No. ____

In the
Supreme Court of the United States

Romelly Dastinot,
Petitioner

v.

United States of America,
Respondent

On Petition For Writ of Certiorari to the Court of Appeals for the First Circuit

PETITION FOR WRIT OF CERTIORARI

Timothy E. Zerillo, Bar No. 9108
CJA Appointed *Counsel of Record*
ZERILLO LAW FIRM, LLC
1250 Forest Avenue, Suite 3A
Portland, Maine 04103
tim@zerillolaw.com
207.228.1139

QUESTIONS PRESENTED

1. Was it reversible error for the First Circuit and the District Court to ignore the availability of cell site and GPS tracking against the necessity requirement of Title III, when the agent who drafted the wiretap warrants indicated that the use of such technology would have been helpful to achieve the aims of the wiretap?

2. Was it reversible error for the Court to ignore Petitioner's request for a Franks hearing on the issue of whether the necessity requirement could be met through the use of cell site and GPS tracking?

LISTING OF PARTIES

All parties are identified in the Cover Page of the Petition. None of the parties are corporations.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTORY AUTHORITIES

No. ____

In the
Supreme Court of the United States

Romelly Dastinot,
Petitioner

v.

United States of America,
Respondent

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

Petitioner Romelly Dastinot respectfully petitions for a writ of certiorari to the First Circuit Court of Appeals in docket number CA-16-1272.

OPINION BELOW

Petitioner respectfully prays that a writ of certiorari issue to review the judgment below. The opinions of the United States Court of Appeals for the First Circuit appears in Appendix A to the Petition and is reported in *United States v.*

Gordon, 871 F.3d 35 (1st Cir. 2017) and *United States v. Dastinot*, No. 16-1272 (1st Cir. 2017).

JURISDICTION

The date on which the United States Court of Appeals decided the Petitioner's case was September 13, 2017 and no petition for rehearing was filed. The jurisdiction of this Court is invoked under 28 U.S.C. s.1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the United States Constitution provides "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Further statutory support for the propositions in this Petition is found in Title III, 18 U.S.C. §2518.

STATEMENT OF THE CASE

On December 9, 2014, a federal grand jury returned an indictment against Dastinot and nine co-defendants. Count 1 of the Second Superseding Indictment charged that Dastinot conspired with co-defendants to distribute and possess, with intent to distribute, various controlled substances in violation of 21 U.S.C. §§

841(a)(1), 846. Count 5 of the Second Superseding Indictment charged that Dastinot and one co-defendant possessed oxycodone with intent to distribute in violation of 21 U.S.C. §841(a)(1). Count 8 charged that Dastinot conspired with two co-defendants to launder money in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1956(h).

On October 31, 2014, Dastinot filed a Motion to Suppress Wiretap Evidence Under Title III and Request for a *Franks* Hearing. The District Court denied that Motion on March 23, 2015. On April 17, 2015, Dastinot entered a conditional guilty plea as to Count 1 of the Second Superseding Indictment. The First Circuit denied Dastinot's appeal on September 13, 2017.

These charges were born from a comprehensive investigation into Dastinot and several co-defendants that culminated in the winter and spring of 2014 with the authorization of four wiretaps. The investigation, orchestrated by the Drug Enforcement Agency ("DEA"), Maine Drug Enforcement Agency ("MDEA"), and other law enforcement agencies, gathered information that suggested that Dastinot and another individual named Jacques Victor had organized a drug trafficking operation that was responsible for the importation and distribution of "significant quantities of cocaine base and heroin" into the state of Maine, specifically into the City of Lewiston. Law enforcement used a variety of routine investigative techniques to build the case against Dastinot and Victor, which they laid out in detail in the February 24, 2014 Affidavit in Support of Application for Authorization to Intercept Wire and Electronic Communications by law enforcement Agent Joey Brown.

According to the Brown Affidavit, Dastinot was a crack cocaine trafficker who, along with a Jacques Victor, purchased drugs outside of Maine and then distributed them in the greater-Lewiston, Maine area.

The investigation had been extremely productive. Still, law enforcement contended that more information was needed before moving forward with indictments. The Brown Affidavit summarized the alleged gaps in investigator's knowledge at the time of the wiretap application:

> A primary focus of this investigation is to identify and prosecute all of Dastinot and Victor's sources of supply who are responsible for illegal drugs arriving in Maine for further distribution... the identities of the source(s) of supply are presently unknown. Another objective is to understand the drug relationship between Dastinot and Victor... CS-1 told me that based on his/her dealings with both Dastinot and Victor, he/she believes that the two pool their money together for resupply trips and visit a common source of supply in the Boston area. CS-1 told me that he/she further believes that once Dastinot and Victor are supplied, they primarily deal with separate customers in Maine... review of phone records for TT1 and TT2 shows regular connections between the two numbers as well as connections with common numbers. Despite the indications of a drug trafficking relationship between Dastinot and Victor, I do not know the full extent of their conspiratorial relationship or their individual and collective relationship with the source(s) of supply.

The Court agreed with Agent Brown that wiretaps were necessary, and authorized the initial wiretap in this case on February 24, 2014, amending that order on February 25, 2014. That wiretap targeted Dastinot, Victor, and additional co-defendant, Ashley Gleason. Three subsequent wiretaps were authorized on March 25, 2014, April 24, 2014, and May 1, 2014 respectively. The subsequent wiretaps were based upon the first illegal wiretap.

REASONS FOR GRANTING THE PETITION

When establishing the necessity requirement for the wiretaps against Petitioner, Agent Brown indicated that cell site or GPS tracking would be helpful to establish Petitioner's source of supply. In the same Affidavit, Agent Brown swore that the technology was not available. Petitioner proffered at the District Court level, with no real contradictory information presented by the Government, that cell site and GPS technology was available. Since Agent Brown agreed the technology, if available, would have been helpful, the wiretaps failed to meet the necessity requirement. The District Court failed to consider that Brown's Affidavit did not meet the necessity requirement and the First Circuit blindly stamped its approval. Reasonable requests to hold a *Franks* hearing on this issue were denied or ignored.

I. THE NECESSITY REQUIREMENT WAS PLAINLY NOT MET AND IT WAS REVERSIBLE ERROR FOR THE FIRST CIRCUIT TO IGNORE THE AVAILABILITY OF CELL SITE TRACKING AND GPS TRACKING WHICH THE WARRANT APPLICANT SAID WOULD HAVE BEEN HELPFUL TO HIS INVESTIGATION

To obtain an eavesdropping warrant, 18 U.S.C. §2518(3) mandates that the Government establish that probable cause exists to believe that (i) the individual has committed or is about to commit one of the offenses specified by Congress in Section 2516, (ii) communications concerning that offense will be intercepted, and (iii) the particular telephone or device being tapped is itself being used in the connection with the commission of the offense. The Warrant Judge is also required to find that the wiretap is necessary because "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. §2518(3)(c).

Further, Title III requires that law enforcement provide the authorizing court with a full and complete statement of the facts and circumstances relied upon by the applicant to establish probable cause related to the particular offense being investigated under Title III. 18 U.S.C. §2518 (1)(b). Also required is a full and complete statement as to whether or not other investigative procedures have been tried and failed, why they reasonably appear to be unlikely to succeed if tried or why they are too dangerous. 18 U.S.C. 2518(1)(c). *See also United States v.*

Tortorello, 480 F.2d 764, 773 (2d. Cir. 1973).

A wiretap has been recognized to be an extraordinary intrusion, and a wiretap should be only made available if it is genuinely necessary. In *United States v. Concepcion*, the Court remarked "...it would be in some sense more efficient to wiretap whenever a telephone was used to facilitate the commission of a crime," but, "the cost of such efficiency in terms of privacy interests is too high." 579 F.3d 214, 218 (2d. Cir. 2009) *quoting United States v. Lilla*, 699 F.2d 99, 105 n.7 (2d. Cir. 1983). 18 U.S.C. 2518(d) requires the prosecution provide an affidavit disclosing the use, success and potential success of other investigative techniques. The affidavit is required to show with specificity why in this particular investigation, ordinary means of investigation will fail. *United States v. Robinson*, 698 F.2d 448, 453 (D.C. Cir. 1983); s*ee generally, United States v. Ippolito*, 774 F.2d 1482, 1486 (9^{th} Cir. 1985).

Two independent protections for those aggrieved of a federal wiretap violation co-exist: the Fourth Amendment, and the statutory requirements of Title III. *See United States v. Donovan*, 429 U.S. 413, 432 n.22 (1977) ("The availability of the suppression remedy [for Title III], as opposed to constitutional violations...turns on the provisions of Title III rather than the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights.").

Wiretap law is statutory. Fourth Amendment exclusionary rules are judicially created. As a result, federal courts cannot import Fourth Amendment exclusion exceptions into Title III suppression remedies. This includes the "good faith" exception found in *United States v. Leon*, 468 U.S. 897 (1984).

In *Leon*, the Supreme Court held that the Fourth Amendment did not require exclusion of evidence obtained by law enforcement officers who acted in reasonable reliance on a search warrant which was issued by a detached and neutral magistrate, but was ultimately found to be unsupported by probable cause. As illustrated by *Leon*, federal courts enjoy the freedom to carve exceptions to the court-created Fourth Amendment exclusionary rule. The suppression remedies in Title III, however, were created by Congress, and federal courts cannot alter or limit those remedies.

In addition, to assure the privacy of oral and wire communications, Title III establishes strict procedures for obtaining authorization to intercept such communications. *See generally, United States v. Giordano*, 416 U.S. 505 (1974). These procedures include the requirement that the district court make certain enumerated findings before granting authorization to conduct electronic surveillance. *See* 18 U.S.C. 2518(1), (3) & (4).

