2019

The Wireless Wiretap Paradox: Fixing Illogical Interpretations of the Mobile Interception Device Exception

Anthony Ladouce

The Wireless Wiretap Paradox:

Fixing Illogical Interpretations of the Mobile Interception Device Exception

Anthony Ladouce

I. INTRODUCTION

In 1986, Congress enacted the Electronics Communications Privacy Act (ECPA), which modified federal wiretap law to exempt wiretaps that used a "mobile interception device" from

territorial jurisdiction limitations.[1] Most mobile phone users have no need to ask themselves who could be listening in to their conversations, tracking their Internet use, and monitoring their texts. In 1997, the Seventh Circuit set a precedent that granted this access to any law enforcement officer in the country able to get a warrant from the magistrate judge.[2] Until recently, this broad standard was unchallenged, leaving wiretaps for mobile phones explicitly open to any combination of judge and enforcer willing to reach out and listen in. But since 2013, judges and litigants have questioned the statutory construction, suggesting that Congress should resolve this jurisdictional paradox.[3]

In response, Congress must add a definition for the phrase "mobile interception device" to clarify its scope and purpose. Society is quickly becoming more mobile, and a jurisdictional exception exclusively for mobile phones is redundant and invasive in the waves of governmental mass surveillance scandals. This Comment will argue that the historical interpretation of the term "mobile" in the "mobile interception device" exception is seriously flawed and allows courts to violate key jurisdictional protections for a growing segment of the population. Specifically, this Comment will argue for a narrow, plain meaning interpretation of the phrase, which includes only interception devices capable of continuous operation while in motion. This Comment will also address the legislative and judicial loopholes that have masked the flawed exception, and argue that even if these loopholes are properly addressed, Congress must clarify the exception to

1 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 106(a), 100 Stat. 1848, 1856 (1986) (codified at 18 U.S.C. § 2518(3) (2012)).

2 *See* United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997).

3 *See, e.g.*, United States v. Dahda, 853 F.3d 1101, 1118 (10th Cir. 2017) (Lucero, J., concurring), *cert. granted*, 138 S. Ct. 356 (2017).

foreclose potential abuse by law enforcement and keep safeguards in place over realms of historically private communications.[4]

II. BACKGROUND

A. Wiretapping from Telegraphs to Mobile Phones

Wiretap law began with the telegraph in the mid-1800s, when eavesdroppers began "tapping" into telegraph wires to listen to messages, and several states began to criminalize wiretapping and disclosing messages in general.[5] Despite these laws, intercepted telegrams were widely used during the Civil War, and in 1920, the first black chamber was set up by the military to intercept communications through Western Union.[6] In 1928, the United States Supreme Court held that warrantless telephone wiretapping—and wiretapping by law enforcement in general—was constitutional.[7] Wiretap warrants were not required until 1967, when the Court held that the Fourth Amendment guarantees the protection of privacy in telephone conversations for even public telephone users.[8]

4 *See* Katz v. United States, 389 U.S. 347, 353 (1967).

5 *See* Christopher Woolf, *The History of Electronic Surveillance, from Abraham Lincoln's Wiretaps to Operation Shamrock*, PUBLIC RADIO INTERNATIONAL (Nov. 7, 2013), https://www.pri.org/stories/2013-11-07/history-electronic-surveillance-abraham-lincolns-wiretaps-operation-shamrock.

6 *See id.*

7 *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

8 *See Katz*, 389 U.S. at 353.

The new warrant requirement created the potential for jurisdictional ambiguity. Calls that passed through multiple territorial jurisdictions were not new when wiretaps were declared constitutional in 1928: the first transcontinental phone call was placed between New York City and San Francisco in 1915.[9] In 1951, long distance direct-dialing was introduced in a handful of states with an inaugural call between Englewood, New Jersey and Alameda, California.[10] By 1967, when the Supreme Court established the warrant requirement, courts were well aware that calls could frequently cross state lines.[11] Courts had no need to question territorial jurisdiction in the age of landline phones because law enforcement could simply obtain a warrant from a court with jurisdiction over the telephone line they wish to monitor.[12]

The question of jurisdiction arose when telephones suddenly became mobile. In 1946, phone companies experimented with mobile phone service in which the wire was replaced by a radio signal between the phone and a single transmission tower in a single city.[13] In 1983, the first handheld mobile phone was unveiled, along with the first mobile service in the United States

9 *See Phone to Pacific from the Atlantic*, N.Y. TIMES, Jan. 25, 1915, http://www.nytimes.com/learning/general/onthisday/big/0125.html.

10 *See* Tom Wilk, *Ringing In the New*, N.J. MONTHLY, Oct. 10, 2011, https://njmonthly.com/articles/jersey-living/ringing-in-the-new/.

11 *See, e.g.*, *Katz*, 389 U.S. at 348 (noting that calls were placed from Los Angeles to Miami and Boston).

12 *See* 18 U.S.C. § 2518(1) (2012) (procedure for wiretap order applications).

13 *See* Gordon A. Gow & Richard K. Smith, MOBILE AND WIRELESS COMMUNICATIONS: AN INTRODUCTION 23 (Open University Press 2006).

capable of calls outside the subscriber's home city.[14] Phones could move between "cells" managed by individual radio relays that acted as small telephone exchanges.[15] While businessmen and technology fans celebrated the start of the wireless age, legislatures contemplated how to legally wiretap a phone that transmits calls over unpredictable paths and could be moved outside a wiretap warrant's jurisdiction with little more than a drive across a state line.[16]

[14] *See Flashback: What We Said About Mobile Phones in 1983*, CBSNEWS.COM (Jan. 12, 2015), https://www.cbsnews.com/news/flashback-what-we-said-about-mobile-phones-in-1983/; *First Cell Phone a True 'Brick'*, NBCNEWS.COM (Apr. 11, 2005), http://www.nbcnews.com/id/7432915/ns/technology_and_science-wireless/t/first-cell-phone-true-brick/.

[15] *See id.* It is also important to note that although the cellular network generates valuable metadata such as subscriber locations and call records, the wiretaps discussed in the scope of this Comment are limited to communications, not metadata. Metadata collection invokes separate—albeit similarly disturbing—privacy concerns. *See generally* Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, EXHAUSTIVE SEARCH (Dec. 13, 2013), http://www.crypto.com/blog/celltapping/ (discussing various metadata collection methods that are not considered wiretaps).

[16] *See, e.g.*, *Electronic Communications Privacy Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 27–40 (1985) (statement of Philip J. Quigley, President, PacTel Mobile Cos., and Robert W. Maher, Executive Director, Cellular Telecommunications Industry Association) (discussing privacy concerns regarding then-unencrypted cellular calls placed in multiple states).

B. Legislative History of the Wiretap Act and ECPA

The Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act), passed partially in response to the Supreme Court's 1967 warrant mandate, included a federal framework for law enforcement to request wiretap orders from district courts, often referred to as the Wiretap Act.[17] Law enforcement was required to justify an application for a wiretap order by stating the crime committed or to be committed; the location and duration of interception; the type of communications law enforcement wishes to intercept; the suspect's identity, if known; and why other investigative procedures have failed or are likely to fail.[18] The Act also afforded defendants the right to move to suppress evidence derived from a wiretap that was unlawful, granted by a facially insufficient order, or performed in violation of the order.[19] If the government knew, or had reason to know, that the wiretap was unlawful or the order was insufficient, the evidence must be suppressed.[20] Originally, the judge could authorize an order for interception only within the judge's jurisdiction.[21] This presented little cause for concern in the landline era, because the jurisdiction where the phone was located could not be changed.

