageID # 24. Investigators could not locate the vehicle after it

"exited MARK MARTIN's apartment complex," but "based on the wire interceptions, investigators believe that HOWLAND was meeting with DEGROOT for the purposes of conducting a narcotics transaction." Case No. 1:18-MJ-135, RE. 1-1, PageID # 24; Case No. 1:18-MJ-139, RE. 1-1, PageID # 24.

Regarding a package, the Lantana and Neland warrant applications refer to monitoring Mr. Howland's phone and intercepting phone contact between Mr. Howland, and Hickmon, Martin, and Newbern. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 32-34; Case No. 1:18-MJ-139, RE. 1-1, PageID # 32-34. The warrant applications go on to refer to intercepted calls that the affiant believed related to firearms. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 41-42; Case No. 1:18-MJ-139, RE. 1-1, PageID # 41-42. Then the warrant applications discuss a call, ostensibly between Mr. Howland and Jacarr Cox, and a supposed narcotics order. *See* Case No. 1:18-MJ-135, RE. 1-1, PageID # 48-49; Case No. 1:18-MJ-139, RE. 1-1, PageID # 48-49. This extensive reliance on the wiretap of phone 9351 demonstrates these warrants' wiretap-derivative nature . . . and the need for suppression of all evidence seized in accordance with them.

Congress has carefully circumscribed the government's power to engage in the extraordinary intrusion of wiretapping. A violation of the rules results in suppression of *all* evidence derived from the illegal wiretap. The affidavits in support of the April warrant for the 2017 Ford pickup and the May warrants for residences on Lantana Avenue and Neland Drive relied on the communications and evidence derived from the illegal wiretap of phone 9351. All evidence derived under these warrants thus represents evidence derived from the illegal wiretap. For these reasons, Mr. Howland asks the Court to suppress all evidence derived from the wiretap of phone 9351/Target Phone 1, including evidence derived under these three derivative warrants.

Because it seems clear that the prosecution used illegally intercepted communications during the grand-jury proceedings in this matter, such proceedings must now be revisited. Any illegally

intercepted communications should have been suppressed and unavailable for grand-jury proceedings. And any proceedings that relied on these interceptions must now be struck.

XIV. Section 2515 explicitly calls for suppression of all evidence—without qualification—derived from illegal wiretaps. If the prosecution presented such evidence to the grand jury as a foundation for the indictments issued, such indictments should now be struck.

Under 18 U.S.C. § 2515, a court must suppress all evidence derived from an illegal wiretap—namely a wiretap conducted in violation of Chapter 119 of Title 18. Whenever the government intercepts wire or oral communications in violation of the chapter, it may not use those communications, or any evidence derived from them, "in any trial, hearing, or other proceeding in or before any court," including before a grand jury. 18 U.S.C. § 2515.

This suppression provision reflects the gravity with which Congress considers wiretaps. In Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (addressing 18 U.S.C. §§ 2510 through 2522), Congress discusses, and place strict limits on, wiretaps. These limits reflect the act's "essential purpose," which "was to combine a limited and carefully articulated grant of power to intercept communications with an elaborate set of safeguards to deter abuse and to expunge its effects in the event that it should occur." In re *Evans*, 452 F.2d 1239, 1243 (D.C. Cir. 1971). Courts have admonished that "[i]t is thus important to keep in mind not only the powers that Congress was willing to grant, but also those that it refused to make available despite the needs of law enforcement." *Id.* Since the act's prohibitions and limitations stand as preconditions "to the acceptability of any wiretapping at all, [courts] must enforce them zealously or else throw Congress's entire conception into jeopardy." *Id.*

Here, such enforcement means ordering production of the grand-jury transcripts related to this matter and, if such transcripts show use of illegally obtained wiretap evidence (or evidence derived from such wiretaps), quashing the resulting indictments. While a committee report behind the wiretap legislation suggests that "one who has been illegally wiretapped but is not a witness called by the grand

jury may not move to suppress; and that even a witness or defendant who objects to the use of illegal wiretaps in the proceedings may not move to quash the entire proceeding or even an indictment growing out of it," courts have rejected the idea of leaving an aggrieved person without a remedy. *See id.* at 1245-46 (discussing committee report). To this end, courts have interpreted § 2518(10)(a) as permitting an attack by a grand-jury witness on the admissibility of evidence seized in violation of the Fourth Amendment. *See id.* at 1246.