Among its other requirements, Title III contains the "necessity" provision that must be satisfied before a wiretap order may lawfully issue. 18 U.S.C. § 2518(1)(c), 2518(3)(c). "This requirement is a critical one." *United States v. King*, 991 F.Supp 77, 82 (E.D.N.Y. 1998). This critical requirement is designed to ensure that the intrusive device of wiretapping "is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." *United States v. Kahn*, 415 U.S. 143, 153 n. 12 (1974); *see also, United States v. Lilla*, 699 F.2d 99 (2d. Cir. (1983) (wiretap procedures are "not to be routinely employed as the initial step of the criminal investigation.").

Pursuant to the necessity requirement:

> Each application for an order authorizing or approving the interception a wire, oral or electronic communication shall include 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.

18 U.S.C. §1528(1)(c).

In addition, before issuing a wiretap order, a district court judge must independently determine that ordinary "investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. §2518(3)(c). In several cases, the necessity requirement has been held to be insufficient. *See e.g. United States v. Castillo-Garcia*, 117 F. 3d 1179 (10th Cir. 1997); *United States v. Gonzalez, Inc.*, 412 F. 3d 1102 (9th Cir.

2005).

Title III authorizes the aggrieved person to seek suppression of any communication that was unlawfully intercepted under Title III or the Fourth Amendment. 18 U.S.C. § 2510(11) and 18 U.S.C. § 2518(10)(a). Indeed, Title III's exclusionary rule is different from and is in addition to the Fourth Amendment's exclusionary rule. It requires suppression where there is failure to satisfy the statutory requirements that implement the intention of Congress to limit the use of intercept procedures only to those situations that call for the employment of this extreme investigative device. *See Giordano*, 416 U.S. at 524; *see also, United States v. Arrequin,* 227 F.Supp. 2d 1057, (E.D. Calif. 2003) (Title III enacted to provide greater protection against wiretapping than that mandated by the Constitution).

When law enforcement officers circumvent the procedural requirements of 18 U.S.C. 2518(1)(c), courts must suppress the evidence obtained from the illegal wiretap. 18 U.S.C. 2515 ("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, hearing or other proceeding...if disclosure of that information would be in violation of this chapter.").

The Government here, in its applications, represented that the use of undercover officers, cooperating witnesses, controlled buys, confidential informants, physical surveillance, telephone and toll records, search warrants, arrests, and witness interviews were insufficient to achieve the goals of the investigation. To the contrary, the investigation at the time of the application was rich, varied and productive.

The traditional techniques employed here were many, and highly successful. In fact, the first wiretap application is rich in detail, belying the very "necessity" for phone call intercepts. Wiretap usage is intended for scenarios where traditional investigatory techniques cannot function, due to threats of violence, intimidation, lack of record keeping, etc... *See* S. Rep No. 90-1097 at 42-44 (1968) see U.S.C.C.A.N. 2112, 2159-2160. There was no evidence of the same here. Rather, the rich, varied and productive investigation did not need wiretaps to flourish.

Despite the successful investigation, the Government sought the shortcut of a wiretap. Agent Brown's Affidavit for the wiretaps squarely claims that cell site, GPS and live tracking data is *not possible*. He also states that if it were possible, it would have been *helpful* to the investigation. In his Affidavit he states:

> I have considered obtaining precise location information for TT1 and TT2 in an effort to monitor and study Dastinot and Victor's travel schedules. **This**

> **information could help identify stash locations and/or the locations of sources or supply**. However, I know based on my training and experience and conversations with other law enforcement officers that **Verizon Wireless does not make precise location available to law enforcement**. I could obtain cell-site location information for TT1 and TT2, but the range of error in this type of data prevents narrowing down a precise residence (especially in dense places like Boston and Lewiston).

Very clearly then, the Government acknowledged that the cell and GPS data would have been *helpful* to the goals of their investigation - thereby clearly meeting the necessity requirement. Agent Brown's claim was that the helpful information was *not available*, based on his training, experience and a call to Verizon Wireless (which Petitioner rebutted in his Motion by providing the Verizon manual explaining how law enforcement can acquire location data).

As a result, Petitioner proffered information to the lower courts to establish that the technology was, in fact, available. The information provided established that both cell site data and GPS devices allow the government to identify an individual's whereabouts with startling precision. *United States v. Maynard*, No. 08-3030 (D.C. Cir. Aug. 6, 2010), slip op. at 30. Investigators can use information from the cellular towers that process cell-phone calls to pinpoint caller's locations and track their movements over time. *United States v. Pineda-Moreno*, 617 F.3d 1120 (9th Cir. Aug. 12, 2010) (Kozinski, J., dissenting from rehearing *en banc*). Since this data is stored by cellular providers, agents can not only perform this tracking in real time, but also reconstruct the analysis after the fact. Use of cell site information "is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources." *State v. Earls*, 214 N.J. 564, 586, 70 A.3d 630, 642 (2013).

Petitioner explained to the lower courts that cellular telephones act with a radio connection. *Geolocation Privacy and Surveillance*: Hearing before the H.Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary, 113th Cong. 50 (2013) (testimony of University of Pennsylvania Professor Matthew Blaze) (cited hereafter as "Blaze Testimony"). The cell phone's service provider operates a network of base stations within its coverage area. *Id.* These base stations can include towers or sector antennas. *Id.* These base stations are limited by radio range and their spectrum capacity. *Id.* So, as demand for cellular services have risen, the service providers have reduced the geographic area each base station covers to account for capacity issues. *Id.*

These base stations now cover smaller and smaller geographic areas. *Id.* The number of cell sites have risen from 139,338 in 2002 to 301,779 in 2012. *See Commonwealth v. Augustine*, 4 N.E. 3d 846, 467 Mass. 230 (2014).

Professor Blaze observed:

> One of the trends is the use of small cell sites that cover very small geographic areas, such as an individual home or an individual office. These are sometimes called microcells or picocells or femtocells. Various service providers offer them. These may cover an area as small as this hearing room or our homes.
>
> Because of this increased density and because of this increased amount of usage, it's become more difficult to meaningfully distinguish between cell site location and other geolocation technologies, such as vehicle-based GPS and precise location technologies that are used for E911 services, particularly if we consider how revealing this information is about our daily lives.
>
> Unlike vehicle-based GPS surveillance, we carry our cellular telephones with us everywhere we go. We have them on at all times. We take advantage of data services that cause them to send and receive data without us being aware that it's occurring in many cases. And we can use them indoors and in private spaces, unlike GPS devices, which generally work only outdoors with a view to the satellite.

Agent Brown's assertions that "the range of error in this type of data (cell site data) prevents narrowing down a precise residence (especially in dense places like Boston and Lewiston)." To the contrary, the density of the population and its increased demand for cellular services makes the cell site data more precise. *Blaze testimony.*

In *Earls*, the New Jersey Supreme Court made findings that reflect these arguments. In determining whether the use of cellular location information required a warrant, the *Earls* Court noted that cell phones identify themselves with cell towers every seven seconds. *Earls supra* at 568. The *Earls* Court found that "Cell providers collect data from these contacts which allows carriers to locate cell phones on a real-time basis and to reconstruct a phone's movement from recorded data." *Id.* The Court noted that:

> Today, cell-phone providers can pinpoint the location of a person's cell phone with increasing accuracy. In some areas, carriers can locate cell-phone users within buildings, and even within individual floors and rooms within buildings.

Earls, citations omitted at 577. *See also Tracey v. State*, 152 So. 3d 504, 507 (Fla 2014) (cell phones can be accurately tracked in near real time).

Global Positioning Satellite (hereinafter "GPS") tracking works differently than cell site tracking. The GPS system syncs with satellites. This GPS satellite data can precisely locate a person or object within 10 meters of accuracy. *Earls Supra* at 578, citing *Blaze Testimony*.

It is equally worth noting that the phone at issue here used Verizon Wireless as a provider. All Verizon Wireless phones sold after December 31, 2003 contained a GPS chip that provides location information. *Earls Supra* at 580. GPS tracking was clearly available without the need for eavesdropping.

The proffer at the District Court level and at the First Circuit was more than adequate for Petitioner to at least get a hearing. Counsel requested a *Franks* hearing to discover Agent Brown's contrary information as to why the technology was not available. The *Franks* hearing request was denied. In a completely wrong-headed conclusion, the First Circuit holds:

> Other methods considered but left by the wayside included cell-site location data and vehicle tracking. Brown plausibly explained that the "range of error" of the cell-site data provided by Verizon Wireless prevented that data from being very useful, "especially in dense places like Boston and Lewiston." At any rate, the data would not be able to "narrow down a precise residence" in such areas. With respect to multi-unit buildings (common in Boston and Lewiston), targeting a particular building through location data would not serve to identify individual conspirators. More critically, neither the cell-site data nor vehicle tracking could reveal the purpose for the conspirator's

> movements, the identity of the persons with whom they were meeting, or the purposes of those meetings. To obtain this kind of intelligence, Brown believed that wiretapping was needed.

United States v. Gordon, 871 F.3d 35, 46 (1st Cir. 2017).

Unfortunately, the First Circuit decision entirely misses the point. Moreover, it is factually wrong. In fact, Agent Brown did swear in his Affidavit that tracking *would have been helpful* to the underlying objective of the investigation, which was to establish the source of supply. Further, the technology was available, and there was a more than sufficient proffer to establish the same, or to at least proceed to a *Franks* hearing on that issue.

The broader appeal of this case to SCOTUS relates to the standard of proof required to get a hearing on a Title III warrant. When such an extraordinary invasion of privacy, like wiretapping, is at stake, there must be a mechanism to challenge the necessity of the wiretapping. The proffer here was adequate, yet unconsidered.

This leaves defendants like Petitioner without any real mechanism to debate the wiretap. While the courts offer platitudes about protecting against the extraordinary invasion of a wiretap, Courts like the First Circuit close the courthouse doors. SCOTUS should grant the Petition for Certiorari here to explain the defendant's burden of production to get a testimonial hearing on a Title III wiretap case. Since the Petitioner was never given that opportunity, he was denied due process and a Petition for a Writ should be granted.