The challenges of the new cellular system were addressed by a 1986 amendment that relaxed the jurisdictional requirement when law enforcement uses a "mobile interception device"

17 18 U.S.C. § 2518 (2012).

18 *Id.* § 2518(1).

19 *Id.* § 2518(10)(a).

20 *Id.* § 2515.

21 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 219 (1968) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

to wiretap the target phone.[22] The Electronics Communications Privacy Act (ECPA) introduced a comprehensive set of new provisions and amendments in response to the explosion of personal computers and electronic communication devices.[23] Congress included the "mobile interception device" exception in response to judicial ambiguity over wireless conversations. The exception is the only language that authorizes a wiretap order outside a judge's territorial jurisdiction within the Wiretap Act as amended by the ECPA. Since 1986, when the ECPA was enacted, Congress has passed no new legislation expanding, limiting, or clarifying mobile phone wiretap order jurisdiction. Courts have grappled over what the ECPA amendments actually mean in practice within the already contentious framework for wiretap orders, and whether Congress actually intended it to actually apply to all mobile phone wiretaps.[24] The ECPA also broadened the scope of wiretaps to include "wire, oral, [and] electronic communications."[25] Electronic communications in turn include almost all data transferred to and from mobile phones, including

[22] 18 U.S.C. § 2518(3) ("[T]he judge may enter an ex parte order . . . authorizing or approving interception of wire, oral, or electronic communications . . . outside [the court's] jurisdiction but within the United States in the case of a mobile interception device . . . .").

[23] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[24] *Compare* United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017), *with* United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997).

[25] 18 U.S.C. § 2518(3) (2012).

Internet content and text messages.[26] As a result, most voice messages, texts, and data sent to and from mobile phones can be wiretapped by law enforcement under the ECPA.

C. Circuit Approaches to the Mobile Interception Device Exception

The mobile interception device exception creates three separate issues: when it applies, how it is relevant to the statutory framework, and whether abuse by law enforcement requires suppression of evidence gained by a wiretap. All of these issues have been fiercely debated by the circuits. The Seventh and Tenth Circuits directly interpreted the phrase "mobile interception device" in the context of mobile phone warrants.[27] The Seventh Circuit, in *United States v. Ramirez*, adopted a broad, implicit definition that includes any device that intercepts mobile phone communications.[28] The Tenth Circuit, in *United States v. Dahda*, disagreed and adopted a narrow, literal definition that only includes interception devices that are mobile themselves.[29]

The Second Circuit, among several others, has also interpreted the term "interception" to allow an interception to occur both at the location of the phone and the location where the wiretapped conversations are first heard by law enforcement at a listening post, which would question the efficacy of jurisdictional limitations.[30] Judge DeMoss of the Fifth Circuit argued for the narrow, literal definition of "mobile interception device," and that jurisdictional violations from misuse of the exception mandate suppression, as jurisdiction is a core concern of the Wiretap

26 *See id.* § 2510(12).

27 *See Dahda*, 853 F.3d at 1114; *Ramirez*, 112 F.3d at 853.

28 *See* 112 F.3d at 853.

29 *See* 853 F.3d at 1114.

30 *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992).

Act.[31] Additionally, the D.C. Circuit interpreted the phrase in the context of a listening device installed in a vehicle, and held that misuse of the exception by misclassifying the interception device requires suppression of evidence, in agreement with Judge DeMoss.[32] Consequently, the Tenth Circuit adopted Judge DeMoss's definition but refused to mandate suppression as argued by Judge DeMoss and the D.C. Circuit.[33]

Until 2017, when the Tenth Circuit challenged the Seventh Circuit's broad interpretation in *Ramirez*, legal scholars paid little attention to the mobile interception device exception. The only references to the exception outside judicial and legislative work have been through incidental analysis of wiretap jurisdiction as a whole, with scant focus on the exception itself.[34] The pending decision by the Supreme Court in *United States v. Dahda* will likely spark scholarly interest in the subject.

[31] *See* United States v. North, 735 F.3d 212, 215–16 (5th Cir. 2013) (DeMoss, J., concurring).

[32] *See* United States v. Glover, 736 F.3d 509, 513–15 (D.C. Cir. 2013).

[33] *See Dahda*, 853 F.3d at 1114–16.

[34] *See, e.g., Appendix A: State Wiretap Laws (as of June 1, 2002)*, 52 HASTINGS L.J. 987 (2003).

1. The Seventh Circuit's Broad Interpretation

In *United States v. Ramirez*, the Seventh Circuit held that the "mobile interception device" exception applies broadly to all communications sent to and from mobile devices.[35] The government was investigating a suspected methamphetamine distributor who lived in Wisconsin and traveled to Minnesota to conduct his business using a mobile phone.[36] A district judge in the Western District of Wisconsin issued a wiretap order for the suspect's mobile phone.[37] To avoid being recognized in Wisconsin, the government set up a listening post in Minnesota that intercepted calls as they were transmitted over microwave transmission towers using a stationary wiretap device.[38] Agents soon realized that one of the suspect's associates was using the phone, and he did not leave Minnesota, but he still discussed the illegal operation under investigation.[39] The government returned to the Wisconsin court to apply for an extension for the wiretap, but did not disclose that the conversations were occurring in, intercepted in, and monitored in Minnesota.[40] The Seventh Circuit noted that the original order provided that the interception could continue if the mobile phone was moved outside Wisconsin, under the authority granted by the "mobile interception device" exception in 18 U.S.C. § 2518(3).[41]

35 112 F.3d 849, 853 (7th Cir. 1997).

36 *Id.* at 850–51.

37 *Id.* at 851.

38 *Id.* at 851, 853.

39 *Id.* at 851.

40 *Id.*

41 *See Ramirez*, 112 F.3d at 852–53.

The Seventh Circuit was the first circuit to interpret the ECPA's "mobile interception device" language, and the court concluded that the exception applies to what is intercepted, not the device that is intercepting the calls.[42] The Seventh Circuit noted that the legislative history refers "to both a listening device installed in a vehicle and to a tap placed on a cellular or other telephone instrument installed in a vehicle," and interpreted such devices to be stationary in reference to the phone; therefore, a stationary "bug" device must still qualify as a "mobile interception device."[43] Additionally, the Seventh Circuit pointed out that a wiretap would be placed further along the connection than the handset itself, which implies a wiretap placed at a stationary location outside the vehicle would also be a "mobile interception device."[44] Accordingly, the Seventh Circuit interpreted the word "mobile" to invoke the concept of a mobile phone as a wiretap target, and held that a completely stationary interception device can still qualify as a "mobile interception device" if it intercepts mobile phone calls.[45] Under the Seventh Circuit's broad interpretation, the Wisconsin court could issue a wiretap order for mobile phone calls placed, intercepted, and first heard in any other jurisdiction in the United States, even if the phone and its user were never located within Wisconsin.[46]

42 *Id.* at 853.