On a fundamental level, the analysis starts with ascertaining whether illegally obtained evidence came before the grand jury. Under 18 U.S.C. § 3504(a)(1), "when a party aggrieved by an unlawful wiretap moves for the suppression of evidence on the basis of the alleged interception, the opponent of the claim must affirm or deny the allegation." *Id.* at 1247. Specifically, as found by the D.C. Circuit in In re *Evans*, a defendant may request relief if they suspect wiretap abuses. *See id.* The dissent in *Evans* looked at a senate report addressing Title III of the Omnibus Crime Control Act to support its contrary position; the report suggested that, because no one is a *party* to a grand-jury proceeding, no one stands eligible to bring a motion to suppress evidence in such a proceeding. *See id.* at 1258 (Wilkey, J., dissenting). The majority, of course, rejected this position. But even without a resort to this case law, such a position must fail in the instant case because Mr. Howland is not attacking the subject evidence only in a grand-jury setting, preindictment. He is attacking the evidence in a trial court, as a party to the action, and in accordance with § 2515's prohibition on *all* use of illegally obtained wiretap evidence.

The dissent in *Evans* focused on the issue of a grand-jury *witness* raising a wiretap issue—rather than a defendant raising the issue. *See id.* at 1261 (Wilkey, J., dissenting) (commenting on a "mere witness"); *see also id.* at 1266, 1271-72 (Wilkey, J., dissenting). One has to wonder if the dissent would have seen things the same way had a defendant been raising the issue post-indictment. If courts were to change course (the majority in *Evans* allowed even a "mere witness" to bring a challenge) and

disallow grand-jury challenges, one would have to wonder how the dictates of § 2515 would find vindication. In citing Ninth Circuit case law on the issue, the *Evans* dissent implicitly recognized this need for an avenue for vindication. It cited the Ninth Circuit as concluding: "'As witnesses [before a grand jury], they have no standing to question the source of the government's information. It will be time enough to do that if any of them *should ever become a defendant*, a most unlikely event in view of the immunity granted them.'" *Id.* at 1262 (Wilkey, J., dissenting) (emphasis added).

Likewise, the dissent pointed out cases frowning on *pre-indictment* motions to suppress before the grand jury. *See id.* at 1262-63 (Wilkey, J., dissenting). None of these cases rebuff defendants' post-indictment efforts to enforce wiretapping prohibitions. Nor does an ostensible judicial authorization of a wiretap effect such a rebuff when a later, reviewing, court finds that wiretap to have been illegal. *Cf. id.* at 1242 n.12 (pointing out in dicta, but not truly addressing the issue of, prior judicial authorization of a wiretap). If later judicial condemnation of a wiretap could not right the earlier wrongs of that tap, relief would be a mere chimera.

The *Evans* court, the majority and dissent, discussed *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920), and its conclusion, in the grand-jury context, that "[t]he essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all." While the *Silverthorne* Court recognized concepts like the independent-source doctrine, it remained steadfast on the fundamental issue: "the knowledge gained by the Government's own wrong cannot be used by it in the way proposed." *Silverthorne Lumber Co.*, 251 U.S. at 392.

The majority's decision in *Evans* parallels the Third Circuit's decision in In re *Grand Jury Proceedings*, 450 F.2d 199 (3d Cir. 1971). The court in that case offered pellucid guidance: "Section 2515 is an unequivocal bar to questioning one before a grand jury if the questions are derived from electronic surveillance conducted in the absence of a properly issued warrant and aimed at the witness,

if the witness himself objects to the interrogation." *Grand Jury Proceedings*, 450 F.2d at 202. The court found that "Congress in § 2515 specifically prohibited the disclosure to a grand jury of evidence derived from illegal wiretaps." *Id.* In considering legislative history, the court found ambiguity. *See id.* at 205.