Dated this 11th day of December, 2017, at Portland, Maine.

Respectfully submitted,

Timothy E. Zerillo, Esq.
Counsel of Record for Petitioner
ZERILLO LAW FIRM, LLC
1250 Forest Avenue, Suite 3A
Portland, Maine 04103
tim@zerillolaw.com
207.228.1139

No. ____

In the
Supreme Court of the United States

Romelly Dastinot,
Petitioner

v.

United States of America,
Respondent

PROOF OF SERVICE

I, Timothy E. Zerillo, do swear or declare that on the below date, as required by Supreme Court Rule 29, I have served the enclosed PETITION FOR WRIT OF CERTIORARI on each party to the above proceeding or that party's counsel, and on every other person required to be served, by depositing an envelope containing the above documents in the United States mail properly addressed to each of them and with first-class postage prepaid, or by delivery to a third-party commercial carrier for delivery within 3 calendar days.

The names and addresses are as follows:

1. Clerk, Supreme Court of the United States, 1 First Street, N.E.,

Washington, D.C. 20543;

2. Solicitor General of the United States, Room 5614, Department of Justice, 950 Pennsylvania Avenue, N.W., Washington DC 20530-0001;

3. Renee M. Bunker, AUSA, District of Maine, 100 Middle Street, Sixth Floor, Portland, ME 04101;

4. Romelly Dastinot, Romelly Dastinot, 08543-036, Federal Correctional Complex, United States Penitentiary, P.O. Box 1033, Coleman, FL 33521-1033.

I declare under penalty of perjury that the foregoing is true and correct.

Dated this 11th day of December, 2017, at Portland, Maine.

Respectfully submitted,

Timothy E. Zerillo, Esq.
Counsel of Record for Petitioner
ZERILLO LAW FIRM, LLC
1250 Forest Avenue, Suite 3A
Portland, Maine 04103
tim@zerillolaw.com
207.228.1139

INDEX TO APPENDICES

Appendix A: *United States v. Gordon*, 871 F.3d 35 (1st Cir. 2017) and *United States v. Dastinot*, No. 16-1272 (1st Cir. 2017).

Appendix B: *United States v. Romelly Dastinot*, Order on Defendant Romelly Dastinot's Motion to Suppress, District of Maine, Judge Jon Levy.

Appendix A

United States v. Dastinot

United States Court of Appeals for the First Circuit

September 13, 2017, Decided

No. 16-1272

Reporter
2017 U.S. App. LEXIS 17708 *

UNITED STATES OF AMERICA, Appellee, v. ***ROMELLY DASTINOT***, Defendant, Appellant.

Notice: PLEASE REFER TO *FEDERAL RULES OF APPELLATE PROCEDURE RULE 32.1* GOVERNING THE CITATION TO UNPUBLISHED OPINIONS.

Prior History: **[*1]** APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MAINE. Hon. Jon D. Levy, U.S. District Judge.

*United States v. **Dastinot**, 2015 U.S. Dist. LEXIS 36013 (D. Me., Mar. 23, 2015)*

Counsel: Daphne H. Donahue, with whom Timothy E. Zerillo and Hallett, Zerillo & Whipple, P.A. were on brief, for appellant.

Renée M. Bunker, Assistant United States Attorney, with whom Richard W. Murphy, Acting United States Attorney, and Margaret D. McGaughey, Assistant United States Attorney, Appellate Chief, were on brief, for appellee.

Judges: Before Torruella, Selya and Kayatta, Circuit Judges.

Opinion by: SELYA

Opinion

SELYA, Circuit Judge. Following a protracted investigation of drug-trafficking in and around Lewiston, Maine, spearheaded by the federal Drug Enforcement Administration (DEA), a federal grand jury handed up an indictment naming defendant-appellant ***Romelly Dastinot*** and eleven codefendants. The indictment charged ***Dastinot*** with, inter alia, conspiracy to distribute and possess with intent to distribute controlled substances, see *21 U.S.C. §§ 841(a)(1), 846*, and conspiracy to commit money laundering, see *18 U.S.C. § 1956(a)(1)(B)(i)*. Some of the evidence against ***Dastinot*** and his coconspirators was gathered through court-authorized wiretaps, see id. *§§ 2510-2522*, and ***Dastinot*** moved to suppress the evidence gleaned through wiretapping. One of his codefendants, Dimitry **[*2]** Gordon, filed a similar motion.

The district court denied both ***Dastinot***'s motion to suppress and Gordon's motion to suppress. Thereafter, ***Dastinot*** entered a conditional guilty plea to the lead count of the indictment, see *Fed. R. Crim. P. 11(a)(2)*, reserving the right to challenge the district court's suppression ruling. Gordon, too, entered a conditional guilty plea. After the district court sentenced the two men, both of them filed timely notices of appeal.

We consolidated ***Dastinot***'s and Gordon's appeals and heard oral argument on July 26, 2017. We rejected Gordon's appeal by an opinion issued on September 8, 2017. See *United States v. Gordon, __ F.3d __, 2017 U.S. App. LEXIS 17423 (1st Cir. 2017)* [No. 15-2087]. We noted at that time that ***Dastinot***'s appeal would be decided separately. See id. at _ n.1 [slip op. at 2 n.1].

We now turn to ***Dastinot***'s appeal. It presents a narrower subset of the issues already considered and resolved in Gordon's appeal. No useful purpose would be served by repastinating soil already well-plowed. Accordingly, we deny ***Dastinot***'s appeal for substantially the reasons set forth in our earlier opinion. See id. at _ [slip op. at 16-20].

We need go no further. The judgment of the district court is summarily

Affirmed. See *1st Cir. R. 27.0(c)*.

End of Document

United States v. Gordon

United States Court of Appeals for the First Circuit

September 8, 2017, Decided

No. 15-2087

Reporter
871 F.3d 35 *; 2017 U.S. App. LEXIS 17423 **; 2017 WL 3947106

UNITED STATES OF AMERICA, Appellee, v. ***DIMITRY GORDON***, Defendant, Appellant.

Prior History: [**1] APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MAINE. Hon. Jon D. Levy, U.S. District Judge.

United States v. Gordon, 2015 U.S. Dist. LEXIS 36055 (D. Me., Mar. 23, 2015)

Disposition: Affirmed.

Case Summary

Overview

HOLDINGS: [1]-The DEA agent's affidavits set forth convincing reasons for tracking telephones by electronic serial number or International Mobile Equipment Identity number--drug traffickers change telephone numbers frequently in an attempt to avoid detection and, in the bargain, tend not to associate their names with telephone numbers--and the orders were specific in that they restricted interception to particular serial numbers; [2]-The wiretap applications were more than minimally adequate to justify the wiretap orders; [3]-The district court did not abuse its wide discretion in declining to hold a general evidentiary hearing to delve further into the minimization issue.

Outcome

Order affirmed.

Counsel: Edward S. MacColl, with whom Thompson, MacColl & Bass, LLC, P.A. was on brief, for appellant.

Renée M. Bunker, Assistant United States Attorney, with whom Richard W. Murphy, Acting United States Attorney, and Margaret D. McGaughey, Assistant United States Attorney, Appellate Chief, were on brief, for appellee.

Judges: Before Torruella, Selya and Kayatta, Circuit Judges.

Opinion by: SELYA

Opinion

[*40] SELYA, Circuit Judge. Defendant-appellant ***Dimitry Gordon*** strives to persuade us that the district court erred in denying his motion to suppress wiretap evidence and/or in refusing to hold one or more evidentiary hearings in connection therewith. We are not convinced and, therefore, we affirm the challenged orders (that is, the order denying the motion to suppress and the orders denying the two requests for evidentiary hearings).

I. BACKGROUND

Around September of 2012, a joint task force spearheaded by the federal Drug Enforcement Administration (DEA), and including state and local law enforcement officers, began investigating a drug-distribution ring centered in Lewiston, Maine. This probe led investigators [**2] to identify Romelly Dastinot and Jacques Victor as the likely leaders of the ring.[1] The task force came to believe that the two regularly pooled their resources to buy drugs in bulk quantities in Boston and transport them to Maine. Once the drugs arrived in Maine, the pair apparently peddled them through separate distribution channels.

In the course of its investigation, the task force obtained Dastinot's and Victor's telephone records. That trove of information yielded several text-message exchanges detailing drug transactions.

In addition, the task force implemented a gallimaufry of other investigative strategies. To cite one example, it executed controlled buys from both Dastinot and Victor. Some of the controlled buys implicated the appellant as a lower-level member of the conspiracy, who sold drugs (either oxycodone pills or crack cocaine) on Dastinot's behalf. To cite another example, the task force partnered with confidential sources and turncoat members of the drug ring.[2]

Despite its investigative efforts, the task force was unable to learn either the identity or specific location of the drug ring's suppliers. Nor was the task force able to get a handle on the drug ring's organizational [**3] structure. In hopes of catching bigger fish, the government submitted a series of wiretap applications to the district court between February and May of 2014, seeking to monitor a total of five telephones. Only three of the target telephones, known as TT1, TT2, and TT5, are relevant to this appeal (Dastinot used TT1 and TT5, while Victor used TT2). The appellant was identified as a target-subject of the wiretaps even though his own telephone was never tapped.

[*41] A DEA agent, Joey Brown, prepared supporting affidavits for the wiretap applications. All of these applications were approved by the district court and renewed as needed. See *18 U.S.C. § 2518(5)* (limiting wiretap authorization to thirty days). In Agent Brown's first affidavit (dated February 24, 2014), he spelled out investigative techniques that the task force had used up to that point. For instance, investigators had worked extensively with cooperating sources, executed controlled purchases, analyzed telephone data (obtained through pen registers, telephone toll records, historical text-message records, and trap-and-trace devices), conducted physical surveillance, examined public records, and used available subpoena powers (both administrative [**4] and grand jury).