43 *Id.* at 852–53; *see also* S. REP. NO. 99-541, at 30 (2d Sess. 1986).

44 *Ramirez*, 112 F.3d at 853.

45 *Id.*

46 *See id.* at 852 ("It is not certain that the phone in issue *was* transferred outside of the Western District of Wisconsin; it may never have been there; but we do not read the order as limited to the case in which the phone was at some time in the district.").

2. The Second Circuit's Interception Loophole

In *United States v. Rodriguez*, the Second Circuit held that the term "interception" in the Wiretap Act allows a listening post to be the point of interception for jurisdictional purposes in addition to the actual location where the lines are tapped.[47] The government obtained a wiretap order on five landline phones to investigate an organization suspected of distributing crack cocaine.[48] Four of the phones were located in a café in New Jersey and one was in an apartment in New York.[49] All five were monitored using a combination of leased telephone lines that rerouted calls through recording devices in New York, as authorized by the Southern District of New York.[50] Because *Rodriguez* addressed landline phones, the Second Circuit did not interpret the phrase "mobile interception device;" however, it laid the foundation for interpreting the term "interception."

The court noted that for the four New Jersey phones, an interception occurred when the local telephone company rerouted the calls from New Jersey to the listening post in New York.[51] Additionally, an interception occurred when the recorded conversations were first heard by the government at the listening post in New York, because the definition of "interception" includes

47 968 F.2d 130, 136 (2d Cir. 1992).

48 *Id.* at 133.

49 *Id.* at 134–35.

50 *Id.* at 135; *see also* United States v. Rodriguez, 734 F. Supp. 116, 119 (S.D.N.Y. 1990) (discussing the method used for the wiretap, which was identical to the preceding pen register method noted by the Second Circuit).

51 *See Rodriguez*, 968 F.2d at 135–36.

the "aural or other acquisition of the contents" of a communication.[52] Therefore, the Second Circuit held that the out-of-state wiretaps were still jurisdictionally sound, because the devices were installed within the authorizing court's jurisdiction, and the intercepted communications were first heard by agents within the same jurisdiction, regardless of the actual locations of the phones.[53]

Judge Meskill, in his concurrence, rejected the majority's reasoning in holding the interception authorized, but concurred because at the time of trial, the government did not know or have reason to know that the information had been obtained in violation of Title III—the wiretap provisions of the Omnibus Act.[54] Regarding the lawfulness of the interception, Judge Meskill argued that the territorial jurisdiction limitation of section 2518(3) would be effectively repealed by the majority's interpretation of the term "interception."[55] Judge Meskill pointed out that a plain meaning interpretation of "the 'acquisition of the contents' of a communication" refers to the acquisition of the communications as they are diverted; a transformation of those contents into sound to be heard by law enforcement is simply a conversion of previously acquired communications.[56] Because pen registers were unregulated at the inception of the Wiretap Act in 1968, the phrase "aural acquisition" was originally intended to simply exclude such non-conversational devices from the scope of the Act; the broad interpretation was arguably an

52 *Id.* at 136; *see also* 18 U.S.C. § 2510(4) (2012) (definition of an interception under the Wiretap Act).

53 *Rodriguez*, 968 F.2d at 136.

54 *Id.* at 145 (Meskill, J., concurring).

55 *Id.* at 143–44.

56 *Id.* at 144.

unintended effect.[57] Additionally, the ECPA's rephrasing of "aural or other acquisition" was simply to allow for interception of electronic communications, which were generally already in text form.[58]

While Judge Meskill posited that Congress never intended a broad interpretation of interception that bypassed section 2518(3)'s territorial jurisdiction limitation, he stopped short of recommending suppression.[59] Section 2515 only requires suppression if the government knew, or had reason to know, that the wiretap was unlawful or the order was insufficient.[60] Judge Meskill found no evidence that suggested the government knew, or should have known, that the wiretap order was facially insufficient due to the jurisdictional flaw; therefore, suppression was not mandatory, and the district court's refusal to suppress the evidence was proper.[61]

3. The Fifth Circuit's Prophetic Concurrence

In *United States v. North*, the Fifth Circuit avoided the territorial jurisdiction issue in *Ramirez* by finding that the government failed to minimize its monitoring to exclude conversations that were not connected to the investigation.[62] Although the court withdrew the original opinion and issued a revised decision based on the government's failure to satisfy the minimization

57 *Id.* (citing S. REP. NO. 90-1097 (2d Sess. 1986); Castillo v. State, 810 S.W.2d 180, 184 (Tex. Crim. App. 1990)).

58 *See id.* at 145.

59 *Rodriguez*, 968 F.2d at 145 (Meskill, J., concurring).

60 18 U.S.C. § 2515 (2012); *see id.* at 145.

61 *Rodriguez*, 968 F.2d at 145 (Meskill, J., concurring).

62 735 F.3d 212, 215–16 (5th Cir. 2013).

requirement, a concurrence in the revised opinion captured the original conclusion.[63] Judge DeMoss first noted that the order in question, issued by the Southern District of Mississippi, was used to intercept calls at a stationary listening post in Louisiana as they were made in Texas.[64] Notably, this included a call to another Texas phone during which the appellant disclosed incriminating information about an hour into the call.[65] Absent the mobile interception device exception, such an interception would be outside the Mississippi court's authority.[66] In his concurrence, Judge DeMoss pointed out that a statute's plain meaning controls unless it is at odds with the clear legislative intent.[67] Judge DeMoss interpreted "mobile" to modify "device" in the phrase "mobile interception device" and argued that the Seventh Circuit's broad interpretation in

[63] *Compare North*, 735 F.3d at 219 (DeMoss, J., concurring) (finding territorial jurisdiction a core concern of Title III of the Omnibus Act), *with* United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013) (citing United States v. North, 728 F.3d 429, 437 (5th Cir. 2013), *withdrawn*, *North*, 735 F.3d at 213) (noting that the Fifth Circuit held that territorial jurisdiction is a core concern of Title III).

[64] *North*, 735 F.3d at 217 (DeMoss, J., concurring).

[65] *Id.*; *see also id.* at 214 (majority opinion).

[66] *Id.* at 217 (DeMoss, J., concurring).

[67] *Id.* at 217–18 (citing United States v. Ron Pair Enters., Inc., 489 U.S. 235, 242 (1989); New Orleans Depot Servs., Inc. v. Dir., Office of Worker's Comp. Programs, 718 F.3d 384, 393 (5th Cir. 2013) (en banc)).

Ramirez, which focuses on the mobility of the mobile phone, is not obvious when reading the statute.[68]

Judge DeMoss also argued that suppression of the Texas call would have been justified under section 2518(10)(a), as the territorial jurisdiction violation was a core concern of Title III.[69] Suppression is not a guaranteed remedy—it is only required when a statutory element that "directly and substantially implement[s] the congressional intention to limit the use of intercept procedures" is violated.[70] Judge DeMoss noted that there was scant legislative history on whether jurisdiction was a core concern; however, the territorial jurisdiction requirement safeguards against the risk of forum manipulation by law enforcement.[71]

Similarly, in *United States v. Denman*, the Fifth Circuit previously held that an interception occurs at the point where the communication is captured or redirected, as well as the point where the contents are first heard.[72] While *Ramirez* and *North* had listening posts outside the courts' jurisdiction, the wiretap in *Denman* was authorized by and listened to in the Eastern District of Texas, despite intercepting a landline in the Southern District of Texas.[73] The Fifth Circuit agreed with the Second Circuit in *Rodriguez* and reasoned that a listening post where the contents of a

68 *Id.* at 218.