While Mr. Howland recognizes that the exclusionary rule's interdiction of the use of tainted evidence does not necessarily extend to barring prosecution altogether, the extent of the wiretap evidence in this case, and the government's heavy reliance on it (as evidenced in the numerous warrants referring to it), suggest that the grand-jury proceedings here would have focused on the contents of illegally intercepted communications and evidence derived from these communications. *Compare id.* So the dicta in *Grand Jury Proceedings* musing about legislative history and reluctance to quash an indictment based on illegal wiretap evidence having come before a grand jury cannot answer the question here, where such evidence seems likely to have been the proverbial "main event" for the grand jury. *Cf. id.* at 205-06. The *Grand Jury Proceedings* court actually read *Silverthorne* to support Mr. Howland's position: grand-jury witnesses may not constitutionally be held in contempt for failing to respond to a subpoena when the government is seeking to avail itself of evidence, obtained by illegal means, which it otherwise would not have had. *See id.* at 211. The Fourth Amendment prevents the government from using illegally seized evidence as the basis for questioning an aggrieved party in front of a grand jury. *Id.*

The *Grand Jury Proceedings* court saw that matter as straightforward. It felt that "[o]nly in a minimal number of cases" would the government "be found to have conducted surveillance in violation of the statute," and in such cases, "the hearing will not be overly complicated or lengthy, because the primary matter of inquiry would be whether the Government can demonstrate an independent basis, aside from the illegal surveillance, upon which to justify the questions propounded

before the grand jury." *Id.* at 216. The government "would have the burden of proof in attempting to dull the edges of a constitutional right." *Id.* at 216-17.

The *Grand Jury Proceedings* concurrence emphasized the need to have an avenue for relief if the government used illegally obtained wiretap evidence in a grand-jury proceeding. If a prosecutor called as a grand-jury witness an agent who had participated in an illegal wiretap or listened to tapes of such a tap, or introduced the tapes themselves before the grand jury, they would be violating the law. *See id.* at 219 (Rosenn, J., concurring). An "aggrieved person should be able to stand mute and in the event of a subsequent civil contempt proceeding, raise the unequivocal prohibition of Section 2515 as a defense to a finding of contempt, unless the prosecutor can show an *untainted independent basis* for the questions sought to be asked." *Id.* (emphasis added). All Mr. Howland seeks here is the same remedy—a chance to challenge the grand-jury evidence. If the government can prove the illegal wiretaps did not taint the evidence presented, then the indictments obtained can stand.

The *Grand Jury Proceedings* concurrence found § 2515 compelling, and felt that Congress, in enacting § 2515, "undoubtedly weighed the competing policy considerations involved in excluding tainted evidence from grand jury consideration" and then concluded that § 2515 should provide a remedy for those aggrieved by illegal wiretaps who chose to stand mute before a grand jury. *See id.* at 220 (Rosenn, J., concurring). Congress, the concurrence felt, expressed "strongly" a "desire to eliminate illegal electronic eavesdropping," and reading § 2515 as the court did would provide "victims of illegal surveillance with a semblance of some minimal relief in the fact of 'an unlawful invasion of privacy.'" *Id.*

The dissent (frowning on expanding standing to challenge grand-jury evidence related to illegal wiretaps) seemed to suggest that even a defendant would have to wait until an indictment issued to bring a challenge. *See id.* at 227 (Gibbons, J., dissenting). But the dissent did *not* suggest a *defendant* should be left without a remedy altogether. *See id.* Rather, the dissent looked to cases discussing the

gravity of government violations of the Fourth Amendment. The government, these cases emphasized, cannot violate the Fourth Amendment and then use the fruits of its unlawful conduct to secure a conviction. *Id.* at 229 (Gibbons, J., dissenting). Nor can the government make indirect use of illegally obtained evidence (the citation the dissent looked to even included a nod to *Silverthorne*). *Id.* Likewise, the government cannot support a conviction on evidence derived from the unlawfully obtained evidence. *Id.* The law forbids all these "methods," and courts must invalidate any convictions obtained by means of them because these methods "encourage the kind of society that is obnoxious to free men." *Id.* (citation omitted).

The majority recognized that alternatives to suppression (namely a civil action for money damages) will not make an aggrieved party whole. *See id.* at 213 n.20. Going back some seventy years, one can see that courts have never meant to leave parties with only these inadequate civil remedies. In In re *Fried*, 161 F.2d 453, 458 (2d Cir. 1947), the Second Circuit stated that, "[i]f an article has been illegally seized by a federal official, its potential use as evidence will be restrained by a district court, although no indictment is pending."

