Boston College Law Review

Volume 59
Issue 9 *Electronic Supplement*

Article 3

3-19-2018

If Technology is the Hare, Is Congress the Tortoise? Split Circuits in the Wake of *Dahda*

Michael Koch
Boston College Law School, michael.koch.2@bc.edu

IF TECHNOLOGY IS THE HARE, IS CONGRESS THE TORTOISE? SPLIT CIRCUITS IN THE WAKE OF *DAHDA*

Abstract: In *United States v. Dahda*, the U.S. Court of Appeals for the Tenth Circuit held that, under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), the lower court properly denied Dahda's motion to suppress evidence gathered by law enforcement using a mobile interception device—a device that wiretaps cell phones. A key part of the decision focused on the definition of mobile interception devices. The Tenth Circuit defined them as devices used to intercept communications that are movable. The Seventh Circuit, in contrast, has defined mobile interception devices as devices used to intercept mobile communications. This Comment argues that both definitions are overly broad in the modern context and are at odds with the congressional intent underlying Title III.

INTRODUCTION

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") governs the legality of the interception and disclosure of oral and wire communications.[1] Title III generally makes the interception and disclosure of wire and oral communications an unlawful activity.[2] This legislation, enacted in 1968, addresses the problem of balancing the need to protect the privacy of individuals' communications against the necessity of facilitating law enforcement investigations.[3] Technological advances, however, have begun to upset this balance, resulting in a circuit split over the definition of one class of tools used to intercept communications: "mobile intercept devices."[4]

---

[1] *See* Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (2012) (covering the entire text of Title III).

[2] *Id*. at §§ 2515, 2516. Section 2516 provides for a small number of law enforcement officers who may apply for authorization to intercept communications. *See id.* § 2516. Law enforcement may seek authorization to intercept communications during investigations of certain crimes including embezzlement, murder, terrorism, bribery of public officials, and a number of other federal crimes. *See id.* § 2516(1)(a)–(t).

[3] *See* S. REP. NO. 90-1097, at 2153 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153. In enacting Title III, Congress sought to implement the dual purposes of protecting oral and wire communications' privacy and creating a uniform set of circumstances and conditions under which authorizations for interception may be issued. *See id.* To protect privacy, Congress forbade wiretapping and electronic surveillance by any person other than a law enforcement officer. *See id.* To ensure a uniform set of circumstances and conditions for authorization, wiretapping and electronic surveillance are only allowed for the investigation or prevention of specified kinds of serious crimes and require a showing of probable cause and authorization by a judge. *See id.*

[4] *Compare* United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017) (limiting the definition of interception devices to those devices that are mobile), *with* United States v. Ramirez, 112

In the 2017 decision *United States v. Dahda*, the Tenth Circuit declined to follow the Seventh Circuit's definition for the term "mobile interception device."[5] The Tenth Circuit held that a series of extraterritorial wiretap authorizations were facially insufficient based on a plain language definition of mobile intercept device.[6] Ultimately, however, the Tenth Circuit upheld the district court's denial of the defendant's motion to suppress the evidence gathered.[7] The U.S. District Court for the District of Kansas convicted the defendant, Los Dahda, of crimes related to an alleged marijuana distribution conspiracy.[8] The court accordingly sentenced Dahda to imprisonment and a fine of nearly seventeen million dollars.[9] The defendant appealed the verdict, focusing on nine orders issued by the district court authorizing wiretaps on the defendant's and his co-conspirators' cell phones.[10] The orders further provided that interception could take place in any other jurisdiction within the United States, should the targeted cell phone leave the issuing judge's jurisdiction.[11] At trial, the defendant moved to suppress the intercepted communications, asserting that the wiretap orders violated Title III's limitation on interceptions outside the issuing court's territorial jurisdiction.[12] The district court denied the motion and the defendant appealed to the Tenth Circuit on the grounds that the facial insufficiency of the authorizations entitled him to suppression of the evidence gathered from the related interceptions.[13]

This Comment argues that neither the Tenth Circuit's nor the Seventh Circuit's definition, in the modern context, is consistent with the congression-

---

F.3d 849, 853 (7th Cir. 1997) (defining devices for intercepting mobile communications more broadly).

[5] *Dahda*, 853 F.3d at 1114.

[6] *Id.* The court held that the wiretap orders authorized the use of stationary listening posts to intercept cell phone communications, both of which could be beyond the court's territorial jurisdiction. *Id.* The Tenth Circuit, however, defined "mobile interception device" as an interception device that can be easily moved, thus excluding stationary listening posts from the exception in Section 2518. *See id.* Used in this context, an extraterritorial wiretap authorization refers to an order authorizing a wiretap outside of the issuing judge's territorial jurisdiction. *See id.* at 1111 (noting that the wiretap orders under which evidence was gathered exceeded the issuing judge's territorial jurisdiction); *see also Extraterritorial*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "extraterritorial" as "occurring beyond the geographic limits of a particular jurisdiction"). A facially insufficient authorization order is an order that does not conform to the requirements under 18 U.S.C. § 2518(1).

[7] *Dahda*, 853 F.3d at 1116.

[8] *Id.* at 1105. According to the trial court findings, Dahda helped the network by driving cash from Kansas to California, helping with the purchasing, packaging, and shipping of the marijuana, and selling the marijuana in Kansas. *Id.* The charges levied against Dahda and his co-conspirators alleged a conspiracy to distribute in excess of 1,000 kilograms of marijuana. *Id.*

[9] *Id.*

[10] *Id.* at 1111.

[11] *Id.* at 1112.

[12] *Id.* at 1111.

[13] *Id.* at 1105.

al intent underlying Title III because both definitions are overly broad and do not accomplish Congress's goals for the statute.[14] Part I of this Comment presents an overview of Title III and its provisions, and outlines the state of the law prior to *Dahda*.[15] Part II examines and discusses the Tenth Circuit's *Dahda* decision and how the court analyzed Title III and the specific term "mobile intercept device," and ultimately arrived at its definition.[16] Part II additionally considers the *Dahda* concurrence.[17] Part III argues that neither court has accounted for technological changes in formulating its definition for "mobile interception device" and that a more narrow definition would better serve the congressional intent underlying the statute.[18]

I. TITLE III: LEGAL FRAMEWORK PRE-*DAHDA*

Title III permits law enforcement officers to apply for, and courts to issue, authorizations to intercept telephone communications using wiretaps or other means of interception.[19] To obtain a wiretap authorization order under Title III, an application must be filed with the court.[20] This application must contain the applicant's identifying information and the facts and circumstances justifying the wiretap, including the nature and location of the facilities from which, or the place where, the communications are to be intercepted.[21] Upon review of the application, a judge may enter an ex parte order authorizing the requested wiretap within the territorial jurisdiction of the court in which the judge is sitting.[22] In most cases, judges may only author-

---

[14] *See infra* notes 114–145 and accompanying text.

[15] *See infra* notes 19–48 and accompanying text.

[16] *See infra* notes 49–113 and accompanying text.