69 *Id.* at 219.

70 *North*, 735 F.3d at 218 (DeMoss, J., concurring) (quoting United States v. Donovan, 429 U.S. 413, 433–34 (1977)).

71 *Id*. at 219.

72 *See* 100 F.3d 399, 403 (5th Cir. 1996).

73 *Id.* at 401.

communication are first heard must qualify as the location of an "aural acquisition" of the intercepted communication and, therefore, is included as the location of an interception.[74]

4. The D.C. Circuit's Facial Insufficiency Mandate

In *United States v. Glover*, a case from 2013, the D.C. Circuit held that in the case of a facially insufficient order, the core concern test discussed by Judge DeMoss in *North* is irrelevant because the test posed for suppression by section 2518(10)(a)(ii) is mechanical; an order either is or is not facially insufficient, regardless of the core concern test.[75] The government obtained a wiretap order from the D.C. District Court for a recording device in the defendant's vehicle, which was located in Maryland, outside the district court's jurisdiction.[76] The D.C. Circuit first addressed whether the last two tests of section 2518(10)(a)—the sufficiency of the order, and an interception made outside the order's authorization—conflated with the first test, which simply grants suppression in cases of unlawfully intercepted communications.[77] To avoid making the last two tests redundant, which would violate a cardinal rule of statutory interpretation, the D.C. Circuit noted that the Supreme Court has applied the core concern analysis to the first test alone as a catch-all over the government's intercept procedures.[78] Other circuits, such as the Third, Fifth, and Sixth

74 *Id.* at 403.

75 736 F.3d 509, 513–14 (D.C. Cir. 2013).

76 *Id.* at 510.

77 *Id.* at 513; *see generally* 18 U.S.C. § 2518(10)(a) (2012).

78 *Glover*, 736 F.3d at 513.

Circuits, have drawn the core concern test into whether an order is insufficient on its face.[79] The D.C. Circuit held that in the case of a facially insufficient order, suppression is not only afforded by section 2518(10)(a), but required by section 2515, because the core concern test would ignore the plain meaning of the statute and render it redundant.[80]

The D.C. Circuit also addressed whether a mobile interception device must be initially installed within the warrant-issuing judge's jurisdiction.[81] Although this case addressed an actual microphone installed to record conversations in a vehicle instead of a telephonic wiretap, such devices are still considered mobile interception devices and are classified as wiretaps, as noted in an example in the legislative history.[82] When first read, it appears that section 2518(3) paradoxically allows judges to "authoriz[e] . . . interception . . . within the territorial jurisdiction of the court in which the judge is sitting," and to authorize interception anywhere in the United States for a mobile interception device, but the mobile interception device must be "authorized by a Federal court within such jurisdiction."[83] The D.C. Circuit reasoned that the phrase "such jurisdiction" must either refer to the judge's jurisdiction or implicitly refer to the property on which

79 *Id.* (citing United States v. Traitz, 871 F.2d 368, 379 (3d Cir. 1989); United States v. Vigi, 515 F.2d 290, 293 (6th Cir. 1975); United States v. Robertson, 504 F.2d 289, 292 (5th Cir. 1974)).

80 *Id.* at 513–14.

81 *See id.* at 514.

82 S. REP. NO. 99-541, at 30 (2d Sess. 1986).

83 18 U.S.C. § 2518(3) (2012).

the device is installed.[84] The D.C. Circuit pointed out that either way, for a judge to issue a valid order, the device must be authorized.[85] For the device to be authorized, it must be initially installed on property located within the judge's jurisdiction—otherwise, the phrase would be superfluous because there would be no other reason to authorize a mobile interception device.[86] The D.C. Circuit reframed the warrant under Rule 41 of the Federal Rules of Criminal Procedure, which states that a judge may issue a warrant for property outside their jurisdiction if the property is located within it when the order is issued.[87] Accordingly, the D.C. Circuit held that the property on which a mobile interception device is installed must be inside the authorizing judge's jurisdiction at least when the warrant is issued.[88]

The D.C. Circuit also distinguished *Glover* from two other circuit cases that excused facially insufficient warrants as "technical defects."[89] In *United States v. Moore*, the Eighth Circuit did not mandate suppression when a properly completed wiretap order was mistakenly not signed by the magistrate judge.[90] Similarly, in *United States v. Traitz*, the Third Circuit addressed an order with a mistakenly omitted page, and used the requesting affidavit and the fact that the judge signed the order to presume that the statutory requirements under section 2518 were met, refusing

84 *Glover*, 736 F.3d at 514.

85 *Id.*

86 *Id.*

87 *Id.* at 515 (citing FED. R. CRIM. P. 41(b)(2)).

88 *Id.*

89 *Id.*

90 41 F.3d 370, 375 (8th Cir. 1994).

to mandate suppression.[91] The D.C. Circuit argued that in these cases, the defect was the result of a mistake that did not have any practical consequences; however, violation of the territorial jurisdiction limitations of section 2518(3) was more than a technical defect and, absent the mistake, the order could not have possibly been issued.[92] Accordingly, the D.C. Circuit held that an order for a mobile interception device must, at a minimum, be issued when the property on which the device is installed is located within the judge's jurisdiction; a judge may not simply issue an order for a mobile interception device that would be installed on property consistently outside their jurisdiction.[93]

5. The Tenth Circuit's Frustrated Narrow Interpretation

In *United States v. Dahda*, decided on April 4, 2017, the Tenth Circuit became the first circuit court to explicitly exclude stationary wiretaps from the definition of "mobile interception device."[94] The government obtained wiretap orders from the District of Kansas for mobile phones used by the defendant and his co-conspirators.[95] The Tenth Circuit addressed whether the orders were facially insufficient because they authorized interceptions if the phones were moved outside the court's jurisdiction, regardless of how the interceptions took place.[96] The Tenth Circuit agreed with all other circuits in holding that an interception occurs both when the communications are

91 871 F.2d 368, 376–77 (3d Cir. 1989).

92 *See Glover*, 736 F.3d at 515.

93 *Id.* at 516.

94 853 F.3d 1101, 1114 (10th Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017).

95 *Id.* at 1111.

96 *Id.* at 1111–12.

redirected in the jurisdiction where the phone is installed, and when the communications are first heard at the listening post.[97] The Tenth Circuit departed from its sister circuits over the core definition of "mobile interception device," taking issue with the Seventh Circuit's first holding in *Ramirez*.[98]

The Tenth Circuit offered three possible definitions for a mobile interception device: "(1) a listening device that is mobile, (2) a cell phone being intercepted, or (3) a device that intercepts mobile communications, such as cell-phone calls," reasoning that only the first definition is in accord with the statute.[99] Unlike other circuits, the Tenth Circuit began by interpreting the plain language of the exception, and reasoned that the term "mobile" is an adjective that modifies "device" as opposed to modifying a "phone," which is not written in the statute.[100] The Tenth Circuit noted that the Seventh Circuit admitted that the broad interpretation deviates from the plain language of the statute.[101] The Tenth Circuit rejected this approach, countering the Seventh Circuit's invocation of the car phone bug example in the legislative history by pointing out that such a device would be mobile under either interpretation, which demonstrates that the legislative history is still in accord with a narrow, literal interpretation.[102] Accordingly, the Tenth Circuit held that while the listening post was located in the authorizing judge's jurisdiction, the fact that

97 *Id.* at 1112.

