Is the Long Arm of the Law Shrinking? Geographic Boundaries for the Approval of Wiretaps and Bugs and the Shifting Jurisdictional Reach of Federal Judges to Authorize Electronic Surveillance

*By Mike Hurst**

Recent court decisions from around the country are raising serious questions as to the potential jurisdictional limitations on law enforcement in conducting electronic surveillance on cellular telephones and with recording devices (i.e., "bugs") in private places. Specifically, questions have arisen as to whether, for example, a federal judge in State A has the authority to approve a wiretap for the recording of a cellular telephone which, while sometimes within State A, is physically located in State B when the wiretap approval order is signed, and the government's monitoring station of that particular cell phone is located State C. A related question concerns the authority of a federal judge in State A to authorize the installation of a bug in a vehicle or residence located in State B. Until recently, few restrictions were recognized as to a federal judge's power to authorize multi-jurisdictional electronic surveillance orders. However, some federal appellate courts are beginning to find that such authority does not exist, sometimes suppressing evidence obtained from such surveillance when jurisdictional limits have been violated.

Supporters of these recent decisions would argue that such jurisdictional limitations are necessary in order to prevent forum shopping by industrious prosecutors and law enforcement officers. Otherwise, there would be no restriction on an overzealous prosecutor and a rubber stamping judge. On the other hand, opponents of these latest decisions would argue that such jurisdictional restrictions unnecessarily limit law enforcement's ability to adequately fight crime, as criminals do not limit themselves to any specific judicial districts but rather are always on the cutting edge of technological innovations in order to stay one step ahead of the cops. Tying the hands of law enforcement by limiting access to certain judicial officers or causing confusion about the distribution of authority to approve wiretaps would allow criminals to arbitrage the system to their advantage, significantly hampering the ability of law enforcement to investigate and secure the necessary evidence to ultimately obtain convictions. The following article presents some background on the primary statute used to authorize electronic surveillance and the historical interpretation by some federal appellate courts, juxtaposed against recent federal appellate court decisions that turn the traditional thinking about territorial jurisdiction under the statute on its head.

I. Background

The use of wiretaps and evidence obtained from them is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or the "Wiretap Act").[1] Pursuant to Section 2518(1), in order to obtain a wiretap authorization order, a law enforcement officer must file an application with a "judge of competent jurisdiction," which is defined to include "(a) a judge of a United States district court or a United States court of appeals[.]"[2] Section 2518(3) authorizes a judge to approve a wiretap "within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction) [.]"[3] Section 2515 states that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any . . . proceeding . . . if the disclosure of that information would be in violation of this chapter."[4] The statute further states that an:

> [A]ggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[5]

The Seventh Circuit was apparently the first—and until recently was the only—court to address the issues of territorial jurisdiction and the definition of "mobile interception device." In *United States v. Ramirez*, multiple individuals were convicted of conspiring to distribute drugs based on evidence obtained from a wiretap of cellular telephones.[6] Two of the defendants moved to suppress evidence obtained from wiretaps of their phones. The government believed that one of the defendants, Paul Hotchkiss, who lived in Wisconsin but was dealing drugs in Minnesota, was using a cellular phone owned by another defendant, Patrick Flynn, in furtherance of the conspiracy, and that Hotchkiss carried the phone with him as he traveled between the two states dealing drugs. The government obtained a wiretap for the phone from a district judge in the Western District of Wisconsin, where the conspiracy was being investigated and would ultimately be prosecuted. The government set up a listening post for the tapped phone in Minnesota. A few days later, agents realized that the phone was not being used by Hotchkiss but rather by another co-conspirator who did not seem to travel outside of Minnesota but who was using the phone to further the conspiracy with Flynn. The government later applied to the same district judge in the Western District of Wisconsin for an extension of the wiretap, without disclosing that the cell phone and listening post were in Minnesota. The judge granted the extension.[7]

** Mike Hurst is a lawyer in Mississippi and former federal prosecutor. He is known for his work targeting corrupt public officials as an Assistant U.S. Attorney in the Southern District of Mississippi.*

The case was subsequently reassigned to another federal judge. When the defendants filed their motion to suppress, the judge denied it as to evidence obtained under the original wiretap, holding that the order had been approved based upon the government's reasonable and good faith belief that the phone line was being used in the Western District of Wisconsin. However, the judge granted the motion to suppress evidence obtained from the wiretap extension, holding that Title III did not permit a district judge in one district to authorize wiretapping in a different district.[8]

Chief Judge Richard Posner of the Seventh Circuit wrote the opinion for the court and began by stating that "[w]e do not think that the location of the phone affected the legality of the tap[.]"[9] In reviewing the language of Section 2518(3), the court adopted the position of the Fifth and Second Circuits that "[a]n interception takes place both where the phone is located (including, we suppose, although we can find no cases, where the receiving phone is located) and where the scanner used to make the interception is located."[10] In light of this precedent, the court reasoned that a literal interpretation of the statutory language would make very little sense. Such an interpretation would prohibit the actions taken in this case (a Wisconsin judge authorizing a tap of a phone in Minnesota with a government listening post in Minnesota), while allowing a judge in any district where the government sets up a listening post or a district where a mobile listening post is authorized in a particular district but located anywhere in the United States to authorize a wiretap of a phone located anywhere, "even though that location is entirely fortuitous from the standpoint of the criminal investigation."[11]