The affidavit identified the objectives of the wiretap investigation as obtaining:

> a. The identity of the sources of supply for Dastinot and Victor, their locations, and the manner in which they acquire[d] and transport[ed] drugs to Maine and elsewhere for distribution;
>
> b. The precise roles of the Target Subjects [including the appellant] in this drug conspiracy and the methods being utilized by the Target Subjects to distribute illegal drugs;
>
> c. The identity of all persons receiving drugs from Dastinot and Victor for further distribution;
>
> d. Identification of the site(s) being utilized for the storage and concealment of illegal drugs;
>
> e. The existence, location and disposition of proceeds (including currency, real estate, motor vehicles, and personal property) derived from the Target Subjects' involvement in drug distribution;
>
> f. The precise date(s), time(s) and location(s) of shipments of illegal drugs to/from this

[1] This appeal was consolidated for oral argument with an appeal taken by Dastinot, which raised a narrower subset of the issues advanced by the appellant. Dastinot's appeal, No. 16-1272, will be resolved by means of a separate opinion.

[2] The record reflects that the task force's investigation involved no fewer than four confidential sources and that some seven members of the drug ring cooperated with the government at various stages of the investigation. For ease in exposition, we do not distinguish between the confidential sources and the turncoats but, rather, refer to all of them as cooperating sources.

organization and the manner of delivery.

The affidavit revealed that the task force had learned very little about the drug ring's sources of supply, finances, organizational structure, or the roles of its members.

According to Brown, the task force had mulled a number of additional investigative [**5] strategies, but had rejected them as either too risky or too unlikely to yield worthwhile results. In this vein, the task force had decided against conducting more aggressive physical surveillance, attempting to install cameras in selected public locations, obtaining search warrants for known drug-distribution venues, collecting target-subjects' trash, widening the use of grand jury interviews, or attempting to introduce undercover agents into the ring. Brown added that he did not believe that further controlled purchases would yield more information about the drug ring. Nor did he think that either approaching or arresting the target-subjects and asking them to reveal their sources of supply was apt to prove fruitful.

Brown also noted that the task force had considered obtaining cell-site location information for at least some of the telephones. This option was rejected because "the range of error in this type of data prevents narrowing down a precise residence (especially in dense places like Boston and Lewiston)." What is more, the location data are often several minutes behind the actual location of the telephone. And location data alone, he reasoned, whether from cell-site records [**6] or from vehicle trackers, would not reveal the identity of the person with whom a target-subject meets or the nature of the encounter.

Brown concluded that wiretapping was "the only available technique that ha[d] a reasonable likelihood of securing the evidence necessary to accomplish the goals of th[e] investigation." His affidavit chronicled [*42] minimization procedures that would be instituted if the wiretaps were approved. At the outset, the monitors (the persons intercepting calls) would be provided with a minimization memorandum, the wiretap applications, and the authorizing orders. In pertinent part, the memorandum instructed that monitors should stop listening to conversations that did not relate to the criminal enterprise (though they could periodically check on seemingly innocuous discussions to see if the conversation had shifted). Each monitor would sign a form indicating that he had read the documents.

After the district court granted the first of the wiretap applications, the task force set up a wire room to serve as a central location for intercepting and monitoring calls. The room was staffed from 8:00 a.m. to midnight, and any calls not monitored by staff in real time were not recorded. [**7] Through the duration of the wiretaps, the authorities intercepted approximately 23,000 completed calls and text messages, many of which were in Haitian Creole (the language of choice for members of the drug ring). Along the way, the government compiled and submitted periodic statistical summaries to the district court.

Armed with, inter alia, the fruits of the wiretapping, a federal grand jury sitting in the District of Maine indicted the appellant and eleven codefendants. The indictment charged the appellant with conspiracy to distribute and possess with intent to distribute controlled substances, see *21 U.S.C. §§ 841(a)(1), 846*, and conspiracy to commit money laundering, see *18 U.S.C. § 1956(a)(1)(B)(i)*.

In due course, the appellant moved to suppress the evidence obtained through the wiretaps and requested two kinds of evidentiary hearings. First, he requested a general evidentiary hearing as to the adequacy of the government's minimization procedures. Second, he requested a Franks hearing on the ground that Brown's affidavits in support of the wiretap applications included false statements. See *Franks v. Delaware, 438 U.S. 154, 155-56, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*.

The district court heard arguments on these motions on January 28, 2015, but reserved decision. It later ordered the government to submit additional [**8] information regarding the statistical makeup of the intercepted conversations. In response, the government submitted Brown's supplemental affidavit dated February 13, 2015, which clarified and corrected the double-counting of some intercepted calls and reported that 14% of the calls lasting more than two minutes had been minimized in some way.

After further briefing, the district court denied not only the motion to suppress but also the twin requests for evidentiary hearings. The appellant thereafter entered a conditional guilty plea to the drug conspiracy count, see Fed. R. Crim. P. 11(a)(2), preserving his right to appeal the denial of both his motion to suppress and his related requests for evidentiary hearings. The district court accepted the conditional plea and subsequently sentenced the appellant to a 28-month term of immurement. At the same time, the court dismissed the money laundering charge. This timely appeal followed.

II. THE MOTION TO SUPPRESS

Insisting that his motion to suppress the wiretap evidence should have been granted, the appellant, ably represented, attacks the wiretap orders on multiple fronts. We start with his assertion that the orders were insufficiently particular. We next proceed [**9] to his claims that wiretapping was unnecessary and that, in all events, the government failed adequately to minimize [*43] its intrusion into the target-subjects' privacy rights.

Familiar standards of review guide our analysis. When assaying a district court's ruling on a motion to suppress wiretap evidence, we review its factual findings for clear error and its legal conclusions de novo. See *United States v. Lyons, 740 F.3d 702, 720-21 (1st Cir. 2014)*. The key question is whether the wiretap application and its supporting affidavits were "minimally adequate" to support the issuance of the wiretap order. *United States v. Santana, 342 F.3d 60, 65 (1st Cir. 2003)* (quoting *United States v. Villarman-Oviedo, 325 F.3d 1, 9 (1st Cir. 2003))*.

A. Particularity.

With the passage of *Title III of the Omnibus Crime Control and Safe Streets Act of 1968* (Title III), see *18 U.S.C. §§ 2510-2522*, Congress authorized wiretapping as needed to allow effective investigation of criminal activities while at the same time ensuring meaningful judicial supervision and requiring specific procedures to safeguard privacy rights. See *United States v. Rodrigues, 850 F.3d 1, 6 (1st Cir. 2017)*; see also *Gelbard v. United States, 408 U.S. 41, 48, 92 S. Ct. 2357, 33 L. Ed. 2d 179 (1972)* (describing Title III as "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized" (quoting S. Rep. No. 1097, at 66 (1968), [**10] as reprinted in 1968 U.S.C.C.A.N. 2112, 2153)). Among other things, Title III provides for the suppression of wiretap evidence on the ground that "the order of authorization or approval under which it was intercepted [was] insufficient on its face." *18 U.S.C. § 2518(10)(a)(ii)*.

Here, the appellant complains that the wiretap orders failed to satisfy Title III's particularity requirements in three respects. He submits that they did not include "a particular description of the type of communication sought to be intercepted," id. *§ 2518(4)(c)*; that they did not include "a statement of the particular offense to which [the communication] relates," id.; and that they did not include a sufficient description of "the agency authorized to intercept the communications," id. *§ 2518(4)(d)*. We examine these plaints sequentially.

The appellant's remonstrance regarding the type of communication sought focuses on the fact that the orders were not limited to existing telephone numbers but, rather, extended to numbers "subsequently assigned to or used by the instruments bearing the same" electronic serial number (ESN) or International Mobile Equipment Identity (IMEI) number as the original tapped telephone. For example, if Dastinot changed the ten-digit [**11] telephone number assigned to a particular cellular telephone, the order would automatically cover the new ten-digit number, and the task force would not have to seek a further order every time that number changed. Relatedly, the orders authorized the interception of "background conversations intercepted in the vicinity of the target telephones while the telephones are off the hook or otherwise in use." In the appellant's view, extending the authorizations in this manner rendered them impermissibly broad.

These arguments comprise more cry than wool. Brown's affidavits set forth convincing reasons for tracking telephones by ESN or IMEI number: drug traffickers change telephone numbers frequently in an attempt to avoid detection and, in the bargain, tend not to associate their names with telephone numbers. To cinch the matter, the orders were specific in that they restricted interception to particular serial numbers. We can think of no good reason [*44] why Title III's particularity requirement should be read as limiting a wiretap to a specific telephone number rather than a specific ESN or IMEI number reasonably believed to be used by the target. Cf. *United States v. Oliva, 705 F.3d 390, 400-01 (9th Cir. 2012)* (holding, with respect to *18 U.S.C. § 2518(4)(b)*, that order [**12] authorizing wiretap by reference to specific serial number was sufficiently descriptive to satisfy Title III's mandate that order describe "the nature and location of the communications facilities").

The appellant's argument regarding background conversations overheard through an off-the-hook telephone is equally unavailing. This language is standard fare in wiretap applications, see *id. at 397 n.7*, and its inclusion does not make the wiretap orders impermissibly broad. After all, describing potential types of communications to be intercepted appears fully consistent with Title III's directive to define the sought-after communications with particularity. And, finally, it is doubtful whether Title III even applies to background conversations. Cf. *United States v. Couser, 732 F.2d 1207, 1210 (4th Cir. 1984)* (questioning whether "plain view" doctrine creates an exception to Title III requirements for background conversations). See generally *United States v. Williams, 827 F.3d 1134, 1153 (D.C. Cir. 2016)* (assuming, arguendo, that overheard conversations implicate Title III's requirement to name target individuals but noting lack of authority for the proposition), cert. denied, *137 S. Ct. 706, 196 L. Ed. 2d 579 (2017)*.