[17] *See infra* notes 109–113 and accompanying text

[18] *See infra* notes 114–145 and accompanying text.

[19] 18 U.S.C. §§ 2516(1), 2518(1) (2012). Section 2516(1) authorizes specific law enforcement personnel to file an application seeking authorization for the Federal Bureau of Investigation (or other responsible federal agency) to intercept wire or oral communications. *See id.* § 2516(1). Section 2516(1) further authorizes federal judges to approve such applications in conformity with Section 2518. *See id.* Section 2518 details the procedure by which law enforcement must make an application and the procedure by which the judge reviews, approves, and issues an order authorizing the requested interceptions. *See id.* § 2518.

[20] *Id.* § 2518(1) (requiring an application for an order authorizing or approving the interception of a wire, oral, or electronic communication to be made in writing to a judge).

[21] *Id.* § 2518(1) (detailing what information must be included in the application for a wiretap authorization order). Further information that must be contained in the application includes other investigative procedures (if any) used and their success or failure, the period of time for which the interception is required to be maintained, statement of the facts concerning all previous applications known to the applicant related to the same persons, facilities, or places specified, and, if applicable, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of failure to obtain such results. *See id.*

[22] *Id.* § 2518(3). An ex parte order is a judicial order issued in the presence of only one party and without opposition from the adverse party. *See Ex Parte*, BLACK'S LAW DICTIONARY (10th ed. 2014).

ize wiretaps where the interception takes place within the judge's territorial jurisdiction.[23]

The term "intercept" under Title III is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device".[24] Title III does not define *where* an interception takes place, leaving open the question of whether interception occurs at the site where the telephone is being wiretapped or at the site where law enforcement hears the communications.[25] In the 1992 case *United States v. Rodriguez*, however, the Second Circuit held that interception takes place in both locations—at the site of the phone and at the site of hearing.[26] Relying on *Rodriguez*, a court could issue a wiretap authorization order allowing law enforcement to listen to communications within the judge's territorial jurisdiction, even though the wiretapped device may be outside the judge's territorial jurisdiction.[27]

Title III specifically includes an exception allowing for interceptions outside of a judge's territorial jurisdiction, provided that the order limits those interceptions to instances involving a "mobile interception device."[28] As with the term "intercept," the statute does not define "mobile interception device."[29] The seminal case defining "mobile interception device," until recently, was the 1997 Seventh Circuit decision in *United States v. Ramirez*.[30] In *Ramirez*, the Seventh Circuit concluded that the term described a device that intercepts mobile communications, such as a device designed to intercept

---

[23] 18 U.S.C. § 2518(3); *see* United States v. Dahda, 853 F.3d 1101, 1111 (10th Cir. 2017). Judges may issue orders authorizing interception outside of their territorial jurisdiction in the event that law enforcement plans to use a mobile interception device. *See* 18 U.S.C. § 2518(3). The statute is silent on the definition of mobile interception device. *See id.* As will be discussed in the remainder of this comment, at least two United States Circuit Courts of Appeal have written opinions containing their respective definitions for mobile interception device, though the definitions are divergent.[See supra note 4?] *Compare Dahda*, 853 F.3d at 1104 (limiting the definition of interception devices to those devices that are mobile), *with* United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997) (defining devices for intercepting mobile communications more broadly).

[24] 18 U.S.C. § 2510(4).

[25] *See* United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992). Interception consists of two parts: where the device used acquires the content of the message being intercepted (e.g. where a traditional wiretap receives a signal through a phone line) and where the law enforcement official hears the contents of the message acquired through the device. *See id.*

[26] *Id.* (holding that because the definition of "intercept" under Title III includes actually hearing the message, the interception must also be considered to occur at the place where the contents of the message being intercepted are heard).

[27] *See id.* at 132, 136 (upholding the denial of the defendant's motion to suppress wiretap evidence obtained in New Jersey by agents in New York authorized by a New York magistrate judge).

[28] 18 U.S.C § 2518(3).

[29] *Id.* § 2510.

[30] *Ramirez*, 112 F.3d at 853.

mobile phone calls.[31] Under *Ramirez*, the statutory exception accordingly applied where a judge issued a wiretap authorization order allowing for interception of communications originating from a mobile phone.[32] Moreover, the limitation carried no further jurisdictional limitations.[33]

The definitions and legal framework above carry particular importance when analyzing the availability of suppression as a remedy under Article III.[34] Suppression is available as a remedy in cases where, (1) a communication was unlawfully intercepted, (2) a facially insufficient order authorized the interception, or (3) an interception occurred that was not in conformance with the order authorizing it.[35]

With regard to the first category, Article III expressly forbids, except in a narrow band of circumstances, the interception of wire, oral, or electronic

---

[31] *Id.* One modern and controversial device fitting this definition is the class of devices called StingRays. *See generally* Linda Lye, *New Docs: DOJ Admits That StingRays Spy on Innocent Bystanders*, ACLU N. CAL. (Oct. 28, 2015), https://www.aclunc.org/blog/new-docs-doj-admits-stingrays-spy-innocent-bystanders [https://perma.cc/X5F3-PV3U]. Public documents obtained by the ACLU indicate that some stingray devices may have the functionality to intercept wireless communications. *See* Documents Obtained by ACLU Pursuant to FOIA Request, ACLU N. CAL. 11, https://www.aclunc.org/docs/20151027-crm_lye.pdf [https://perma.cc/W4PH-TYML] [hereinafter StingRay Documents]. These StingRay devices, if possessing the functionality to intercept wireless communications, would not be subject to the territorial restrictions of Section 2518(3) under the Seventh Circuit's definition for mobile interception device. *See Ramirez*, 112 F.3d at 853; *see also* StingRay Documents, *supra*, at 11 (claiming that digital analyzers/cell site simulators/triggerfish and similar devices, like the StingRay, may be able to intercept the contents of wireless communications if the function is not disabled). This definition, therefore, could lead to the widespread use of a controversial piece of technology by placing it within the statutory exception. *See Ramirez*, 112 F.3d at 853.

[32] *See Ramirez*, 112 F.3d at 853 (holding that the orders fell within the exception under Title III, because a mobile interception device is a device used to intercept mobile communications and the wiretap authorization order authorized interception of communications from a mobile phone).

[33] *See id.* ("[S]o understood [the definition for mobile interception device] authorized the district judge in the Western District of Wisconsin to order a tap on the phone . . . regardless of where the phone or listening post was.").

[34] *See* 18 U.S.C. § 2518(10) (providing suppression as a remedy).