The *Fried* court's reasoning for its decision warrants a thorough examination. In *Fried*, the government had argued "that an indictment founded upon such illicit evidence will do the applicant no harm, since such evidence will not be admitted at the trial which follows the indictment." *Fried*, 161 F.2d at 458. The *Fried* court found this position to be "astonishingly callous" and one that "ignore[d] the obvious." *Id.* Wrongful indictment are no laughing matter: they often work "grievous, irreparable injury" to those who are indicted. *Id.* The stigma of an indictment "cannot be easily erased"; "[i]n the public mind, the blot on a man's escutcheon, resulting from such a public accusation of wrongdoing, is seldom wiped out by a subsequent judgment of not guilty." *Id.* The public will often remember "the accusation, and still suspect[] guilt, even after an acquittal." *Id.* at 458-59. Prosecutors wield "an immense discretion in instituting criminal proceedings which may lastingly besmirch

reputations," an "almost completely unfettered" discretion. *Id.* at 459. This discretion "should surely not extend so far as to preclude judicial interference with a prosecutor's aim to induce an indictment by offering to a grand jury evidence which is the product of illegal acts of federal officers." *Id.*

Allowing a challenge to grand-jury proceedings that leaned heavily on illegal wiretaps simply vindicates the judiciary's interest in "clean" proceedings. Such allowance does not involve prematurely barring an entire prosecution that could have been founded on untainted evidence. *Cf. United States v. Blue*, 384 U.S. 251, 255 (1966). In *Blue*, the Supreme Court discussed the government's potential use of tainted evidence, positing that "[o]ur numerous precedents ordering the exclusion of such illegally obtained evidence assume implicitly that the remedy does not extend to barring the prosecution altogether." *Id.* In *Blue*, however, no one "contended that tainted evidence was presented to the grand jury." *Id.* at 255 n.3. While the Court said in dicta that "our precedents indicate this would not be a basis for abating the prosecution pending a new indictment, let alone barring it altogether," the Court was *not* considering a grand-jury proceeding based primarily on illegally obtained evidence. *See id.*

In such circumstances—those of a grand jury primarily hearing evidence from illegal wiretaps—some avenue for relief must exist, and it would not burden courts to consider transcripts, excise the illegally obtained evidence, and consider whether the remaining evidence established probable cause to support an indictment. The process would resemble that for warrants based on misstatements. *Compare Franks v. Delaware*, 438 U.S. 154 (1978). Review would likely take far less time than that involved in considering the legality of the wiretap itself under 18 U.S.C. § 2518, either to issue authorization for the wiretap or in response to a motion to suppress. Given the interests involved and the precedent available on the need for curbing unlawful law-enforcement investigations, courts do not and should not countenance prosecutors using illegally obtained evidence during grand-jury proceedings.

The interests at stake involve far more "than just the smooth functioning of grand jury investigations." In re *Evans*, 452 F.2d at 1249. Grand-jury proceedings—"indeed our entire criminal process—could be streamlined if our laws and Constitution left room for draconian efforts to obtain evidence from defendants or witnesses." *Id.* Yet while it is "perhaps less crude than some of the measures which might be employed, electronic surveillance nevertheless menaces the interests protected by the fourth amendment," and it represents "the greatest leveler of human privacy ever known." *Id.* (footnote omitted). Where such surveillance occurs "without legal sanction, Congress wisely concluded that any evidence it yields should not be admissible before a court or grand jury." *Id.* "That result may well be inefficient, but Congress considered it an indispensable prerequisite for insuring that law enforcment [sic] officials obey the law." *Id.*

The *Grand Jury Proceedings* court had equally grave words to share on the matter: "we must be ever mindful of the admonition that in a government of laws, the very existence of the Government will be imperiled if it fails to observe the law scrupulously." *Grand Jury Proceedings*, 450 F.2d at 217. By its example, "the Government teaches the whole people." *Id.* And if the government breaks the law, "it breeds contempt for law." *Id.* To allow the government to "commit crimes in order to secure the conviction of a criminal may well bring unfortunate retribution." *Id.*

Mr. Howland asks the Court to order production of the grand-jury transcripts in this case and consider the effect the illegal wiretap evidence had on these grand-jury proceedings.

Mr. Johaun Howland has moved this Court to suppress all evidence derived from the wiretaps and "ping" warrants in this matter. He has raised the issue of suppressing all evidence derived the illegal wiretaps in this case, including evidence discovered in accordance with subsequent warrants issued in this case (including the residential warrants issued). In this regard, he has so far focused on residences and property in which he unequivocally enjoyed a reasonable expectation of privacy (colloquially called "standing" at times). Passing beyond just this property and these residences, he

now moves the Court to suppress all evidence derived from all residences and property (including electronic devices and a package in the U.S. mail) for which the issued warrants relied on the illegal wiretaps. Because these warrants were derived from the wiretaps, the statutes at issue call for suppression, regardless of expectations of privacy. In support of his position, Mr. Howland offers this memorandum of law.