98 *Id.* at 1113–14.

99 *Id.* at 1113.

100 *Dahda*, 853 F.3d at 1113.

101 *Id.*

102 *Id.* at 1114.

the order authorized stationary interception of mobile phones outside the jurisdiction at all, in violation of the narrow interpretation, is enough to render it facially insufficient, in violation of section 2518(10)(a)(ii).[103]

While the Tenth Circuit held that the order was facially insufficient, the court refused to suppress the evidence obtained from it under section 2515 because it already extended the core concern test to section 2518(10)(a)(ii).[104] The Tenth Circuit pointed out that the congressional examples listed in the Wiretap Act do not show any examples of jurisdictional violations, which suggests that suppression is not warranted.[105] The Tenth Circuit also suggested that strict adherence to jurisdictional rules would cause confusion by requiring prosecutors to coordinate wiretap efforts among different jurisdictions on the same case.[106] Finally, the Tenth Circuit

[103] *Id.*; *see also* United States v. Dahda, No. 12-20083-01-KHV, 2014 U.S. Dist. LEXIS 53529 at *8 (D. Kan. Apr. 2, 2014) (noting that the listening post was located in the authorizing court's jurisdiction).

[104] *Dahda*, 853 F.3d at 1114 (citing United States v. Giordano, 416 U.S. 505, 527 (1974) (introducing the core concern test for 18 U.S.C. § 2518(10)(a)(i)); United States v. Radcliff, 331 F.3d 1153, 1162 (10th Cir. 2003) (extending the core concern test to 18 U.S.C. § 2518(10)(a)(ii))).

[105] *Id.* at 1115 (citing United States v. Chavez, 416 U.S. 562, 578 (1974) (declining to require suppression when an application for a wiretap misidentified the Assistant Attorney General who approved it, because such clerical errors were not mentioned as examples in the legislative history)).

[106] *Id.* (citing Adams v. Lankford, 788 F.2d 1493, 1499 (11th Cir. 1986)).

disagreed with Judge DeMoss in his *North* concurrence, reasoning that the jurisdictional restraints do not actually curb the risk of forum shopping because governments could either use an actual mobile interception device or establish a listening post in the preferred jurisdiction, which would still comply with the statute but could be performed anywhere.[107] On October 16, 2017, the Supreme Court granted certiorari to decide whether Title III mandates suppression for a facially insufficient warrant under *Dahda*.[108] The petition and initial briefs submitted to the Court did not, however, call into question the interpretation of the mobile interception device exception.[109]

In his concurrence, Judge Lucero specifically noted that the exception needs congressional attention.[110] While Judge Lucero did not object to the majority's refusal to suppress the evidence obtained under the facially insufficient warrant, he suggested that the exception was authored under the assumption that a mobile device would be required to intercept mobile phone calls, which is no longer the case.[111] Although this may have been the goal of Congress, Judge Lucero emphasized that the courts cannot torture the language to satisfy the exception in the absence of

[107] *Id.* at 1115–16.

[108] Dahda v. United States, 138 S. Ct. 356 (2017); *see* Petition for a Writ of Certiorari at I, *Dahda*, 138 S. Ct. 356 (Jul. 3, 2017) (No. 17-43), 2017 U.S. S. Ct. Briefs LEXIS 2372, at *6 [hereinafter *Petition*].

[109] *Petition*, *supra* note **Error! Bookmark not defined.**108, at *6; *see also* Brief for the United States in Opposition at I, *Dahda*, 138 S. Ct. 356 (Sep. 6, 2017) (No. 17-43), 2017 U.S. S. Ct. Briefs LEXIS 3249, at *3–4 [hereinafter *Brief in Opposition*].

[110] *Dahda*, 853 F.3d at 1118 (Lucero, J., concurring).

[111] *Id.* at 1119.

even an implied congressional mandate, which is not present in either the language of the statute or the legislative history.[112] Instead, Congress must modernize the Wiretap Act to meet the demands of an increasingly mobile society.[113]

112 *Id.*

113 *Id.*

III. ANALYSIS

A. Breaking into Modern Telecommunications Networks

To understand the importance of limiting wiretaps, it is important to understand the technological capabilities of law enforcement today. The circuit cases discussed in this Comment are almost all based on phone conversations, yet phone calls are becoming less common than text messages.[114] Unfortunately, Americans' shift away from talking does not hinder the Wiretap Act—texting and data usage, for Internet access or instant messaging, is still electronic communication subject to the same rules as wire communication.[115] To that end, privacy-conscious citizens have long feared governmental intrusion into the privacy of their phones and computers.

Sadly, that intrusion is real, and law enforcement does not want us to know about it. For example, the National Security Agency's (NSA) mass surveillance programs were kept secret until details were leaked to the press.[116] Security experts suggested that such programs can target

[114] Corilyn Shropshire, *Americans Prefer Texting to Talking, Report Says*, CHICAGO TRIBUNE (Mar. 26, 2015), http://www.chicagotribune.com/business/ct-americans-texting-00327-biz-20150326-story.html.

[115] *See* 18 U.S.C. § 2510(12) (2012) (definition of electronic communication); 18 U.S.C. § 2518 (2012) (subjecting electronic communication to the same wiretap authorization procedure as wire communication).

[116] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (Jun. 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

essentially any email, chat, voice, file, or social networking communication in the United States.[117] The NSA has also tapped into international data networks to obtain warrantless access to much of this web content, as it was hosted and accessible outside the United States.[118] Beyond the NSA, the FBI has strong-armed large Internet companies into turning over customer data without warrants by using hundreds of thousands of national security letters, which are rarely contested.[119] Of course, these programs are not only relatively old news, but are apparently focused on mass surveillance of suspected terrorists, who are generally non-citizens.[120] The announcement of these programs sparked widespread media attention and spawned waves of articles written by legal

[117] *See NSA Surveillance*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance (last visited Oct. 30, 2017); Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, THE GUARDIAN (Jun. 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[118] Sean Gallagher, *How the NSA's MUSCULAR Tapped Google's and Yahoo's Private Networks*, ARS TECHNICA (Oct. 31, 2013), https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/.

[119] Rebecca Grant, *Google Tried to Resist FBI Requests for Data, but the FBI Took it Anyway*, VENTUREBEAT (Jun. 6, 2013), https://venturebeat.com/2013/06/06/google-tried-to-resist-fbi-requests-for-data-but-the-fbi-took-it-anyway/.

[120] Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms that it Gathers Online Data Overseas*, N.Y. TIMES (Jun. 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html.

scholars. Mass surveillance is outside the scope of this Comment, but the announcement of its prevalence has informed the public how deep law enforcement has dug into the telecommunications industry.