[35] *Id.* § 2518(10)(a); *see, e.g.*, United States v. Giordano, 416 U.S. 505, 525, 533 (1974) (affirming grant of motion to suppress and holding that communications were unlawfully intercepted where the Attorney General's executive assistant approved the application); United States v. Lomeli, 676 F.3d 734, 742 (8th Cir. 2012) (affirming district court's grant of motion to suppress evidence obtained by wiretap and holding that wiretaps were made unlawfully where applications for authorization did not identify the law enforcement officers authorizing the applications); State v. Mazzone, 648 A.2d 978, 987–88 (Md. 1994) (vacating Court of Special Appeals' judgment denying motion to suppress and holding that failure to minimize interception is tantamount to intercepting beyond the scope of an authorization). Suppression is a remedy by which the court stops certain evidence from being introduced at trial. *Suppress*, BLACK'S LAW DICTIONARY (10th ed. 2014). In cases under Title III, suppression prevents the introduction at trial of content from wrongfully intercepted communications. *See, e.g.*, *Giordano*, 416 U.S. at 509 (noting that suppression hearings began when the government announced that it would use intercepted communications).

communications.[36] Therefore, any person who intercepts a communication and is not otherwise authorized by Title III has done so unlawfully, rendering the intercepted communication vulnerable to suppression.[37] Second, Article III sets forth specific requirements for orders authorizing the lawful interception of communications.[38] Orders issued by courts that do not satisfy these requirements are deemed facially invalid.[39] Communications intercepted pursuant to a facially invalid order are similarly susceptible to suppression.[40] Finally, otherwise lawful interceptions performed after issuance of a facially valid order, but intercepted in a manner that is not in conformity with the wiretap authorization order, could be suppressed.[41]

An aggrieved party may assert any of the defects above and move for suppression, but bears the burden of proving the defect.[42] If the burden is met, the analysis then proceeds to a second step in which the court determines whether or not suppression is appropriate based on the nature of the defect.[43] If a court decides that the defect interferes with the implementation of the congressional intent of Article III, suppression may be the appropriate remedy.[44] The legislative history of Title III reveals the goals of the statute and provides examples of how Title III accomplishes such goals.[45] Its two

---

[36] 18 U.S.C. §§ 2511(1), 2516.

[37] *Id.* §§ 2511(1), 2516, 2518(10); *see, e.g.*, *Lomeli*, 676 F.3d at 742 (affirming grant of defendant's motion to suppress and holding that wiretap authorization applications that did not identify the law enforcement officer who approved the application violated the statutory requirements under Section 2518(1)).

[38] *See* 18 U.S.C. § 2518(1)–(4) (detailing the procedure by which law enforcement files its application and the authorizing judge reviews and approves or denies the application).

[39] *See Dahda*, 853 F.3d at 1114 (holding that a wiretap authorization order that violated Title III's territorial jurisdiction restriction was facially insufficient).

[40] 18 U.S.C. § 2518(10)(a)(ii).

[41] *Id.* § 2518(10)(a)(iii)

[42] United States v. Radcliff, 331 F.3d 1153, 1160 (10th Cir. 2003) (citing United States v. Mitchell, 274 F.3d 1307, 1309 (10th Cir. 2001)) (holding that wiretap authorizations carry a presumption of validity and the defendant bears the burden of rebutting this presumption).

[43] *See Giordano*, 416 U.S. at 527 (requiring suppression only where the defect is related to one of "those statutory requirements that directly and substantially implement[s] the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device").

[44] *See id.*; *see also Radcliff*, 331 F.3d at 1162 (holding that the rule requiring suppression only where a defect is related to a requirement directly and substantially implementing the congressional intent underlying the statute, as established in *Giordano*, applies to facially insufficient authorization orders or approvals as well).

[45] *See* S. REP. NO. 90-1097, at 2153 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153. Congress passed Title III primarily for the dual purposes of protecting the privacy of wireless communications and creating a uniform set of circumstances and conditions under which interception of wireless communications may be authorized. *Id.* Furthermore, Congress sought to ensure that the authority to authorize applications for the use of wiretapping was centralized as much as possible in a publicly responsible official subject to the political process. *Id.* at 2185. Centralization in politically-accountable public officials ensured that the public would be able to identify the official responsible if abuses of the wiretap authority began to occur. *Id.* With the threat of the

primary goals are to protect the privacy of oral and wire communications and to establish a consistent set of circumstances under which wiretaps may be authorized.[46] Title III, however, does not explicitly identify which requirements meaningfully implement these goals.[47] Accordingly, it has thus far fallen to the courts to differentiate technical defects from defects undermining the purpose of the statute.[48]

II. THE TENTH CIRCUIT BREAKS WITH THE SEVENTH CIRCUIT IN *UNITED STATES V. DAHDA*

In 2017, in *United States v. Dahda*, the U.S. Court of Appeals for the Tenth Circuit reviewed the denial of the defendant's motion to suppress intercepted communications presented as evidence against him at trial.[49] To determine whether the motion was appropriately denied, the court analyzed the denial in two steps.[50] First, the court decided that the orders authorizing the intercepted communications were facially deficient.[51] The court ultimately concluded, however, that the facial deficiency was technical in na-

---

political process hanging over their heads, Congress hoped that law enforcement officials would be sufficiently deterred from abusing wiretap authority. *See id.*

[46] *Id*. at 2185. The legislative history also states that Title III was intended to delineate on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. *Id.*

[47] *See generally* 18 U.S.C. §§ 2510–2520 (covering the entire text of Title III). Section 2518 in particular contains a large number of requirements for applications for and authorizations of wiretap approvals. *See Id*. at § 2518. None of these requirements, however, are explicitly identified as more important than the others and a large body of case law has arisen around what constitutes a material defect as opposed to a technical defect. *See, e.g.*, *Lomeli*, 676 F.3d at 742 (affirming the district court's grant of motion to suppress evidence obtained by wiretap and holding that wiretaps were made unlawfully where applications for authorization did not identify the law enforcement officers authorizing the applications); *Radcliff*, 331 F.3d at 1162–63 (holding that omission of the requesting official's name from the authorization order was a technical defect that did not disrupt the purpose of the statute and therefore suppression was not required).

[48] *See Radcliff*, 331 F.3d at 1162–63 (holding that omission of the requesting official's name from the authorization order was a technical defect that did not disrupt the purpose of the statute and therefore suppression was not required).

[49] United States v. Dahda, 853 F.3d 1101, 1111 (10th Cir. 2017).

[50] *Id.* at 1114. This two-part analysis is consistent with the history of cases related to Section 2518(10). *See, e.g.*, United States v. Giordano, 416 U.S. 505, 527 (1974) (holding that suppression is only appropriate where an identified defect relates to a requirement that directly and substantially carries out the congressional intent underlying Title III); United States v. Radcliff, 331 F.3d 1153, 1162 (10th Cir. 2003) (holding that the rule limiting suppression as a remedy to defects related to requirements that directly and substantially carry out the congressional intent underlying Title III applied to suppression for facial insufficiency as well as illegal interceptions).