Next, the appellant posits that the wiretap orders are invalid for failing to identify "the particular offense to which" the sought-after communications [**13] relate. *18 U.S.C. § 2518(4)(c)*. The critical fault, he says, is that the orders simply cite statutory sections without providing any broader context. But the appellant sets the bar too high: the enumeration of specific criminal statutes itself serves to identify particular offenses and, thus, satisfies this facet of the particularity requirement. See *United States v. Spillone, 879 F.2d 514, 517-18 (9th Cir. 1989)*.

The overall structure of the statute buttresses this view: an earlier subsection — *section 2518(3)(a)* — uses the term "particular offense" in reference to "a particular offense enumerated in *section 2516*." *Section 2516*, in turn, lists criminal offenses, some by statutory citation and others by even broader descriptions, such as "the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States." *18 U.S.C. § 2516(1)(e)*. In light of this provision, abecedarian principles of statutory construction lead to the conclusion that the "particular offense" requirement in *section 2518(4)(c)* is satisfied when a wiretap order simply lists the charging statute. See *United States v. Nippon Paper Indus. Co., 109 F.3d 1, 4-5 (1st Cir. 1997)* ("It is a fundamental interpretive principle that identical words or terms used in different parts of the same act are intended to have the same meaning. This principle **[**14]** . . . operates not only when particular phrases appear in different sections of the same act, but also when they appear in different paragraphs or sentences of a single section." (citations omitted)).

The appellant has one last shot in his particularity sling. Title III requires a wiretap order to specify "the agency authorized to intercept the communications." 18 U.S.C. § 2518(4)(d). The appellant assails the description of the authorized agency contained in the wiretap orders as virtually "unbounded."

[*45] By their terms, the orders authorize "special agents of the United States Drug Enforcement Administration and other investigative and law enforcement officers, and civilian monitors operating under a contract with the Government" to conduct the wiretapping. The appellant correctly notes the looseness of this language: phrases such as "other investigative and law enforcement officers" are not moored to any particular agency. Even so, the orders must be read in the context of Brown's affidavits and the wiretap applications, and those documents leave little doubt that the DEA was the agency involved.

For one thing, Brown's affidavits made pellucid the DEA's pervasive involvement in the case. For another thing, **[**15]** the wiretap orders specified that the wiretapping would "be executed at a listening post maintained at the United States Drug Enforcement Administration Resident Office, in Portland, Maine." They also described a cooperative effort between Verizon Wireless and the DEA. Given a practical, commonsense reading, we hold that the wiretap orders were sufficiently particular in describing the DEA as "the agency authorized" to conduct the wiretapping.

Even if we assume, for argument's sake, that inclusion of the loose language challenged by the appellant departed from the statutory "agency identification" requirement, the violation would not demand suppression. Not every blemish in an order of authorization demands suppression: such a remedy is required only when there is a failure to satisfy "statutory requirements that directly and substantially implement the congressional intention to limit" wiretaps. United States v. Giordano, 416 U.S. 505, 527, 94 S. Ct. 1820, 40 L. Ed. 2d 341 (1974); see United States v. Cunningham, 113 F.3d 289, 293-94 (1st Cir. 1997). This principle recognizes that suppression is "strong medicine," which should not be profligately dispensed. United States v. Adams, 740 F.3d 40, 43 (1st Cir. 2014).

The putative violation of the "agency identification" requirement is more a matter of form than of substance. That lapse, though regrettable, cannot plausibly be said to directly **[**16]** or substantially weaken the protections that Congress sought to craft in connection with wiretapping. See United States v. López, 300 F.3d 46, 55-56 (1st Cir. 2002) (holding that "government must disclose, as a part of its application for a wiretap warrant, any intention to utilize the services of civilian monitors in the execution of the warrant" but concluding that omission did not require suppression). It follows that suppression would be manifestly disproportionate to the putative violation and, thus, should not be required.

That ends this aspect of the matter. We reject the appellant's importunings and hold that the wiretap orders were not so lacking in particularity as to demand suppression.

B. Necessity.

In investigating criminal activity, "wiretapping is to be distinctly the exception — not the rule." United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987). To balance "privacy and the rights of the individual," Title III requires the government to establish necessity as a prerequisite for obtaining a wiretap order. Id. Seizing on this requirement, the appellant asserts that the government failed to establish that it was necessary to resort to wiretapping.

In the Title III lexicon, necessity is not an absolute. Rather, it must be viewed through the lens of what is pragmatic and achievable **[**17]** in the real world. See *United States v. Uribe, 890 F.2d 554, 556 [*46] (1st Cir. 1989)* (explaining that "Title III demands a practical, commonsense approach to exploration of investigatory avenues"). It is a relative term — and it is context-specific. To demonstrate necessity, a wiretap application must include "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." *18 U.S.C. § 2518(1)(c)*. Such a showing "should demonstrate that the government has made a reasonable, good faith effort to run the gamut of normal investigative procedures before resorting to means so intrusive as electronic interception of phone calls." *United States v. Martinez, 452 F.3d 1, 4 (1st Cir. 2006)* (quoting *Villarman-Oviedo, 325 F.3d at 9*).

This does not mean, though, that the government is "required to show that other investigatory methods have been completely unsuccessful." *United States v. Rivera-Rosario, 300 F.3d 1, 19 (1st Cir. 2002)*. Nor does it mean that "the government [is] forced to run outlandish risks or to exhaust every conceivable alternative before resorting to electronic surveillance." Id.; accord *Santana, 342 F.3d at 65*.

On appeal, our task is not to undertake a de novo determination of necessity as if we were deciding whether to issue the wiretap order. See *United States v. Ashley, 876 F.2d 1069, 1074 (1st Cir. 1989)*; accord *Rodrigues, 850 F.3d at 9*. We need only "decide if the facts set **[**18]** forth in the application were minimally adequate to support the determination that was made." *Ashley, 876 F.2d at 1074* (quoting *United States v. Scibelli, 549 F.2d 222, 226 (1st Cir. 1977)*). In evaluating whether the government has crossed this threshold, we have not hesitated to uphold wiretap orders based on an agent's plausible, good faith "assert[ion of] a well-founded belief that the techniques already employed during the course of the investigation had failed to establish the identity of conspirators, sources of drug supply, or the location of drug proceeds." *Rodrigues, 850 F.3d at 10* (collecting cases). As we explain below, that is exactly the type of assertion that the government proffered here.

Brown's affidavits related that it was not until early 2014 — approximately a year and a half into the investigation — that the government turned to wiretaps. At that point, the task force already had employed a myriad of investigative techniques, including the use of confidential sources, physical surveillance, controlled buys, analysis of telephone data and public records, and the issuance of subpoenas (both administrative subpoenas and grand jury subpoenas). Extensive use of these tools had left the agents in the dark about important matters such as the drug ring's sources of supply, its **[**19]** organizational structure, and its finances. By the same token, Brown spelled out plausible reasons for not employing certain other strategies. The task force did not want to attempt more intensive use of undercover agents or cooperating sources for fear of arousing suspicion.[3] For much the same reasons, the task force did not recommend either more aggressive physical surveillance or trying to install cameras. Further surveillance of public spaces would be ineffectual, Brown reasoned, because the vast majority of this drug ring's crimes occurred indoors.

To be sure, the task force had considered simply revealing its evidence, at least in part, to selected coconspirators and attempting **[*47]** to elicit their cooperation. This tactic was not pursued because the task force reasonably concluded that the possibilities of success were slim and the risks of

[3] The maxim "once bitten, twice shy" was in play: Brown was concerned that at least one confidential source already had been outed because the source had been sold fake (or extremely low-quality) heroin in executing a controlled buy.

failure were great.

Other methods considered but left by the wayside included cell-site location data and vehicle tracking. Brown plausibly explained that the "range of error" of the cell-site data provided by Verizon Wireless prevented that data from being very useful, "especially in dense places like Boston and Lewiston." At any rate, the data [**20] would not be able to "narrow[] down a precise residence" in such areas. With respect to multi-unit buildings (common in Boston and Lewiston), targeting a particular building through location data would not serve to identify individual conspirators. More critically, neither the cell-site data nor vehicle tracking could reveal the purpose for the conspirator's movements, the identity of the persons with whom they were meeting, or the purposes of those meetings. To obtain this kind of intelligence, Brown believed that wiretapping was needed.

The short of it is that Brown's affidavits, read as a whole, show that the task force carried out a long-lasting, wide-ranging, good-faith investigation that ran the gamut of standard investigative techniques. Those affidavits reflect a careful and rational balancing of the utility of various investigatory tools against the possibility of prematurely alerting the drug ring to the probe. The foundation laid in Brown's affidavits substantiates a plausible judgment that the investigation had reached a point at which wiretapping was reasonably necessary. We conclude, therefore, that the wiretap applications were more than minimally adequate to justify [**21] the wiretap orders. It follows that the appellant's necessity challenge fails.

C. Minimization.

Title III warns monitors to minimize irrelevant calls. See *18 U.S.C. § 2518(5)* (declaring that monitoring must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception"); see also *Scott v. United States, 436 U.S. 128, 140, 98 S. Ct. 1717, 56 L. Ed. 2d 168 (1978)* (explaining that Title III "instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of [irrelevant] conversations"). Consistent with this admonition, the wiretap orders directed the monitors to stop listening and/or recording when it became apparent that a conversation was not related to the criminal investigation. The minimization memorandum distributed to the monitors contained a similar warning. Even so, the monitors were permitted to check periodically on any given conversation to ascertain whether the discussion had shifted. The appellant insists that the government failed to comply with these requirements.

Blanket suppression of wiretap evidence is a "drastic" remedy, which should be reserved for the most "egregious" cases. *Hoffman, 832 F.2d at 1309*. A minimization violation often can be cured through a less draconian remedy: suppression of only those [**22] calls that the court determines should have been minimized. See id. Here, however, the appellant has not identified even a single call that he contends should have been minimized, but was not.[4] Thus, the relevant question reduces to whether the government's handling [*48] of its minimization responsibilities was so egregious as to support a blanket exclusion of the evidence obtained through wiretapping.