While local police departments would not have had access to top secret NSA surveillance data, the Communications Assistance for Law Enforcement Act (CALEA) provides enough of a framework to grant law enforcement technical access to all telephone and Internet traffic in the United States, similar in scope to the NSA's programs.[121] Since 1995, CALEA requires telecommunications companies to implement technology that intercepts wire and electronic communications in real time without detection and delivers communications to a listening post anywhere in the United States.[122] CALEA also facilitates smooth transitions for data collection between mobile service providers, such as mobile phones roaming on a different company's network.[123]

Although CALEA-based wiretaps would qualify as a mobile interception device only under the broad interpretation of the exception, many law enforcement agencies have actual mobile devices that can intercept communications between mobile phones and cell towers. Cell site simulators, often called "Stingrays" as a genericized trademark of the Harris Corporation's StingRay, simulate mobile phone carriers' cell towers to force nearby mobile phones to connect to the simulator, which can be used to track users' locations, intercept communications, and deny

121 Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002(a) (2012).

122 *See id.*

123 *See id.* § 1002(d).

service.[124] Simulators can be optionally configured to only track identification and location data, which allows them to be classified as pen registers outside the Wiretap Act, exempting them from warrant requirements.[125]

Unfortunately, the companies that manufacture these devices use trade secret law to force law enforcement agencies to not disclose their technical specifications.[126] Consequentially,

[124] *See* Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. TIMES (Mar. 15, 2015), https://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html.

[125] U.S. DEP'T OF JUSTICE, CELL SITE SIMULATORS/DIGITAL ANALYZERS/TRIGGERFISH, *in* FOIA Document Production, 10–11 (Oct. 27, 2015) ("Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III [Wiretap Act] order."), https://www.aclunc.org/docs/20151027-crm_lye.pdf; *see also* Linda Lye, *New Docs: DOJ Admits that StingRays Spy on Innocent Bystanders*, ACLU OF N. CAL. (Oct. 28, 2015), https://www.aclunc.org/blog/new-docs-doj-admits-stingrays-spy-innocent-bystanders (press release accompanying FOIA production).

[126] *See* Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015) (noting a case in which government offered a plea bargain to avoid an order to show the cell site simulator, which was used to locate defendant, to defense attorneys); *Harris StingRay Datasheet*, USPTO TSDR CASE VIEWER, 27 (Jul. 18, 2002) (note distribution warning at bottom of page),

judges, legislators, and legal scholars are unaware of what these devices are truly capable of.[127] Trademark and patent records show that devices manufactured by Harris Corporation have been capable of intercepting, at least, mobile phone voice calls and texts since the mid-1900s.[128] Critically, the fact that these devices are owned and operated by law enforcement agencies invites warrantless abuse, as opposed to CALEA-based requests from telecommunications companies. This is especially worrying because 2016 was the first year that mobile phone connections

http://tsdr.uspto.gov/documentviewer?caseId=sn76303503#docIndex=19&page=27 [https://www.documentcloud.org/documents/1282621-02-07-18-2002-harris-stingray-datasheet-ocr.html].

127 *See* Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says,* N.Y. TIMES (Feb. 11, 2016) (discussing nondisclosure agreements), https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html; *cf.* Linda Lye, *Justice Department Emails Show Feds Were Less Than "Explicit" with Judges on Cell Phone Tracking Tool,* ACLU OF N. CAL. (Mar. 27, 2013) (describing an example of "the federal government . . . routinely using stingray technology in the field, but failing to 'make that explicit' in its applications to the court to engage in electronic surveillance"), https://www.aclunc.org/blog/justice-department-emails-show-feds-were-less-explicit-judges-cell-phone-tracking-tool.

128 *See* Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data,* ARS TECHNICA (Sep. 25, 2013) (describing "Porpoise", software that can intercept text messages, and "Triggerfish", a device that can intercept voice conversations), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

surpassed landlines.[129] In short, it appears that law enforcement is actively hiding its ability to intercept communications from the most popular method of communication in the United States without the telecommunications service provider's knowledge, and, in theory, without judicial oversight.

Regardless of their ambiguity, cell site simulators are limited to being used in the field, while CALEA-compliant telecommunications equipment can intercept all voice, text, and data communications sent through any public networks in the United States and send them to a remote listening post. Circuit courts are faced with the 1986 mobile interception device exception, which is stuck in the framework of the 1968 Wiretap Act and was only interpreted by a 1997 Seventh Circuit case until recently. This combination of outdated, hardly-scrutinized law leaves district and other circuit courts with very little guidance on how to control law enforcement's unprecedented access to Americans' private conversations and data.

B. Interpreting the Mobile Interception Device Exception

1. The Plain Meaning Suggests a Narrow Interpretation

The phrase "mobile interception device" plainly refers to an interception device that is mobile. The first step to statutory interpretation is deciphering the statute's plain meaning.[130] The

[129] *Milestone for Cellphones vs. Landline Phones*, CBSNEWS.COM (May 4, 2017), https://www.cbsnews.com/news/milestone-for-cellphones-vs-landline-phones/.

[130] *E.g.*, Sebelius v. Cloer, 569 U.S. 369, 376 (2013) (quoting BP Am. Prod. Co. v. Burton, 549 U.S. 84, 91 (2006)) ("As in any statutory construction case, '[w]e start, of course, with the statutory text,' and proceed from the understanding that '[u]nless otherwise defined, statutory terms are generally interpreted in accordance with their ordinary meaning.").

Tenth Circuit's interpretation of the exception's language is refreshingly sound and reflects the obvious plain meaning of the text. Section 2510 implicitly defines an interception device, but does not define "mobile."[131] To do so, we refer to the common definition, which defines "mobile" as both a noun and an adjective.[132] The noun form—"a portable wireless telephone . . . a mobile phone, a cell phone"—lists exclusively British English usage examples.[133] The phrase "mobile phone" is a predominantly British term as well. Americans prefer the phrase "cell phone," however, this Comment avoids this phrase because it implicitly sidesteps inquiry into the term "mobile" entirely.[134]

It is difficult to imagine Congress using such a quaint, unconventional definition when they could have simply used the phrase "mobile phone" or even "cell phone". The adjective form of "mobile" is much more clear—"not fixed or stationary; capable of or characterized by movement;" alternatively, a device that "uses wireless portable transmitters and receivers, rather than physical connections, to transmit and receive signals."[135] As the Tenth Circuit pointed out, the term

[131] *See* 18 U.S.C. § 2510(4) (2012) (definition of "intercept"); 18 U.S.C. § 2510(5) (2012) (definition of "electronic, mechanical, or other device").

[132] *See Mobile, adj.1*, OED ONLINE (Jun. 2017), http://www.oed.com/view/Entry/120489; *Mobile, n.5*, OED ONLINE (Jun. 2017), http://www.oed.com/view/Entry/120487.

[133] *See Mobile, n.5*, *supra* note **Error! Bookmark not defined.**132.

[134] *See Cell Phone, n.*, OED ONLINE (Jun. 2017) (noting the term is chiefly North American), http://www.oed.com/view/Entry/241844; *Mobile Phone, n.*, OED ONLINE (Jun. 2017) (noting the term is chiefly British), http://www.oed.com/view/Entry/253434.