[51] *Dahda*, 853 F.3d at 1114 The orders were facially insufficient because they authorized law enforcement to use stationary listening posts located outside the authorizing court's territorial jurisdiction to intercept calls from mobile phones also located outside the authorizing court's territorial jurisdiction. *Id.* This holding was written in light of the newly adopted definition for mobile interception device as an interception device that is mobile—a categorization that excludes stationary listening posts. *See id.*

ture and did not undermine the congressional intent behind Title III.[52] In so concluding, the Tenth Circuit declined to adopt the definition for "mobile interception device" adopted previously by the Seventh Circuit.[53] Section A of this Part discusses the Tenth Circuit declining to adopt the Seventh Circuit's definition for "mobile interception device" and why this led to the conclusion that the authorization orders were facially deficient.[54] Section B of this Part discusses the court's conclusion that, despite the facial deficiency, suppression was not an appropriate remedy.[55] Section C of this Part discusses the *Dahda* concurrence and its focus on Title III's age, evolving technology, and the need for Congress' attention to bring it into modernity.[56]

A. The Tenth Circuit's Analysis

Prior to trial, Dahda moved to suppress communications intercepted pursuant to nine wiretap authorization orders issued by the U.S. District Court for the District of Kansas.[57] The primary challenge to these orders contended that the orders authorized interception outside the bounds of the court's territorial jurisdiction in violation of Title III.[58] The analysis to determine whether the orders were facially insufficient involved a two-step inquiry: whether the orders permitted interception outside the court's territorial jurisdiction and, if so, whether the orders limited such interception to instances involving a mobile interception device.[59]

The court disposed of the first question—whether the orders exceeded the district court's territorial jurisdiction—by relying on the definition provided by Title III for intercept, paired with an earlier decision discussing how to determine where interception has taken place.[60] The Tenth Circuit, in the 1994 case *United States v. Tavarez*, interpreted the Oklahoma counterpart to Title III and held that interception occurs both where the tapped telephone is located and where the intercepted communications are first

---

[52] *See id.* at 1116. The court reviewed the legislative history, noting several examples of how Congress carried out its intent in the construction of the statute, though none of the examples indicated that the territorial limitation was significant to the congressional intent. *Id.* at 1114–15.

[53] *Id.* at 1114. The Seventh Circuit defined mobile interception device as a device used to intercept mobile communications. United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997).

[54] *See infra* notes 57–92 and accompanying text.

[55] *See infra* notes 93–108 and accompanying text.

[56] *See infra* notes 109–113 and accompanying text.

[57] Dahda, 853 F.3d at 1111.

[58] *Id.*; *see* 18 U.S.C § 2518(3) (allowing a judge to enter an ex parte order authorizing or approving interception of communications within the territorial jurisdiction in which the judge sits, or outside that jurisdiction in the case of a mobile interception device).

[59] *Dahda*, 853 F.3d at 1114.

[60] *Id.* at 1112 (citing United States v. Tavarez, 40 F.3d 1136, 1138 (10th Cir. 1994)). The definition for intercept under Title III includes acquiring the contents of a phone call using a device. *See* 18 U.S.C. § 2510.

heard by law enforcement.[61] In *Dahda,* the court concluded that the language of the orders lacked geographic restrictions on both the locations of the cell phones and the locations of the listening posts to be used.[62] The orders therefore violated the statutory limitation on territoriality.[63]

The inquiry, however, moved on to the issue of whether these orders triggered the "mobile interception device" exception.[64] This question necessarily depended on the definition of "mobile interception device," which is not defined by Title III.[65] The court offered three possibilities for the necessary definition: (1) a listening device that is mobile; (2) a cell phone that is being intercepted; or (3) a device that intercepts mobile communications, such as cell phone calls.[66] The analysis began with the plain meaning of the statutory language, with an eye toward whether the plain meaning would conflict with the legislative history.[67]

The court began by considering the language of Title III itself and relied on grammatical structure to determine the plain meaning.[68] The court noted that the word "mobile" was an adjective, modifying the noun "interception device," and thus concluded that the plain meaning of the phrase referred to the mobility of the device used to facilitate the interception.[69]

---

[61] *Tavarez*, 40 F.3d at 1138; *see Dahda*, 853 F.3d at 1112. The Tenth Circuit in *Dahda* goes on to demonstrate the parallels between the Oklahoma statute and Title III, such as the definitions for "intercept" and "aural communication." *Dahda*, 853 F.3d at 1112. The holding that interception takes place both at the place that the tapped telephone is located and at the place that law enforcement hears the communication is widely accepted and has been adopted by every circuit to hear the issue. *See, e.g.*, United States v. Jackson, 849 F.3d 540, 551–52 (3d Cir. 2017) (holding that the definition of interception includes the location of the listening post and concluding that because the listening post at issue was within Pennsylvania that the interception was lawful); United States v. Henley, 766 F.3d 893, 911, 912 (8th Cir. 2014) (holding that the definition of "intercept," in referencing "aural" acquisition, necessarily encompasses the place where the redirected contents of the communication are first heard); United States v. Luong, 471 F.33d 1107, 1109 (9th Cir. 2006) (holding that the most logical interpretation of the definition of interception is that it occurs both where the phone is located and where law enforcement overhears the call); United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (concluding that an interception occurs in the jurisdiction where the tapped phone is located, where the second phone in the conversation is located, and where the scanner used to overhear the call is located).

[62] *Dahda*, 853 F.3d at 1112.

[63] *Id.* The exact wording of the orders authorized interception to take place in any other jurisdiction within the United States if the cell phones to be tapped were transported outside the territorial jurisdiction of the court. *See id.*

[64] *Id.*; *see* 18 U.S.C. § 2518(3).

[65] *See* 18 U.S.C § 2510 (defining terms of art for Title III but not defining "mobile interception device").

[66] *Dahda*, 853 F.3d at 1112–13.

[67] *Id.* at 1113 (quoting Starzynski v. Sequoia Forest Indus., 72 F.3d 816, 820 (10th Cir. 1995))

[68] *Id.*

[69] *Id.*; *see also* United States v. North, 735 F.3d 212, 218 (5th Cir. 2013) (DeMoss, J., concurring) (noting that, on its face, "mobile interception device" appears to refer to whether or not the device used to intercept communications is mobile, not whether the taped phone is mobile).

Proceeding to the second possible interpretation—a cell phone that was being intercepted—the court dismissed it as contrary to the intent of Title III.[70] Because the statute defined a device as something used to intercept a call, the court held that it would be contradictory to define "mobile interception device" as the cell phone being intercepted.[71]

Finally, the court addressed the third possible interpretation—a device used to intercept mobile communications—which was also the interpretation that the Seventh Circuit adopted in *United States v. Ramirez* in 1997.[72] The Tenth Circuit turned, as with the first interpretation, to the grammatical construction of the phrase, concluding that the third interpretation would require the court to rewrite the statute.[73]

The Seventh Circuit in *Ramirez* declined to adopt the plain meaning of the phrase "mobile interception device," concluding that it seemed inapplicable in context.[74] Under the literal meaning of the phrase, obtaining facially sufficient orders to tap cell phones becomes a function of chance rather than prudent investigation.[75] Because cell phones are meant to be mobile, the Seventh Circuit reasons that they are likely, at some point, to be carried out of the territorial jurisdiction of the district in which the crime is being investigated.[76] Therefore, if law enforcement officers wished to use a stationary listening post outside of the district to maximize the chances of interception, they would be required to obtain subsequent orders authorizing wiretaps in other districts.[77] The Seventh Circuit concluded that a literal reading of the phrase "mobile interception device" imposed illogical limitations on law enforcement's ability to practically investigate crimes using wiretaps.[78]

---

[70] *Dahda*, 853 F.3d at 1113.