As a general matter, whether the government fails adequately to minimize intercepted conversations "depend[s] on the facts and circumstances of each case." *Scott, 436 U.S. at 140*. In evaluating the facts and circumstances of a specific case and the government's fealty to Title III's minimization requirements, a reviewing court must "look at several factors, including: 1) the nature and complexity of the suspected crimes; 2) the

[4] Indeed, the appellant has not identified even a single failure to minimize that prejudiced his rights. The absence of any such prejudice may, in itself, warrant the denial of his motion to suppress. See *López, 300 F.3d at 58* (upholding denial of suppression where defendant was not prejudiced by two intercepted non-pertinent calls).

thoroughness of the government's precautions to bring about minimization; and 3) the degree of judicial supervision over the surveillance process." López, 300 F.3d at 57.

In this instance, the first two factors weigh heavily in the government's favor. The sprawling operations of the drug ring and the complexity of the suspected crimes are manifest. In cases like this one, involving drug conspiracies of indeterminate [**23] proportions, "the need to allow latitude to eavesdroppers is close to its zenith." Hoffman, 832 F.2d at 1308.

To add to the complexity, the appellant and his confederates frequently spoke in Haitian Creole and employed code names on many occasions. The use of "codes and specialized jargon" furnish an added reason for affording monitors leeway because, in such cases, more context is needed to determine whether a conversation is related to the suspected crimes. Uribe, 890 F.2d at 557. The use of a foreign language itself supplies an extra layer of complexity. Cf. United States v. David, 940 F.2d 722, 730 (1st Cir. 1991) (explaining that when intercepted communications are in a foreign language and a real-time translator is not available, minimization may be accomplished as soon as practicable after the fact).

Importantly, the scope of the conspiracy was unknown at the time that the wiretaps were authorized. Indeed, an animating purpose behind the wiretap applications was to flesh out the structure of the organization and to identify the drug ring's sources of supply. These uncertainties also counsel in favor of granting wider latitude to the monitors. See, e.g., Hoffman, 832 F.2d at 1308 (allowing broad latitude when "investigation is focused largely on blueprinting the shape of the conspiratorial wheel and identifying [**24] the spokes radiating from its hub").

Here, moreover, the thoroughness of the government's precautions to bring about minimization is unquestioned. The record reflects that the government established a regime of adequate precautions designed to ensure that monitors were appropriately minimizing irrelevant conversations. All monitors had to confirm in writing that they had read the wiretap applications and supporting affidavits, the wiretap orders, and an instructional memorandum detailing proper minimization procedures. These documents were posted in the monitors' workplace for easy reference. Prosecutors also met with government agents to brief them on minimization standards.

The third factor is not quite as clear-cut; in the end, though, we think that the record indicates sufficient judicial supervision. See Uribe, 890 F.2d at 558. To begin, the court took care, in crafting the wiretap orders, to detail the minimization procedures already discussed. In addition, the government was required to submit statistical reports to the court on an ongoing basis.

It is the contents of these statistical reports that bring us to the crux of the [*49] appellant's minimization argument. When the appellant questioned the accuracy [**25] of some of the proffered numbers in arguing for suppression in the court below — contending, for example, that the reports listed as minimized calls that were not monitored and text messages that were not minimized — the district court ordered the government to submit additional explanations and more detailed data.

Before us, the appellant focuses on the percentage of non-pertinent calls that were not minimized in any way (98%, according to his calculations). Such percentages, though, tell us very little because many calls presumably end before the listener can determine their pertinence. Courts therefore tend to look at the relative percentage of calls minimized out of those calls lasting more than two minutes. See, e.g., United States v. De La Cruz Suarez, 601 F.3d 1202, 1215 (11th Cir. 2010); United States v. Yarbrough, 527 F.3d 1092, 1098 (10th Cir. 2008); United States v. Rivera, 527 F.3d 891, 905 (9th Cir. 2008); United States v. Dumes, 313 F.3d 372, 380

(7th Cir. 2002). Here, the government's data show that there were 1616 such calls, out of which 667 were determined to be not pertinent; 229 calls were minimized, likely meaning that over two-thirds of non-pertinent calls in excess of two minutes were not minimized. Although the fact that over 200 calls were minimized shows that there were real minimization efforts undertaken, the percentage of non-pertinent calls not minimized would seem to warrant some explanation.

The record **[**26]** points to such an explanation — at least enough of an explanation for us to find that the district court's ruling was not unreasonable and, thus, to justify upholding it. As Brown noted, many calls were in Haitian Creole and/or coded parlance, requiring either the use of translators or other assistants. It is eminently reasonable to conclude that determining the lack of pertinence of such calls would take much longer than usual.

Tellingly, there is no evidence of a slew of examples of calls that plainly should have been minimized in less than two minutes, but were not. Through we do not suggest that defense counsel need have reviewed hundreds of calls, we make the more limited point that if the minimization process had not been an "honest effort," *United States v. Charles, 213 F.3d 10, 22 (1st Cir. 2000)*, it should have been easy to find quite a few examples of non-minimized calls that obviously should have been minimized. Nor is there any other sign of either a less-than-serious effort on the part of the government to comply or a less-than-serious degree of supervision by the district court such as would lead us to conclude that the court abused its considerable discretion. Consequently, we decline the appellant's invitation to hold that **[**27]** the failure to minimize more irrelevant calls caused a "taint upon the investigation as a whole." *Hoffman, 832 F.2d at 1307*.

Although we uphold the district court's ruling that suppression was not required due to minimization deficiencies, we note that the appellant was at a disadvantage in manipulating the wiretap data. The government produced the logs for more than 20,000 telephone calls and text messages in the form of 10,000-plus pages in portable document format (PDF). Converting the 10,000 pages of PDFs into a workable spreadsheet would require inordinate time, effort, and resources. The government had available to it, and most likely should have produced the data in, a more serviceable format.[5] The appellant, though, merely **[*50]** mentioned the government's failure to provide the material in an electronically sortable format in his motion to suppress; he did not identify this failure either as a ground for his motion or as a basis for a continuance. Nor did he raise any issue concerning the government's failure to produce materials in an electronically sortable format in his briefs on appeal. Consequently, we do not pursue this point. See *United States v. Iwuala, 789 F.3d 1, 7 (1st Cir. 2015)* (explaining that arguments not made in opening appellate brief are deemed **[**28]** waived), cert. denied, *136 S. Ct. 913, 193 L. Ed. 2d 803 (2016)*; *United States v. Slade, 980 F.2d 27, 31 (1st Cir. 1992)* (explaining that arguments not made in the district court are deemed waived).

III. THE EVIDENTIARY HEARING REQUESTS

We end our journey by examining the appellant's twin requests for evidentiary hearings — his request for a general evidentiary hearing on his failure-to-minimize argument, and a Franks hearing to appraise what he alleges to be false statements in Brown's affidavits. We discuss these hearing

---

[5] The record discloses that the government was able to run reports, sort, and otherwise manipulate the data using a program called VoiceBox. When queried at oral argument in this court, the government offered no explanation as to why it could not have produced for the appellant a spreadsheet embodying the same functionality as it enjoyed by means of the VoiceBox program. But cf. *United States v. Briggs, No. 10-CR-184S, 2012 U.S. Dist. LEXIS 164634, 2012 WL 5866574, at *2 (W.D.N.Y. Nov. 16, 2012)* (discussing limitations of VoiceBox and finding disclosure obligations satisfied with searchable PDFs rather than Excel-style spreadsheets because of data corruption concerns).

requests separately.

A. **General Evidentiary Hearing.**

No criminal defendant has "a presumptive right to [a general] evidentiary hearing on a motion to suppress." *United States v. D'Andrea, 648 F.3d 1, 5 (1st Cir. 2011)*. Rather, a general evidentiary hearing is only warranted if the party seeking suppression "makes a sufficient threshold showing that material facts are in doubt or dispute, and that such facts cannot reliably be resolved on a paper record." Id. (quoting *United States v. Staula, 80 F.3d 596, 603 (1st Cir. 1996)*). When all is said and done, "the defendant must show that there are factual disputes which, if resolved in his favor, would entitle him to the requested relief." *Staula, 80 F.3d at 603*. "The district court has considerable discretion in determining the need for, and the utility of, evidentiary hearings, and we will reverse the court's denial of an evidentiary hearing **[**29]** in respect to a motion in a criminal case only for manifest abuse of that discretion." Id.

In the case at hand, the appellant alleges that he presented a colorable, fact-intensive claim as to whether the government appropriately minimized his communications. That claim, he says, could only be resolved after an evidentiary hearing. We do not agree.

The district court was adequately apprised of the facts relating to minimization through the parties' filings, particularly after the government furnished supplemental information (at the court's direction) explaining its minimization tallies more thoroughly. The Supreme Court has noted the "necessarily ad hoc nature" of minimization determinations and has emphasized the need for flexibility in judicial oversight. *Scott, 436 U.S. at 139*. In the end, whether the government has engaged in adequate minimization is quintessentially a judgment call, and the court below had sufficient facts before it to make an informed decision in that regard. We conclude, therefore, that the district court did not abuse its wide discretion in **[*51]** declining to hold a general evidentiary hearing to delve further into the minimization issue.

B. **Franks Hearing.**

This leaves the appellant's request **[**30]** for a Franks hearing. To obtain a Franks hearing, a defendant must make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and [that] the allegedly false statement is necessary to the finding of probable cause." *438 U.S. at 155-56*. "In considering a district court's decision to deny a Franks hearing, we review factual determinations for clear error and the probable cause determination de novo." *United States v. Arias, 848 F.3d 504, 511 (1st Cir. 2017)*; see *United States v. Tanguay, 787 F.3d 44, 48-50 (1st Cir. 2015)* (reviewing de novo district court's probable cause analysis in connection with Franks hearing).