As the Court knows, this case involves multiple wiretaps and "ping" warrants, which Mr. Howland has challenged. Based on evidence obtained through these wiretaps and warrants, the government obtained warrants for seven residences, a package in the U.S. mail (with a tracking number ending in 8863 US), and numerous electronic devices. For example, the affiant from the earlier warrants and wiretap applications filed the application for the residential warrants on May 15, 2018. *See, e.g.*, Case No. 1:18-MJ-139, RE. 1-1, PageID # 4-5. Much of the evidence used to try to establish probable cause to issue these residential and electronic-device warrants rested on evidence derived from the wiretaps and pings. *See, e.g.*, *id.* at 19, ¶ 24 (referring to ping warrant in residential application); 48, ¶ 122 (citing intercepted call in residential application); *see also* Application for Search Warrant for 9 Electronic Devices (May 31, 2018), at 7, ¶ 12; 11, ¶ 23; *and* May 9, 2018 Application for Search Warrant for Priority Mail Express Parcel, at 3, ¶¶ 11-12; 8, ¶ 24. Mr. Howland now moves to suppress all of this evidence derived from illegal wiretaps (under § 2515) and as the fruit of the poisonous tree of the illegal ping warrants (under the Fourth Amendment).

XV. Section 2515 explicitly calls for suppression of all evidence—without qualification—derived from illegal wiretaps.

Under 18 U.S.C. § 2515, a court must suppress all evidence derived from an illegal wiretap—namely a wiretap obtained in violation of Chapter 119 of Title 18 of the U.S. Code. The statute contains no qualifiers: "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and *no evidence derived therefrom* may be received in evidence in any trial . . . if the disclosure of that information would be in violation of this chapter." 18 U.S.C. § 2515.

Chapter 119 speaks only of "aggrieved persons," any "person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." 18 U.S.C. § 2510(11). An "aggrieved person in any . . . proceeding in or before any court . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, *or evidence derived therefrom*." 18 U.S.C. § 2518(10)(a).

If suppression arguments rest on a statute (rather than the Fourth Amendment), and that statute does not provide for suppression, suppression may not be available as a remedy. *See United States v. Powell*, 847 F.3d 760, 771 (6th Cir. 2017).[9] The natural extension of this idea is that, if a statute governs suppression, the statutory language will provide the parameters for relief. As the cases Mr. Howland discusses in his motion to quash the indictment in this case explain (that motion resting on use of the illegal wiretap evidence, and evidence derived from that material, before the grand jury), § 2515 provides broad prohibitions on the use of illegal wiretap evidence and its derivatives. The section also confers standing to challenge use of such evidence on less likely "players," including grand-jury witnesses who receive immunity.

Standing, of course, concerns (apart from the case or controversy test) analysis of whether the interest a complainant seeks to protect arguably falls within the zone of interests protected or regulated by the statute or constitutional guarantee in question. *See* In re *Grand Jury Proceedings*, 450 F.2d 199, 210 (3d Cir. 1971). In the wiretap context, the concerns focus not on the usual "expectations of privacy" so familiar in the residential-warrant context but on the "sweeping" "prohibition against the use of evidence tainted by an unlawful wiretap." *See* In re *Evans*, 452 F.2d 1239, 1243 (D.C. Cir. 1971). In *Evans*, for example, the majority granted a grand-jury witness the right to challenge an alleged wiretap,

[9] Here, Mr. Howland has raised a Fourth Amendment issue, as discussed in his motions to suppress these wiretaps (and their memos in support).

even without a showing that agents tapped *her* phone. *See id.* at 1254 (Wilkey, J., dissenting); *see also id.* at 1250 (the majority discussing whether "some telephones" had been tapped).