[71] *Id.*

[72] *Id.*; *Ramirez*, 112 F.3d at 853.

[73] *Dahda*, 853 F.3d at 1113. The court again referred to the term "mobile" as an adjective and "interception" and "device" as nouns. *Id.* The court concluded, considering the words' roles in the phrase, that "mobile" must modify "interception," "device," or both. *Id.* The third interpretation, however, uses "mobile" to modify "telephone," which is not present in the phrase in question. *Id.*

[74] *Ramirez*, 112 F.3d at 852.

[75] *Id.*

[76] *Id.*

[77] *See id.* (noting that the literal interpretation would mean that "if . . . the listening post is stationary and is for practical reasons to be located outside the district in which the crime is being investigated and the cellular phone is believed to be located, the government . . . must obtain the wiretap order from the district in which the listening post is located, even though that location is entirely fortuitous from the standpoint of the criminal investigation").

[78] *Id.* The Seventh Circuit observed that the literal statutory language would: (1) forbid a judge in State 1 from authorizing use of a stationary listening post located in State 2 to intercept calls from a phone located in State 2; (2) allow a judge in State 1 to authorize use of a stationary listening post in State 2 to intercept calls from a phone in State 1; (3) allow a judge in State 1 to authorize use of a stationary listening post in State 1 to intercept calls from a phone anywhere. *See*

The Seventh Circuit concluded further that the legislative history of Title III indicated that the term "mobile interception device" should have a broader meaning than the limited literal definition.[79] The legislative history indicates that the provision allowing for "mobile interception devices" applies equally to a physical bug planted on a car and to taps on phones in the car.[80] Because there is no specific reference or limitation to vehicles within Title III, the court concluded that the examples in the legislative history were offered as inclusive illustrations of mobile interception devices rather than exclusive definitions.[81] The court reasoned that a device planted in a car is not a "mobile interception device" because the device itself is stationary.[82] Likewise a tap on a phone is not placed on the phone, rather on a telephone line through which the phone's communications are transmitted.[83] Therefore, the court held that the emphasis in "mobile interception device" is on the mobility of the communications rather than on the devices used to intercept them.[84] Thus the Seventh Circuit defined "mobile interception device," in the context of legislative history, as a device used to intercept mobile communications.[85] The Seventh Circuit further held that the literal interpretation would not serve the legislative intent to protect the privacy of communications because it does nothing to prevent law enforcement from

---

id. In the Seventh Circuit's opinion, this system relied too heavily on chance to be consistent with the congressional goal of establishing a uniform system for the authorization of wiretap orders. *See id.*

[79] *Id.*

[80] *See id.* (quoting S. REP. NO. 99-541, at 30 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3584). Congress recognized the possibility that in either of these cases the vehicle is likely to move, at some point, out of the authorizing judge's territorial jurisdiction. S. REP. NO. 99-541, at 30. Such a change in location would not be problematic, provided the device was installed in the authorizing judge's territorial jurisdiction. *Id.* Where the vehicle is moved prior to installation, installation may not occur until the vehicle is returned to the issuing judge's territorial jurisdiction. *Id.*

[81] *Ramirez*, 112 F.3d at 852.

[82] *Id.* at 852–53.

[83] *Id.* at 853. In *Ramirez*, a judge in the District Court for the Western District of Wisconsin authorized law enforcement to intercept mobile phone calls made from a cell phone in the possession of a co-conspirator who traveled back and forth from Wisconsin to Minnesota. 112 F.3d at 851. The listening post was then set up in Minnesota for practical reasons: law enforcement was fearful that they would be recognized in the defendant's hometown. *Id.* After tapping the phone, law enforcement discovered that the user of the phone they had tapped was not who they believed it would be previously, and that the actual user of the phone never left Minnesota. *Id.* Thus, no part of the interceptions took place in the issuing judge's territorial jurisdiction triggering the need to examine the exception under Title III. *See id.*; 18 U.S.C. § 2518(3).

[84] *Ramirez*, 112 F.3d at 853.

[85] *Id.* With this definition established, the Seventh Circuit went on to conclude that the order issued by the district court in Wisconsin was within the exception under Title III because they authorized interception of mobile communications, even though both the listening post and the phones used for the communications were located outside the court's territorial jurisdiction. *Id.*

seeking the necessary orders in other courts.[86] Rather, the literal definition would only serve to complicate law enforcement efforts.[87]

The Tenth Circuit in *Dahda*, however, held the opposite view.[88] In addressing the legislative history, the court concluded that the illustrations provided lent further support to the plain language of the statute.[89] Both examples depicted in the legislative history are interception devices that are mobile, bringing them in line with the plain language of the phrase.[90] In keeping with the interpretive canon adopted, the court held that, because the plain meaning is not demonstrably at odds with the legislative history, they were unable to interpret the statute differently.[91] Therefore, because the orders in question authorized interception of cell phones using a stationary listening post, all of which were located outside of the court's jurisdiction, the orders were facially insufficient under Title III.[92]

B. Suppression as a Remedy After Defining "Mobile Interception Device"

Facial invalidity in itself does not justify suppression as a remedy.[93] Rather, suppression requires that the deficient element directly and substantially carries out the congressional intent behind the statute.[94] By analyzing the legislative history behind Title III, the court sought to determine whether the territorial limitation substantially implemented Congress's intent.[95] The Tenth Circuit extracted two primary goals from the legislative history: protecting the privacy of communications and creating a uniform set of circumstances and conditions under which interception may be authorized.[96]

---

[86] *Id.* As discussed above, the literal meaning of the term is an interception device that is, itself, easily movable. *See id.* at 852. Had the district court adhered to the literal definition, law enforcement could have sought the same order in Minnesota and likely obtained it, though this would necessitate another application process. *See id.* at 853.

[87] *Id.* at 853.

[88] *Dahda*, 853 F.3d at 1114.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017) (quoting United States v. Foy, 641 F.3d 455, 463 (10th Cir. 2011)).

[94] *Id.* (quoting United States v. Giordano, 416 U.S. 505, 527 (1974)); *see* United States v. Radcliff, 331 F.3d 1153, 1162 (10th Cir. 2003) (extending the second step in the analysis to apply to suppression sought under Section 2518(10(a)(ii)).

[95] *Dahda*, 853 F.3d at 1114–15. Prior to the decision in *Dahda* two courts had analyzed the same issue, coming out on opposite sides. *Compare* Adams v. Lankford, 788 F.2d 1493, 1500 (11th Cir. 1986) (holding that violating the territorial restriction under Title III does not implicate Congress's core concerns underlying the statute), *with* United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013) (holding that the territorial restriction is a core concern of Title III).