Here, the appellant alleges that Brown's affidavits contained false statements with respect to the existence of probable cause vis-à-vis money laundering, the efficacy of cell-site location data, and the likelihood that wiretapping would allow the task force to identify assets of the conspiracy and the precise roles of the individuals involved.

The statements to which the appellant adverts, though, are as much matters of opinion as matters of fact, and the appellant has made no convincing showing that Brown knew the statements were false, yet nonetheless included them in his affidavits. **[**31]**

We add, moreover, that all of the challenged statements appear to have had a reasonable basis in fact. With respect to the money-laundering statements, Brown did not need to have probable cause to believe that the appellant himself was engaging in money laundering. He only needed probable cause to believe that some members of the conspiracy were so engaged. The record adequately evinces that Brown had probable cause to believe that some members of the drug ring were engaging in money laundering; after all, Brown's affidavits presented a detailed showing of repeated buying and selling of drugs, which gave rise to a commonsense inference that the members of the drug ring must have been participating in some kind of scheme to protect and launder their profits.

As to the cell-site location data, the appellant did not proffer enough facts to demonstrate that Brown's statements were false, much less knowingly so. While the appellant's brief relies heavily on a document submitted to the district court (a Verizon Wireless publication for law enforcement officers), the district court took this document into account, see *United States v. Dastinot*, No. 2:14-CR-69, 2015 U.S. Dist. LEXIS 36013, 2015 WL 1292611, at *6 (D. Me. Mar. 23, 2015), concluding (reasonably, we think) **[**32]** that it did not contradict Brown's statements that the location data were neither sufficiently accurate nor sufficiently particularized to enable agents to pinpoint a specific residence, especially in densely populated areas.

We need not linger long over the appellant's allegations that Brown either dissembled or made statements in reckless disregard of the truth when he stated that the task force hoped to learn through the wiretaps about the precise roles of conspirators and the whereabouts of the drug ring's assets. In support, the appellant suggests that these goals were too broad to be reasonably achievable. This contention does not withstand scrutiny.

The goals of identifying a drug conspiracy's organizational structure (at least in rough terms) and locating its assets are **[*52]** achievable in some measurable sense. Intercepted conversations might well give clear indications of the drug ring's hierarchy, and investigators — following up on information gleaned from intercepts — might well locate cash, inventory, real estate holdings, or other items of value. To say that these statements of aspirational goals were either intentionally false or made in reckless disregard of the truth is simply **[**33]** a bridge too far. We have approved similarly broad goals in other wiretap cases, see, e.g., *Martinez*, 452 F.3d at 6; *Villarman-Oviedo*, 325 F.3d at 10, and Brown could not be faulted for the description of goals contained in his affidavits.

To say more would be to paint the lily. We hold, without serious question, that the district court did not commit reversible error in refusing to convene either a general evidentiary hearing or a Franks hearing.

IV. CONCLUSION

We need go no further. For the reasons elucidated above, the orders of the district court are

Affirmed.

End of Document

Appendix B

UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**Crim. No. 2:14-cr-69-JDL-1**
ROMELLY DASTINOT,	)	
	)	
Defendant.	)	

ORDER ON DEFENDANT ROMELLY DASTINOT'S MOTION TO SUPPRESS

Romelly Dastinot moves to suppress wiretap evidence as violating the requirements of the Federal Wiretap Act, 18 U.S.C.A. §§ 2510-2522. ECF No. 451. Dastinot also requests a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). *Id.* For the reasons discussed below, Dastinot's motion is denied.

I. FACTUAL BACKGROUND

On February 24, 2014, the Government submitted an application to this Court seeking authorization to intercept wire and electronic communications occurring over the cellular telephone numbers (207) 330-5654 ("Target Telephone #1" or "TT1") and (207) 713-0380 ("Target Telephone #2" or "TT2"). ECF No. 567 at 1. Accompanying the application was an 88-page supporting affidavit submitted by Task Force Agent ("Agent") Joey Brown (the "February 24 Affidavit"). *Id.* The Court granted the application, and issued an order and an amended order authorizing interceptions of wire and electronic communications occurring over both TT1 and TT2, respectively. Interception of TT1 began on February 26, 2014. *Id.* at 1-2. Interception of TT2 began on February 25. *Id.* at 2.

On March 25, 2014, the Government submitted an application to this Court seeking authorization to continue intercepting wire and electronic communications occurring over TT1 and TT2 for an additional 30 days. *Id.* The application was accompanied by Agent Brown's 83-page supporting affidavit (the "March 25 Affidavit"). *Id.* The Court granted the application and issued orders authorizing interceptions of wire and electronic communications occurring over both numbers. Interceptions pursuant to these orders began on March 25, 2014. *Id.*

On April 24, 2014, the Government again submitted an application to this Court seeking renewed authorization to continue intercepting wire and electronic communications occurring over TT1, plus authorization to intercept wire and electronic communications occurring over the cellular telephone assigned telephone number (857) 236-2924 ("Target Telephone #4" or "TT4"). *Id.* Agent Brown again submitted a supporting affidavit (the "April 24 Affidavit"). *Id.* The Court granted the application and issued orders authorizing interceptions of wire and electronic communications occurring over TT1 and TT4. Interceptions pursuant to these orders began on April 24, 2014. *Id.* at 3.

The Government submitted its final application on May 1, 2014, seeking authorization to intercept wire and electronic communications occurring over the cellular telephone number (207) 240-3478 ("Target Telephone #5" or "TT5"). *Id.* The application was accompanied by a 69-page supporting affidavit from Agent Brown (the "May 1 Affidavit"). *Id.* The Court granted the application and issued an order authorizing interceptions of wire and electronic communications occurring over TT5. Interceptions pursuant to this authorization began on May 1, 2014. *Id.*

On December 9, 2014, a federal grand jury returned a Second Superseding Indictment against Dastinot and nine co-defendants. ECF No. 531. Count One of the Second Superseding Indictment ("Count One") charges that Dastinot conspired with at least five named co-defendants to distribute and possess with intent to distribute various controlled substances, including heroin, cocaine, and oxycodone, all in violation of 21 U.S.C.A. §§ 841(a)(1) and 846. ECF No. 531 at 1-2. Count One further alleges that the conspiracy took place in the District of Maine over a period of approximately 24 months, i.e., "not later than early 2012, and continuing until May 2014." *Id.* at 1.

Count Five of the Second Superseding Indictment ("Count Five") charges that Dastinot and one other co-defendant possessed with intent to distribute oxycodone in violation of 21 U.S.C.A. § 841(a)(1). *Id.* at 4.

Count Eight of the Second Superseding Indictment ("Count Eight") charges that Dastinot conspired with two co-defendants to launder money by engaging in transactions that "were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds" of unlawful activity, in violation of 18 U.S.C.A. §§ 1956(a)(1)(B)(i) and 1956(h). *Id.* at 5-7.

On October 31, 2014, Dastinot filed the instant Motion to Suppress Wiretap Evidence Under Title III and Request for a *Franks* Hearing (ECF No. 451), which was joined by co-defendants Ashley Gleason (ECF No. 454), Pierre Azor (ECF No. 466), Carrie Buntrock (ECF No. 471), Jean Valbrun (ECF No. 475), Jonathan Duffaud (ECF No. 477), Jacques Victor (ECF No. 479), and Alcindy Jean-Baptiste (ECF No. 498).

II. MOTION TO SUPPRESS

Dastinot raises five points in support of suppressing the wiretap evidence: (A) the Government's wiretap applications failed to establish necessity; (B) the wiretap applications dated after February 2014 were based upon an illegal initial wiretap and are therefore tainted; (C) there was no necessity for additional wiretaps after the initial TT1 wiretap; (D) there was no judicial finding of necessity for any of the wiretaps; and (E) the TT1 and TT2 wiretap applications list the incorrect authorizing official, and all the wiretap applications fail to specify a particular authorizing official. ECF No. 451 at 11-19.

A. Necessity

The necessity requirement restricts wiretapping to situations where traditional investigative techniques are not sufficient to expose criminal activity. *See United States v. Rivera-Rosario*, 300 F.3d 1, 19 (1st Cir. 2002). "[A] wiretap application [must] include '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.'" *United States v. López*, 300 F.3d 46, 52 (1st Cir. 2002) (quoting *United States v. Hoffman*, 832 F.2d 1299, 1306 (1st Cir. 1987)).

The necessity requirement does not require the Government to "show that other investigatory methods have been completely unsuccessful" or to "exhaust every conceivable alternative before resorting to electronic surveillance." *Rivera-Rosario*, 300 F.3d at 19. Instead, the Government need only show that "it has made 'a reasonable good faith effort to run the gamut of normal investigative procedures'" before resorting to a wiretap. *Id.* (quoting *Hoffman*, 832 F.2d at 1306). The court may also take into account the nature of the alleged crimes and give weight to the opinion of the investigating agents that other means are too dangerous and possibly counterproductive. *In re Dunn*, 507 F.2d 195, 197 (1st Cir. 1974).

Dastinot argues that the investigation "did not need wiretaps to flourish" and that investigators could have adequately uncovered the same evidence by utilizing a combination of cell site data, and both global positioning system ("GPS") and real time surveillance. ECF No. 451 at 11-16. Dastinot claims that cell site data would have pinpointed alleged sources of supply with precision because the proliferation of telecommunications base stations such as cellular towers and antennas over the past decade has caused such data to become much more accurate. *Id.* at 13-15. Dastinot also claims that Verizon Wireless, the service provider for TT1, includes a GPS chip on all phones sold after December 31, 2003, and that these GPS chips provide location information that is accurate to within 10 meters, thus obviating the need for a wiretap. *Id.* at 15-16.