[135] *Mobile, adj.1*, *supra* note **Error! Bookmark not defined.**132.

"mobile" must modify either "interception," "device," or both.[136] But regardless of which word it modifies, the result is the same. The interception device itself must be mobile. Modifying "interception" would result in a device that can perform mobile interceptions, so at least some part of the device must be mobile. The Wiretap Act states that a "device . . . used to intercept a . . . communication" explicitly excludes "any telephone . . . equipment or facility, or any component thereof," further removing mobile phones from the definition of an interception device.[137] Consequently, the Seventh Circuit's broad interpretation conjures the term "phone" to twist the statute's plain meaning. The obvious plain meaning, from an American linguistic perspective, is that a mobile interception device is an interception device that is mobile.

2. The Legislative History Does Not Conflict with a Narrow Interpretation

In *United States v. Ramirez,* the Seventh Circuit misunderstood the only examples in the legislative history that invoked the mobile interception device exception.[138] Congress pointed "to both a listening device installed in a vehicle and to a tap placed on a cellular or other telephone instrument installed in a vehicle" as examples of uses of the exception.[139] The Seventh Circuit argued that these examples suggested that the exception "was intended to carry a broader meaning than the literal one," rendering the examples "illustrative rather than definitional."[140] The Seventh

136 United States v. Dahda, 853 F.3d 1101, 1113 (10th Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017).

137 18 U.S.C. § 2510(5) (2012).

138 *See* 112 F.3d 849, 852–53 (7th Cir. 1997).

139 S. REP. NO. 99-541, at 30 (2d Sess. 1986).

140 *Ramirez*, 112 F.3d at 852.

Circuit twisted the concept of mobile to suggest that a listening device on a car phone is not mobile because it is "a stationary device affixed to a stationary object in a moving vehicle."[141]

The Seventh Circuit's analytical process here is strained, at best, because a listening device in a moving vehicle is, by common sense, a mobile device. The definition of "mobile" encompasses objects that are "capable of or characterized by movement;" more specifically, a "facility or service [that is] accommodated in a vehicle so as to be transportable and able to operate in different places."[142] To suggest that a device is no longer "capable of or characterized by movement" because it is stationary relative to a moving object is disingenuous and reduces the distinction to absurdity. For example, a wristwatch could not be mobile because it is stationary relative to the user's wrist. As the Tenth Circuit pointed out, the examples posited in the legislative history describe precisely what Congress intended—an interception device that could physically move between jurisdictions to continue intercepting communications as needed.[143] The narrow interpretation is in accord with the legislative history, so the only reason to bypass the plain meaning of the statute would be if it produces an absurd result.[144]

[141] *Id.* at 852–53.

[142] *Mobile, adj.1*, *supra* note **Error! Bookmark not defined.**132.

[143] United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017).

[144] *See* Sebelius v. Cloer, 569 U.S. 369, 381 (2013) (quoting Hartford Underwriters Co. v. Union Planters Bank, N.A., 530 U.S. 1, 6 (2000)) ("[W]hen [a] statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.").

3. The Narrow Interpretation's Result is Far from Absurd

While a plain meaning can be overridden if it produces an absurd result, the result of the narrow interpretation is neither absurd nor even unfair.[145] The timing of the ECPA suggests that Congress was concerned about wiretapping mobile phones, and the lack of any other language relevant to mobile phones suggests that Congress was intending the mobile interception device exception to cover mobile phones. The two different interpretations of the exception, however, both produce incongruent results with the goals of the Wiretap Act.

Under the broad interpretation, jurisdictional limitations are shed when using a "device for intercepting mobile communications."[146] The Seventh Circuit does not define "mobile communications," but under the Wiretap Act, a device is "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," so the only stipulation that the broad interpretation puts on any wiretap is that the communication it captures must be mobile.[147] Of course, the broad interpretation would include interceptions of mobile phone signals as either wire or electronic communications as they are transmitted to and from the cell tower. Indeed, Congress no doubt intended this, because it would have been impossible to predict the path that a mobile phone call would make beyond the radio connection to the cell tower until CALEA's introduction

145 *Id.*

146 *Ramirez*, 112 F.3d at 853.

147 18 U.S.C. § 2510(5) (2012).

in 1995 made it possible for law enforcement to be able to pinpoint those calls from anywhere in the telecommunications network.[148]

Under the narrow interpretation, jurisdictional limitations are shed when using "a mobile device for intercepting communications."[149] While somewhat redundant because devices under the Wiretap Act must intercept communications regardless, it comes to the same result in the age of the ECPA's introduction in 1986. A mobile interception device could not intercept landline calls, and communications from a mobile phone could not be intercepted without a mobile interception device.[150] Once CALEA mandated nationwide wiretap capabilities, mobile phones could be intercepted as they passed through stationary networks and rerouted regardless of their location, but the Wiretap Act was not updated to reflect this change. Landline phones, with the exception of wireless handsets, still cannot be intercepted by mobile interception devices, because the only mobile interception devices created have been to intercept mobile phone signals.

It appears that the results of either interpretation are identical, but they differ in their implementation. The broad interpretation authorizes stationary wiretaps without regard to the plain meaning of the text. On the other hand, the narrow interpretation authorizes mobile wiretaps

148 *See generally* Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002(a)(1) (2012).

149 United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017), *cert. granted*, 138 S. Ct. 356 (2017).

150 *See generally, e.g.*, *Flashback: What We Said About Mobile Phones in 1983*, *supra* note **Error! Bookmark not defined.**14 (describing how calls would be "switch[ed] . . . from one cell to the next," eliminating any single point of stationary interception).

in accord with the plain meaning, hardly an absurd result. While the broad interpretation is not necessarily absurd either, technology has outpaced its spirit and the text of the statute as a whole.

C. Addressing the Loopholes in the Wiretap Act

To eliminate ambiguity and modernize the mobile interception device exception, Congress should amend 18 U.S.C. § 2510 to append the following definition:

> (22) "mobile interception device" means any electronic, mechanical, or other device (as defined under part 5 of this section) capable of continuous interception while in motion.

Although law enforcement typically uses CALEA to perform mobile phone wiretaps, this definition presents two key advantages over simply removing the mobile interception device exception. First, in emergency situations, law enforcement may have a need to identify and intercept communications without telecommunications company assistance, knowledge, or delay.[151] This amendment protects their reliable ability to do so without jurisdictional limitations through the use of a mobile interception device.[152] Second, this definition captures and reinforces the plain meaning of the language, but also adds a safeguard that the device must be able to operate while in motion. For example, a small device that hooks into a phone line could theoretically be described as "mobile" while not in use. This definition avoids that loophole by requiring the device to be "capable of continuous interception while in motion." A cell site simulator installed in a

[151] *See, e.g.*, Nabozny v. Marshall, 781 F.2d 83, 85 (6th Cir. 1986) (noting that a kidnapping and subsequent extortion satisfied all elements of § 2581(7) as an "emergency situation" that demanded expediency).

[152] *Cf.* 18 U.S.C. § 2518(7) (2012) (provisions for emergency interception).

vehicle may not be mobile according to the Seventh Circuit's "stationary bug" theory, but it can continue to operate while in motion.