[96] *Dahda,* 853 F.3d at 1114–15 (citing S. REP. NO. 90-1097, at 2153 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153).

The court found in the legislative history two examples of how Title III protects the privacy of communications.[97] First, Congress limited lawful interception to certain law enforcement officers' investigation of a particular set of crimes, to ensure that wiretaps would be used only in circumstances warranting them.[98] Second, Congress created a "probable cause" evidentiary burden that must be overcome before a wiretap may be authorized.[99]

The territorial limitation was not identified as one of the limitations directly protecting privacy.[100] Therefore, the Tenth Circuit held that the territorial limitation under Title III did not substantially implement Congress's goal to protect the privacy of wire and oral communications.[101]

The court continued its analysis by addressing the second legislative goal of establishing uniformity in authorizations for wiretaps.[102] Congress sought to centralize wiretap decisions with the chief prosecuting officers in the state in which the wiretap is sought.[103] The goal of this centralization was to place responsibility for wiretaps in the hands of publically and politically accountable officials who would bear the consequences of any abuse of the method.[104] The court concluded that not only did the territorial limitation fail to substantially implement this goal, it also may have detracted from it by requiring cooperation of multiple prosecutors in multiple jurisdictions during the course of an investigation.[105] If multiple prosecutors became involved, the clear lines of responsibility Congress envisioned would become muddled.[106] Indirect lines of responsibility would make it more dif-

---

[97] *Id.*

[98] *See generally* S. REP. NO. 90-1097, at 2153 (detailing the legislative intent behind Title III, its purposes, and its development).

[99] *See Dahda*, 853 F.3d at 1115 (citing S. REP. NO. 90-1097, at 2153). In placing this evidentiary burden on those seeking wiretap authorizations, Congress sought to deter law enforcement from filing frivolous applications that would needlessly interfere with the privacy of wireless communications. *See* S. REP. NO. 90-1097, at 2153. Furthermore, a uniform evidentiary burden furthers the congressional goal of ensuring that wiretap authorization applications are made for a consistent set of circumstances under which the surveillance measure is justified. *See id.*

[100] *Dahda,* 853 F.3d at 1115.

[101] *Id.* at 1115, 1116; *see* United States v. Chavez, 416 U.S. 562, 578 (1974) (holding that the absence of legislative history concerning certain Title III provisions contributed to a finding that a statutory violation did not warrant suppression).

[102] *Dahda*, 853 F.3d at 1115.

[103] *Id.* (citing S. REP. NO. 90-1097, at 2187).

[104] S. REP. NO. 90-1097, at 2185. Centralization of the decisions in approving applications for wiretap authorizations also avoids the possibility of divergent practices among law enforcement officials. *Id*. Because another goal for this legislation is delineating a uniform basis for the application for and approval of wiretap authorizations divergent practices would significantly undermine this core aspect of Title III. *Id.* at 2153, 2185.

[105] *Dahda*, 853 F.3d at 1115 (citing *Adams*, 788 F.2d at 1499).

[106] *See* S. REP. NO. 90-1097, at 2185 (noting that the statute was designed to provide clear lines of responsibility to identifiable law enforcement officers).

ficult to hold officials accountable for abuses of the wiretap authority.[107] Therefore, because the legislative history did not identify the territorial limitation as central to the implementation of Congress's intent, the Tenth Circuit concluded that suppression was not required.[108]

C. Judge Lucero's Concurrence

Judge Lucero's concurrence is primarily a cautionary note and a call to action, warning that technology has significantly surpassed the wording of Title III.[109] Exploring the legislative history used throughout the majority opinion, Judge Lucero criticized the statute as "trapped in history" and intended only to cover situations in which a phone being monitored leaves the original jurisdiction.[110] It appeared to Judge Lucero that Congress envisioned that law enforcement would need to affix a physical device on mobile phones to monitor their calls.[111] As Judge Lucero notes, however, evolving technology has enabled law enforcement to monitor phone calls without such physical device, thus rendering Congress's presumption from the 1960's inaccurate.[112] In light of this evolved technology, Judge Lucero called Congress to action in updating the language of the statute to more closely reflect current technology.[113]

III. KEEPING UP WITH THE TECHNOLOGY: BOTH CIRCUITS FAIL TO ADDRESS THE MODERN CONTEXT

The differing definitions for "mobile interception device" highlight the tension between the statute's purpose, language, evolving technology, and

---

[107] *Id*. Congress likely placed such high value on accountability for law enforcement officials due to their vulnerability to the political process, as opposed to appointed judges who are generally insulated from the same forces. *Id.*

[108] *Dahda*, 853 F.3d at 1116. The defendant argued that the territorial limitation was important in thwarting forum shopping by law enforcement and reduced opportunities to choose forums where an application is more likely to be approved. *Id.* at 1115. The court was not persuaded. *Id.* The court reasoned that law enforcement seeking approval in a specific court would only need to use a mobile interception device—defined a few paragraphs earlier in the decision as a mobile device to intercept communications—or using a listening post in the preferred forum's territorial jurisdiction. *Id.* Therefore, the territorial limitation does not meaningfully curb the danger of forum shopping. *Id.*

[109] *Id,* at 1118 (Lucero, J., concurring).

[110] *Id.*at 1118–19.

[111] *Id.* at 1119.

[112] *Id.*

[113] *See id.* (agreeing with the majority that the statutory text need not be tortured to apply to all calls placed from a mobile phone, but indicating that it is for Congress to update Title III to account for modern devices if it so chooses).

judicial response to such evolutions in technology.[114] The U.S. Court of Appeals for the Tenth Circuit's 2017 decision in *Dahda* creates a circuit split between the Tenth and Seventh Circuits, creating the possibility that the U.S. Supreme Court steps in to resolve it.[115] Yet neither circuit has directly addressed what is, perhaps, the central issue: the fact that technology has infinitely outpaced the evolution of wiretap regulation and has left the "quaint language" of the statute in its dust.[116] With the prevalence of mobile phones in modern times, it is abundantly clear that Title III is in need of an overhaul.[117] This Part considers the reasoning in both *Ramirez* and *Dahda* and concludes that the reasoning falls short of considering the broader technological context within which these cases and their accompanying criminal investigations occurred.[118]

The Seventh Circuit adopts a definition that would potentially make every call made over a cell phone vulnerable to a wiretap if either caller is involved in a criminal investigation under Title III.[119] Thus, under the Seventh Circuit's definition, the territorial restriction's applicability turns solely on whether the intercepted communications are placed from a mobile phone.[120] In a modern context, this holding may prove to be overbroad and may open a significant number of phone calls placed to potential interception without territorial restriction on judges issuing authorizations to do so.[121] Although this definition may fit within the legislative history underly-

---

[114] *Compare* United States v. Dahda, 853 F.3d 1101, 1114 (10th Cir. 2017) (limiting the definition of interception devices to those devices that are mobile), *with* United States v. Ramirez, 112 F.3d 849, 853 (7th Cir. 1997) (defining devices for intercepting mobile communications more broadly).