Essentially, the Omnibus Crime Control and Safe Streets Act makes it a crime for anyone (including government agents) "not only to intercept illegally any wire or oral communication, but also to use the contents thereof for any purpose." *Id.* at 1252 (Wright, J., concurring). Under § 2515, the government cannot engage in the "use of the fruit of such crimes in grand jury proceedings." *Id.* To exact, by court order, testimony that is the fruit of wiretapping crimes from a witness before the grand jury would not only involve the courts and the witness in the commission and exploitation of these crimes, but it would also do so in defiance of the explicit command of the statute. *Id.*

One can draw from these conclusions the breadth of § 2515's prohibitions: the government simply cannot use any evidence derived from illegal wiretaps. A defendant can challenge the use of such evidence, regardless of any traditional conceptions of "expectations of privacy." On the most basic level, "a district court may not compel the violation of an express congressional prohibition," and § 2515 "of the Act directly and clearly forbids the presentation to a grand jury of evidence derived from the contents of oral communications improperly obtained." *See Grand Jury Proceedings*, 450 F.2d at 209. The prohibition, of course, extends to trial. *See* 18 U.S.C. § 2515. The analysis revolves around "information discovered through the use of unwarranted wiretaps," rather than the stage of the proceedings. *See Grand Jury Proceedings*, 450 F.2d at 210.

Given this broad congressional prohibition on the use of evidence derived from illegal wiretaps, Mr. Howland can now challenge *all* evidence derived from the illegal wiretaps in this case, even evidence derived from residences, devices, and packages for which he may lack the traditional "reasonable expectation of privacy" . . . if the warrants for those residences and property rested on evidence derived from the illegal wiretaps.

While the fact pattern differs somewhat, *Alderman v. United States*, 394 U.S. 165 (1969), demonstrates the Supreme Court's longstanding condemnation of illegal wiretaps, even when the privacy interests at stake branch out somewhat. In *Alderman*, the Court considered challenges from defendants whom authorities had "overheard" in illegal wiretaps conducted on premises for which these individuals may not have had an expectation of privacy, holding that parties to tapped conversations *and* people who possessed the premises where the tapping/conversations occurred could contest admission of the interceptions (regardless of whether the latter parties participated in the tapped conversations). *See Alderman*, 394 U.S. at 167-68, 178 ("the Fourth amendment protects a person's private conversations as well as his private premises"), 178-80, 185 n.16; *see also id.* at 200-01 (Fortas, J., concurring in part and dissenting in part). In critiquing the *Alderman* majority in his concurrence and dissent, Justice Harlan found fault with a rule that allows premises owners to move to suppress illegally wiretapped conversations that occurred on their premises but in which they did not participate. *Id.* at 189-90 (Harlan, J., concurring in part and dissenting in part). Justice Harlan said, "In the field of conversational privacy, the Fourth Amendment protects persons, not places." *Id.* at 193 (Harlan, J., concurring in part and dissenting in part).

If one flips the *Alderman* conclusions around, one easily finds that the opinion's conclusions support a motion to suppress *all* evidence derived from an illegal wiretap, even evidence derived from residences and property for a which a party may not have the "normal" expectation of privacy—if the searches of those residences rested on warrants that depended on the illegally intercepted communications. In *Alderman*, the parties to the illegally tapped conversations had standing to challenge admission of that evidence, regardless of any property rights in the premises where the taps occurred. The key to the case was the privacy of the conversations—not any standing concepts related to the premises. *See id.* at 178. In this context, the government's use of the illegally obtained

conversation evidence provides the focus. And the government simply cannot use that evidence with impunity to obtain warrants.

In *Alderman*, the government conceded "that when an illegal search has come to light, it has the ultimate burden of persuasion to show that its evidence is untainted." *Id.* at 183. Here in Mr. Howland's case, the prosecution simply cannot make that showing.

XVI. The doctrine of the fruit of the poisonous tree reinforces these conclusions by adding the illegality of the ping warrants into the equations.

If this Court finds that the ping warrants lacked the support of probable cause, the additional warrants derived from those ping warrants constitute fruit from the poisonous tree. This additional—Fourth Amendment—doctrine simply adds fuel to the § 2515 fire here, undermining further any possibility of these subsequent (residential and electronic-device) warrants surviving.

Conclusion

Mr. Howland asks the Court to suppress evidence as specifically identified in the respective sections of his motion to suppress and memorandum in support.

Date: August 5, 2019

SCOTT GRAHAM PLLC

By: /s/ Scott Graham

Scott Graham
Attorney for Defendant
1911 West Centre Avenue, Suite C
Portage, MI 49024
(269) 327.0585
sgraham@scottgrahampllc.com