Several circuits have argued that by limiting law enforcement to a single jurisdiction—or, with the dual reading of "interception," two jurisdictions—the legislature would reduce judicial and enforcement efficiency, and further chip away at privacy, by requiring wiretap orders from judges in each jurisdiction where the mobile phone is used.[153] But as the Tenth Circuit pointed out when admitting the inefficacy of its new interpretation of the exception, the dual reading of "interception" already grants the government the ability to forum shop.[154] The root of the problem is that by permitting listening post interceptions, Congress and the judiciary grant law enforcement the ability to perform wiretaps that are in clear violation of jurisdictional boundaries.[155] No circuit has firmly held that an interception only occurs at the point where the communications are intercepted. Although it would take only a minor change to the Wiretap Act, it appears unlikely that Congress would roll back this popular loophole in wiretap law.

The interception loophole, however, does not render repairing the mobile interception device exception a wholly moot proposition. Assume, hypothetically, that a law enforcement agency in Texas wishes to wiretap a mobile phone in South Carolina, but judges in Texas and South Carolina are protective of privacy and are not willing to issue the order. A judge in New

153 *See, e.g.*, United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) ("If all of the authorizations are sought from the same court, there is a better chance that unnecessary or unnecessarily long interceptions will be avoided.").

154 *Dahda*, 853 F.3d at 1115–16.

155 *See Rodriguez*, 968 F.2d at 144 (Meskill, J., concurring).

York, however, is willing to be flexible, so she issues an order that is used to perform a stationary wiretap. Under the broad interpretation, this is completely acceptable. Under the narrow interpretation, it is not. The Tenth Circuit argued that to comply, law enforcement may simply set up a listening post in New York.[156] But to do so, law enforcement must expend at least some modicum of effort, either by obtaining the cooperation of New York law enforcement or traveling to New York to do it themselves.

Therein lies the paradox. Law enforcement relies on the mobile interception device exception for stationary wiretaps, but courts are reluctant to tighten the exception because law enforcement could still use stationary wiretaps with extra effort. Congress must step in to resolve the issue by amending section 2510 to define the exception and guide judges and law enforcement to satisfactorily apply the proper narrow interpretation, which would be unavoidable under the amended definition. The additional burden that the amendment would place on law enforcement is, perhaps, even too little of a roadblock in the face of such a blatant privacy nightmare as allowing any law enforcement agent in the country to monitor any mobile phone in the country simply on the grounds that it is a mobile phone. To subject law enforcement to the choice of one or two jurisdictions is more than enough for the purposes of such serious invasions of privacy. Ultimately, the safeguard that the narrow interpretation imposes is a critical one in light of ongoing mass surveillance scandals.

1. Effects of the United States v. Dahda Suppression Ruling

156 *See Dahda*, 853 F.3d at 1115–16.

On October 16, 2017, the Supreme Court granted certiorari to decide whether Title III mandates suppression for a facially insufficient warrant under *Dahda*.[157] The government did not dispute the narrow interpretation of the exception used by the Tenth Circuit.[158] During oral argument on February 21, 2018, the Supreme Court appeared to focus on the insufficiency of the *Dahda* wiretap order and did not address the interpretation of the mobile interception device exception.[159] Accordingly, the Supreme Court review of *Dahda* will probably not resolve the interpretation question.

The submitted briefs focus on the right of suppression granted by sections 2518(10) and 2515, and whether territorial jurisdiction is a core concern of Title III.[160] If jurisdiction is a core

[157] Dahda v. United States, 138 S. Ct. 356 (2017); *see Petition*, *supra* note **Error! Bookmark not defined.**108, at *6; *see also Brief in Opposition*, *supra* note **Error! Bookmark not defined.**109, at *3–4.

[158] Brief for the United States at 6, *Dahda*, 138 S. Ct. 356 (Jan. 5, 2018) (No. 17-43), 2018 U.S. S. Ct. Briefs LEXIS 15, at *14.

[159] *See* Richard M. Re, *Argument analysis: What makes wiretap orders "insufficient"?*, SCOTUSBLOG (Feb. 22, 2018, 12:39 PM), http://www.scotusblog.com/2018/02/argument-analysis-makes-wiretap-orders-insufficient/; *see generally Dahda v. United States*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/dahda-v-united-states/ (last visited Mar. 2, 2018) (timeline of proceedings).

[160] *See* Brief for the United States at 12–15, *supra* note **Error! Bookmark not defined.**158, at *23–28; Brief for the Petitioners at 14–16, *Dahda*, 138 S. Ct. 356 (2017), 2017 U.S. S. Ct. Briefs LEXIS 4666, at *26–29.

concern, or the core concern test is irrelevant, the court must suppress evidence obtained through warrants that violate jurisdictional requirements.[161] This result shifts the question back to the interpretation of the mobile interception device exception, because failure to meet the requirements of the exception would trigger suppression of evidence. If, however, jurisdiction is *not* a core concern, Congressional attention is required. The mobile interception device exception, along with the rest of section 2518's territorial jurisdiction requirements, would be rendered superfluous because courts would no longer need to suppress evidence obtained through wiretap orders that do not comply with section 2518, despite Congress's clear intent to impose section 2518's jurisdictional requirements on wiretap orders.[162]

IV. CONCLUSION

Law enforcement is more than well equipped to intercept the communications of Americans without the help of the needlessly broad interpretation of the mobile interception device exception spearheaded by the Seventh Circuit.[163] In 1986, Congress was primarily concerned with simply *facilitating* mobile phone wiretaps. Federal courts and law enforcement have taken that exception to its extremes, imbuing it with a definition it was not intended to have and empowering

161 *Compare* United States v. Dahda, 853 F.3d 1101, 1114–16 (10th Cir. 2017) (finding suppression not required because jurisdiction *is not* a core concern) *with* United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013) (finding suppression warranted because jurisdiction *is* a core concern).

162 *See* S. REP. NO. 90-1097, at 97 (2d Sess. 1968) ("The application must confirm to section 2518 . . . . The judicial officer's decision is also circumscribed by section 2518.").

163 *See generally* United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997).

it with a rapid shift in technology on all sides. The Tenth Circuit caught this interpretive quirk and corrected it, but failed to follow through with mandatory suppression.[164] The Supreme Court has not been asked to weigh in.[165]

Because federal courts are hesitant to move forward, it is Congress's turn to fix the paradox. The only amendment to make is the addition of a definition of the phrase "mobile interception device." Congress was unaware of the future of technology in 1986, but it has had over two decades to catch up since CALEA opened up the possibility of stationary mobile phone wiretaps.[166] Law enforcement now has the technology to intercept mobile phone communications and locations both in the field and from their desks. Worse, they can do so from their desks for any phone in the United States. In the waves of mass surveillance scandals, this is not the theme that our nation's wiretap law should cling to. If the government wishes to break into our private mobile lives, it should do so under clear, concise, and controlling guidelines. To give law enforcement any additional leeway is only another step on the long road to an Orwellian elimination of privacy.

164 *See Dahda*, 853 F.3d at 1114, 1116.

165 *See Petition*, *supra* note **Error! Bookmark not defined.**108, at *6.

166 *See generally* Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1002(a), (d) (2012).