[115] *See* Wright v. North Carolina, 415 U.S. 936, 937 (1974) (Douglas, J., dissenting) (noting that the Court is the only source for resolution of a split amongst the circuit courts and that it is the Court's obligation to create uniformity in the circuits). *Compare Dahda*, 853 F.3d at 1114 (defining "mobile interception device" as a device used for interception that is mobile), *with Ramirez*, 112 F.3d at 853 (defining "mobile interception device" as a device used to intercept mobile communications).

[116] *See Dahda*, 853 F.3d at 1119 (Lucero, J., concurring).

[117] *See Mobile Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/XSB6-PDUB] (presenting data on cell phone ownership and claiming ninety-five percent of Americans owned a smartphone as of the publishing date on January 12, 2017). According to the Mobile Fact Sheet, the figure of ninety-five percent cell phone ownership represents an increase from sixty-two percent as of October 2002. *See id*.

[118] *See infra* notes 114–145 and accompanying text.

[119] *See Ramirez*, 112 F.3d at 853 (holding a "mobile interception device" is a device used to intercept mobile communications).

[120] *See id.* (holding the emphasis in the phrase falls on the mobility of what is intercepted rather than on the mobility of the chosen device).

[121] *See id.* (holding that wiretap authorization orders authorizing interception of mobile communications originating from outside the court's jurisdiction at a stationary listening post outside the court's jurisdiction were not facially deficient). *See generally Cell Phones and American Adults*, PEW RESEARCH CTR. (Sept. 2, 2010), http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/ [https://perma.cc/VWR5-DYTM] (finding that ninety-five percent of adults

ing Title III, it is unlikely that Congress, in 1968, could have conceived of the prevalence of mobile communications five years before the modern cellphone was patented.[122]

In contrast, the Tenth Circuit in *Dahda* was given the opportunity to revisit the definition for "mobile interception device" with full knowledge of the technological advancements since Title III's passage and the Seventh Circuit's decision in *Ramirez*.[123] The court's decision shifted the question to the definition of "mobile" rather than closing the door entirely.[124] The court identified a bug attached to a car phone as an interception device that is mobile, but does not indicate how far that example stretches.[125]The only attempt to define the term in the opinion comes from distinguishing between mobile interception devices and stationary listening posts.[126] The Tenth Circuit fell victim to the same pitfall as the Seventh Circuit in *Ramirez*—it is unlikely that Congress, more than forty years prior, could have accounted for the evolution of wiretap and other interception technology.[127] In relying on a device's mobility, the Tenth Circuit comes closer to addressing the crux of the matter, but ultimately falls short.[128]

The analysis would be better focused on the impact that these definitions would have on the number of wiretap authorization applications that

---

surveyed that owned cell phones made at least one voice call per day); NAT'L 911 PROGRAM, 2015 NATIONAL 911 PROGRESS REPORT (2016) (showing the prevalence of cell phone calls over wireline calls in terms of number of 911 calls placed). The National 911 Program reported that the percentage of 911 calls originating from cell phones increased by six percentage points from 2013 data. 2015 NATIONAL 911 PROGRESS REPORT, *supra*, at 2. This increase was accompanied by a corresponding decrease in wireline 911 calls, which fell four percentage points from 2013. *Id.*

[122] *See Ramirez*, 112 F.3d at 852–53 (analyzing the legislative history and holding that the examples offered were illustrative rather than definitional and that the phrase was intended to be interpreted broadly rather than literally). *See generally* James Janega, *The Cell Phone (1973)*, CHI. TRIB. (Nov. 1, 2013), http://www.chicagotribune.com/bluesky/series/chicago-innovations/chi-cell-phone-1973-innovations-bsi-series-story.html [https://perma.cc/SUA3-KFJE] (exploring the history of the invention and patenting of the modern cell phone in 1973 by Martin Cooper).

[123] *See Dahda*, 853 F.3d at 1114 (addressing the Seventh Circuit's decision in *Ramirez* and holding that the legislative history does not permit a departure from the plain meaning of the phrase).

[124] *See id.* (holding that a "mobile interception device" is an interception device that is mobile but not defining mobility).

[125] *See id.* (holding that the legislative history underscores the statute's plain language).

[126] *See id.* (concluding that because the authorization orders authorized intercepting mobile calls from cell phones outside the court's territorial jurisdiction to be heard at stationary listening posts outside of the court's territorial jurisdiction, the orders were facially insufficient).

[127] *See id.* at 1119 (Lucero, J., concurring) (concluding that Congress presumed a physical device would need to be attached to monitored phones and indicating that evolving technology has rendered this presumption invalid). *See generally* 18 U.S.C. §§ 2510–2520 (2012) (encompassing the entirety of Title III enacted in 1968, nearly 49 years before the Tenth Circuit's opinion in *Dahda)*.

[128] *See Dahda*, 853 F.3d at 1119 (Lucero, J., concurring) (identifying that the statute is in need of congressional attention and writing separately to address the issue).

would be filed and the number of communications that would be exposed to potential interception.[129] Both the Seventh Circuit and the Tenth Circuit definitions for mobile interception device create broad classes of modern devices that could be used without concern for territorial limitations on the authorizing court by invoking the mobile interception device exception under Title III.[130] By creating broad classes of devices that can circumvent the statutory territorial limitations, both courts have detracted from the primary congressional goals underlying Title III.[131]

First, creating broad classes of devices that are not subject to territorial limitations does not protect the privacy of communications.[132] Such broad definitions subject a significantly greater number of communications to possible interception.[133] Privacy is reduced rather than protected if more

---

[129] *See* Lye, *supra* note 31 (discussing the controversial StingRay device and its potential use in intercepting mobile communications); *Mobile Fact Sheet*, *supra* note 117, at 1 (showing the increase over time of cell phone ownership and usage in the United States).

[130] *See* 18 U.S.C. § 2518(3) (limiting a judge's ability to authorize interception outside the court's territorial jurisdiction to cases involving the use of a mobile interception device); *Dahda*, 853 F.3d at 1114 (defining mobile interception device as an interception device that is mobile); *Ramirez*, 112 F.3d at 853 (defining mobile interception device as a device used to intercept mobile communications). The Tenth Circuit's definition appears only to distinguish between the use of a stationary listening post and any other interception device. *See Dahda,* 853 F.3d at 1114. The Seventh Circuit's definition is even broader, distinguishing only between devices used to intercept wireless and wired communications, a distinction that is becoming more meaningless as cellular phones become more prominent. *See Ramirez*, 112 F.3d at 853. *See generally* 2015 NATIONAL 911 PROGRESS REPORT, *supra* note 121, at 2 (detailing the increase in cellular phone calls and the corresponding decrease in wired telephone calls).