Dastinot's arguments are refuted by the wiretap applications themselves. Agent Brown's February 24 Affidavit provides detailed explanations regarding why the traditional investigative methods performed to that point had not been successful in identifying sources of supply and other significant co-conspirators. February 24 Affidavit at ¶¶ 33-50, 146-63. The Affidavit also included a detailed explanation of the shortcomings of cell site data: "Precise location information . . . cannot show who a target meets with inside of a house, the nature of any communications related to drug trafficking, or the identity of other members of the conspiracy." *Id.* at ¶ 176. Agent Brown described, at great length, the use of confidential sources and cooperating defendants to purchase drugs from Dastinot and others, that failed to "provide specific details concerning the inner-workings of this drug trafficking conspiracy and [ ] state sources of supply." *Id.* at ¶ 152. *See also, id.* at ¶¶ 150-163, 182. Agent Brown also described the Government's efforts at physical surveillance, its use of pen registers, and its financial investigation, all of which occurred prior to the wiretap application. *Id.* at ¶¶ 168-180. The Affidavit also addressed various other investigative methods that the Government had considered and rejected as being either too dangerous or too likely to alert the people being investigated of the Government's efforts. *Id.* at ¶¶ 164-167, 181-187.

Where the stated primary goal of the investigation was to identify, prosecute, and convict Dastinot's at-that-point unknown sources of supply for illegal drugs and his significant co-conspirators, *see id.* at ¶ 146, this overview of investigative efforts adequately demonstrates that the sources of supply were unlikely to be learned through traditional law enforcement techniques. The wiretap application demonstrated that the wiretaps were reasonably necessary to develop a provable case against all significant members of the conspiracy. *See United States v. Noonan*, 2014 U.S. Dist. LEXIS 119294, at *11 (D. Me. Aug. 27, 2014).

B. Effect of Alleged Flaws in the Original Wiretap Authorization

Dastinot argues that "[s]ince the original [February 24] intercept was unnecessary here, the subsequent orders were tainted and any conversations intercepted should be suppressed." ECF No. 451 at 17. Because I conclude that the original wiretap authorization was necessary and proper, it follows that subsequent wiretap authorizations based upon the original order should not be suppressed under the theory that they are somehow tainted.

C. Diminished Necessity of Successor Wiretap Authorizations

I am also unpersuaded by Dastinot's alternative argument that even if the original February 24 wiretap authorization was legally obtained, the Government failed to establish necessity for the subsequent wiretap authorizations. *Id.* at 17 ("Rather than evaluate that information [from the original wiretap authorization] and employ traditional investigative techniques, they sought further wiretaps as a shortcut.").

Agent Brown's affidavits dating from March 25, April 24, and May 1, 2014, describe the same or similar investigative techniques as those described above from Brown's February 24 affidavit. Brown stated that law enforcement officers had used confidential sources and cooperating defendants, pen registers, physical surveillance, and financial investigation—and considered and rejected numerous other techniques ranging from undercover agents to pole cameras. March 25 Affidavit at ¶¶ 121-143;

April 24 Affidavit at ¶¶ 103-157; May 1 Affidavit at ¶¶ 81-130. As was the case with regard to the February 24 Affidavit, these affidavits also demonstrate that wiretaps were necessary to develop a provable case against all significant members of the conspiracy. *See Noonan,* 2014 U.S. Dist. LEXIS 119294, at *11.

D. Judicial Finding of Necessity

Dastinot contends that all four wiretap authorizations are deficient because they contain "boilerplate language" taken directly from 18 U.S.C.A. § 2518(1)(c), rather than an in-depth analysis and "judicial fact-finding" that, he asserts, is required by § 2518(3)(c). ECF No. 451 at 18 (citing *United States v. Giordano*, 416 U.S. 505, 533 (1974)). This argument is without merit. Section 2518 requires a judicial determination made "on the basis of the facts submitted by the applicant." 18 U.S.C.A. § 2518(3). Even if the language in each wiretap order tracks § 2518(1)(c) verbatim, that fact does not establish or suggest that the Court neglected to make a determination based upon the facts submitted by Agent Brown in his detailed affidavits, or that the Court failed to consider the results obtained by previous wiretaps, as required by *Giordano,* 416 U.S. at 533.

E. Objections Concerning the Authorizing Department of Justice Official

1. Defect in the Wiretap Application

Dastinot argues that the February 24 wiretap must be suppressed because the wiretap application names Deputy Assistant Attorney General Paul O'Brien as the Department of Justice ("DOJ") official authorizing the application, while the authorization letter attached to the application was signed by Deputy Assistant

Attorney General Kenneth A. Blanco. ECF No. 451 at 18 (citing *United States v. Reyna*, 218 F.3d 1108 (9th Cir. 2000)). Dastinot claims that this inconsistency violates 18 U.S.C.A. § 2518(1), which requires that a wiretap application list the name of the authorizing DOJ official. *Id.*

Dastinot's argument is foreclosed by *United States v. Chavez*, 416 U.S. 562, 574 (1974). Despite the error in listing different authorizing officials in the wiretap application and the authorization letter, both officials are Deputy Assistant Attorneys General. Accordingly, both may properly give authorization, and therefore "[i]n no realistic sense . . . can it be said that the order failed to identify an authorizing official who possessed statutory power to approve the making of the application." *Id.*

2. Defect in the Wiretap Order

Dastinot also notes that none of the wiretap orders state the name of the DOJ official who authorized the wiretap application, violating § 2518(4)(d). ECF No. 451 at 19 (citing *Reyna*, 218 F.3d at 1108). Dastinot argues that all four wiretap orders must be suppressed as a result. *Id.* [1]

A failure to include the identity of the authorizing DOJ official in a wiretap order constitutes a facial defect under § 2518(10)(a)(ii). *United States v. Savoy*, 883 F. Supp. 2d 101, 114 (D.D.C. 2012). However, this failure constitutes a "technical defect" that did not prejudice Dastinot or undermine the purposes of the statute. *Id.*

[1] Although Dastinot is correct that a wiretap order must state the identity of the authorizing Deputy Assistant Attorney General, *Reyna* does not support his argument because the crux of that case was the failure of federal prosecutors to secure the approval of the appropriate DOJ official *prior* to submitting a wiretap application. *Reyna*, 218 F.3d at 1111-12. The Ninth Circuit did not affirm the District Court's suppression of wiretap evidence based solely on the omission of the name of the authorizing DOJ official from the wiretap order. *See id.*

As the government notes, several courts have concluded that a wiretap order's failure to identify the person authorizing the application does not prejudice the defendant, and does not require the wiretap evidence to be suppressed. *Id.* (citing *United States v. Small,* 423 F.3d 1164, 1178 (10th Cir. 2005); *United States v. Radcliff,* 331 F.3d 1153, 1160 (10th Cir. 2003)) (other citations omitted). Thus, suppression is not necessary "where the wiretap application was authorized by an appropriate individual within the Department of Justice and that authorizing individual was identified by name in the wiretap application." *Id.* I see no sound reason to order the suppression of wiretap evidence based on the facial defect shown here.

III. REQUEST FOR A *FRANKS* HEARING

Dastinot seeks a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), which is required when "the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and the allegedly false statement is necessary to the finding of probable cause. *United States v. D'Andrea,* 648 F.3d 1, 12–13 (1st Cir. 2011) (citation and internal quotation marks omitted). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *United States v. Gifford,* 727 F.3d 92, 98 (1st Cir. 2013) (citation and internal quotation marks omitted). "In the case of allegedly material omissions, recklessness may be inferred where the omitted information was critical to the probable cause determination." *Id.* at 98–99 (citation and internal quotation marks omitted).

Dastinot contends that Agent Brown's statements in the February 24 Affidavit regarding the unavailability of GPS data and the inability of cell site data to provide precise location information were either deliberately false or demonstrated a reckless disregard for the truth. ECF No. 451 at 20. As evidence that Brown is lying or reckless, Dastinot cites a 39-page document that purports to originate from Verizon Wireless. *Id.* at 20-21. This document describes the operations of a "Law Enforcement Resource Team" ("LERT"), a "centralized command center for all law enforcement needs," which, the document states, provides 24 hour assistance to law enforcement on matters such as electronic surveillance, call details, cell site records, and requests for location information. *Id.* at 21 (citing *http://cryptome.org/isp-spy/verizon-spy.pdf*) (the "LERT Document").

Setting aside questions about its origin and reliability,[2] the LERT document does not contradict Agent Brown's affidavit. It states that Verizon Wireless can provide the "cell site that handled [a cell phone] call," LERT Document at 10, and that it can provide "cell site, sector, and approximate distance for recently completed calls and text messages." *Id.* at 21. Nothing in the LERT Document supports the notion that cell-site data is nearly as precise as Dastinot claims, nor does it contradict

[2] Dastinot acknowledges that he "is not sure what edition LERT manuel [sic] he has is, but it appears to be from 2007 or 2008, so it is a bit dated. This manual was originally intended for law enforcement use, but several organizations have uncovered it over time, including the American Civil Liberties Union." ECF No. 451 at 21 n.4. The website Dastinot cites is not the ACLU website, and Dastinot does not identify the organization from which he obtained the LERT document.

Brown's statement that "the range of error in this type of data prevents narrowing down a precise residence (especially in dense places like Boston and Lewiston)." *See id.*; February 24 Affidavit at ¶ 175. Also, the LERT Document does not support Dastinot's assertion that Verizon Wireless could make GPS data for a particular phone available to law enforcement. *See* LERT Document at 10, 21.

Dastinot has failed to make a substantial preliminary showing that Agent Brown made a deliberately false statement, or a statement with reckless disregard for the truth, in any of the four warrant affidavits. *See D'Andrea,* 648 F.3d at 12-13. Accordingly, Dastinot's request for a *Franks* hearing is denied.

IV. CONCLUSION

For the foregoing reasons, Dastinot's Motion to Suppress and Request for a *Franks* Hearing (ECF No. 451) is **DENIED**.

SO ORDERED.

This 23rd day of March, 2015.

/s/ Jon D. Levy
U.S. DISTRICT JUDGE