[131] *See Dahda*, 853 F.3d at 1114 (limiting the definition of interception devices to those devices that are mobile); *Ramirez*, 112 F.3d at 853 (defining devices for intercepting mobile communications more broadly); S. REP. NO. 90-1097, at 2154 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154. Congress recognized in 1968 that technological advances had already made the prevalent use of wiretapping possible. S. REP. NO. 90-1097, at 2154. Congress also recognized that these technological developments threatened the privacy of communications. *Id.* This threat and the litigation that had been emerging indicated that the use of interception devices needed limitation. *Id.*

[132] *See* S. REP. NO. 90-1097, at 2154. (expressing concerns about rapidly advancing technology and the possibility that a significant number of communications are already vulnerable to interception).

[133] *See Ramirez*, 112 F.3d at 853. The Seventh Circuit distinguishes mobile communications from non-mobile communications in deciding that a mobile interception device is a device for intercepting mobile communications, but does not define mobile communications explicitly. *See id.* The court does indicate that, under either the narrow literal definition or the broad definition, the government could always seek authorization to intercept cellular phone calls from a stationary listening post within the authorizing court's jurisdiction. *See id.* At the time of the decision in 1997, it could not have been predicted that cellular phone calls would eclipse wired phone calls. *See* 2015 NATIONAL 911 PROGRESS REPORT, *supra* note 121, at 2. Nor could the Seventh Circuit have foreseen the significant advances in interception technology. *See, e.g.*, Lye, *supra* note 31. In 2016, eighty-four percent of interceptions took place via telephone wiretap, the majority of which were placed on cellular phones. *Wiretap Report 2016*, ADMIN. OFFICE U.S. COURTS, http://www.uscourts.gov/statistics-reports/wiretap-report-2016 [https://perma.cc/N8BJ-H3EF].

communications are vulnerable to interception.[134] Therefore, the broad definitions set by the Seventh and Tenth Circuits are at odds with this goal of Title III.[135]

Second, such broad definitions grant law enforcement agencies a high degree of flexibility in how they file applications for wiretap authorizations.[136] Providing for greater flexibility in filing applications for wiretap authorizations conflicts with the second congressional goal for Title III: creating a uniform set of circumstances and conditions for the authorization of interception of communications.[137] A diverse population of mobile interception devices grants law enforcement a variety of options, should the applicant wish to circumvent the territorial limitations under Title III.[138] Both definitions for mobile interception device create broad, flexible standards for obtaining a wiretap authorization order.[139] Broad and flexible standards do not further Congress's second goal underlying Title III: uniformity.[140]

---

[134] *See* S. REP. NO. 90-1097, at 2154 (expressing concern over the vulnerability of communications and recognizing the need to restrict how and when communications are intercepted).

[135] *See Dahda*, 853 F.3d at 1114; *Ramirez*, 112 F.3d at 853; S. REP. NO. 90-1097, at 2153. The Seventh and Tenth Circuits both address congressional intent, but arrive at competing conclusions. *Compare Dahda*, 853 F.3d at 1114 (holding that the narrower, literal interpretation is not at odds with the goals underlying Title III), *with Ramirez*, 112 F.3d at 853 (holding that the narrower, literal interpretation is at odds with the goals underlying Title III thus allowing the court to interpret the phrase more broadly). Neither court addresses the implications of each definition and the potential expansion of the use of mobile interception devices that could follow, thus detracting from privacy protections intended by Congress. *See Dahda*, 853 F.3d at 1114; *Ramirez*, 112 F.3d at 853.

[136] *See Dahda,* 853 F.3d at 1115. The Tenth Circuit addressed the concern of forum shopping and indicated that law enforcement may already forum shop by simply employing an authorized mobile interception device. *Id.* This concern was largely dismissed, however, because the Tenth Circuit held that the territorial limitation did not directly and substantially implement either of Congress' goals in enacting Title III. *Id.*

[137] *See* S. REP. NO. 90-1097, at 2154 (emphasizing the need to limit the use of wiretapping and other forms of interception to a limited set of circumstances and conditions).

[138] *See* 18 U.S.C. § 2518(3); *Dahda*, 853 F.3d at 1115 (concluding that a judge can authorize interception of communications anywhere by permitting law enforcement to use a mobile interception device); *Ramirez*, 112 F.3d at 853 (concluding that the Western District Court of Wisconsin could authorize the tap of the defendant's cell phone, regardless of where the phone was located, from any listening post, regardless of its location).

[139] *See Dahda*, 853 F.3d at 1114 (defining mobile interception device as an interception device that is mobile); *Ramirez*, 112 F.3d at 853 (defining mobile interception device as a device used to intercept mobile communications).

[140] *See Dahda*, 853 F.3d at 1114 (defining mobile interception device as an interception device that is mobile); *Ramirez*, 112 F.3d at 853 (defining mobile interception device as a device used to intercept mobile communications); S. REP. NO. 90-1097, at 2153 (indicating the importance of limiting wiretapping activity only to duly authorized law enforcement agents in a narrow set of circumstances).

A narrower definition for mobile interception device would more effectively implement Congress's goals for Title III.[141] Interpreting the phrase narrowly would restrict the number of devices that could be used to circumvent the territorial limitation and would thus restrict law enforcement's ability to rely on such workarounds.[142] If law enforcement is allowed fewer ways to work around the territorial restrictions within Title III, fewer communications are likely to be vulnerable to interception—meaning that privacy is better protected.[143] Furthermore, careful consideration and a well-defined, narrow category of devices falling within the extraterritorial exception under Title III would ensure that law enforcement looks to the exception only when necessary, creating more uniformity in the way applications are filed.[144]

CONCLUSION

Neither the U.S. Court of Appeals for the Seventh Circuit nor the U.S. Court of Appeals for the Tenth Circuit fully addressed the underlying cause of their circuit split. Both courts attempted to squeeze the square peg of modern technology into the round legislative hole Congress created in 1968. Although the Tenth Circuit's definition likely provided greater protection to the privacy of phone calls, it did not close the loop entirely; it left open the question of the definition of "mobile" while dispensing of the definition of "interception device." Updating a nearly half-century-old piece of technological legislation may be no small task; however, it is a task of paramount importance to ensure the protection of the privacy of mobile communications.

MICHAEL KOCH

Preferred Citation: Michael Koch, Comment, *If Technology Is the Hare, Is Congress the Tortoise? Split Circuits in the Wake of* Dahda, 59 B.C. L. REV. E. SUPP. 45 (2018), http://lawdigitalcommons.bc.edu/bclr/vol59/iss6/45.

---

[141] *See* S. REP. NO. 90-1097, at 2153. Congress expressed substantial concerns related to the widespread use and potential abuse of wiretap technology and the lack of legislation around it prior to Title III's passage in 1968. *See id.* Title III therefore sought primarily to limit the use of wiretapping rather than expand it. *See id*.

[142] *See Dahda*, 853 F.3d at 1115 (addressing the fact that law enforcement has the ability to forum shop by relying on a mobile interception device); *Ramirez*, 112 F.3d at 853 (noting that the narrower definition would complicate law enforcement).

[143] *See* S. Rep. No, 90-1097, at 2154 (indicating that the privacy of communications is threatened by the potential pervasive use of electronic surveillance).

[144] *See id.* at 2185 (expressing the importance of preventing the abuse of wiretaps by law enforcement).