The court then reviewed the legislative history of Title III and concluded that the term "mobile interception device" was intended to carry a broader meaning than a literal reading. According to the court:

> The emphasis in "mobile interception device" falls, it seems to us (there are no other published decisions on the point), on the *mobility of what is intercepted* rather than on the irrelevant mobility or stationarity of the device. The term in context means a device for intercepting mobile communications, and so understood it authorized the district judge in the Western District of Wisconsin to order a tap on the phone thought to be used by Hotchkiss, regardless of where the phone or the listening post was. The narrow, literal interpretation would serve no interest in protecting privacy, since the government can always seek an order from the district court for the district in which the listening post is located authorizing nationwide surveillance of cellular phone calls. The narrow interpretation would merely complicate law enforcement.[12]

Although the decision seemed to suggest that federal judges had authority to authorize orders to conduct electronic surveillance of cellular telephones located in any judicial district in the United States, few if any further challenges were made to the jurisdiction of federal judges to issue such orders covering electronic surveillance of other judicial districts. However, this has begun to change.

II. The Fifth Circuit's Decision and Subsequent Non-Decision Concerning Jurisdictional Limitations on Wiretaps of Cell Phones in *United States v. North*

A case in the Fifth Circuit recently challenged the notion that federal judges possess unbounded power to issue wiretaps extending beyond their judicial districts. In *United States v. North*, a wiretap was authorized by a district judge in the Southern District of Mississippi for a cellular telephone based in Texas but being used to deliver drugs to Mississippi; the phone was based in Texas, while the government's listening post was in Louisiana.[13] The Fifth Circuit first ruled that the district court did not have territorial jurisdiction to issue the wiretap, and that because such jurisdiction was a "core concern" of Congress when passing the law, the evidence from the wiretap should be suppressed. However, just a little over two months later, the Court withdrew its original decision and replaced it with a new opinion that did not address the jurisdictional question, but rather suppressed the evidence from the wiretap based upon minimization issues.

A. Factual Background of the North *Case*

In 2008, the U.S. Drug Enforcement Agency ("DEA") began investigating a drug dealer named Kenneth Lofton in Jackson, Mississippi. After obtaining wiretaps from a federal judge in Jackson, Mississippi, for two cellphones used by Lofton, DEA was able to observe and discover that Lofton's source of supply in Jackson was Jerry Primer. DEA was able to secure a wiretap on Primer's telephone from the same federal judge authorizing the Lofton wiretaps as part of their continuing investigation. Through this wiretap, DEA learned that Primer was receiving his cocaine from someone in Houston, Texas, first known only as "Billy," who was traveling to Jackson to meet and deliver a load of cocaine to Primer. Agents observed this meeting at Primer's home and physically saw "Billy," whom they later identified as Richard North. Agents then observed North and Primer travel to a shopping center in Jackson, where they witnessed the delivery of cocaine to other co-conspirators.[14]

DEA was later able to obtain a court order from the same federal judge in Mississippi authorizing the wiretap of North's phone. In that wiretap application, the government noted that, "[a]lthough [North's phone] is being used primarily in the State of Texas and the monitoring is occurring in the regional center in Louisiana, this order is being sought in the Southern District of Mississippi, because [North's phone] is being used as a facility to distribute narcotics into this district as is fully described below."[15] The judge approved the wiretap and DEA began listening to North's phone. Based on conversations intercepted over North's phone, DEA learned that North would be delivering another load of cocaine to Primer in Jackson a month later. On the date of delivery, agents overheard conversations on North's phone indicating that he was traveling to Mississippi with the cocaine. DEA arranged for Texas state troopers to stop North, but when they searched his vehicle, no drugs were found. After being released, North used his phone to call his girlfriend, to whom he confided that he had hidden the cocaine in the car such that it could not be found by law enforcement. North told the woman that he was cancelling his delivery to Mississippi and was going back home a different way. Shortly

thereafter, police arrested North at his home in possession of cocaine and firearms.[16]

After he was indicted in the drug conspiracy, North moved to suppress the evidence against him, arguing among other things that the federal judge did not have authority under the Wiretap Act to authorize the tapping of his phone because neither his phone nor the government's listening post was in the Southern District of Mississippi where the authorizing judge sat. The government responded by acknowledging that this jurisdictional issue was one of first impression in the Fifth Circuit, and argued that the court should rely on the Seventh Circuit's decision in *United States v. Ramirez*, which found that a Wisconsin district court had jurisdiction to issue a wiretap where a cell phone was being used in Minnesota to conduct business of a conspiracy with ties to Wisconsin even though the listening post was also in Minnesota. The government further argued that the court had jurisdiction because (1) the interception was to be made of a mobile phone, not a land-line phone;[17] (2) the mobile phone was being used to facilitate the distribution of narcotics into the Southern District of Mississippi; (3) on one occasion during this facilitation, North's phone was known to have been located and used in the Southern District of Mississippi; (4) although the monitoring post was located in Louisiana, a simultaneous feed and aural acquisition station was located in the wire room of the DEA's Jackson, Mississippi, office in the Southern District of Mississippi, so that aural acquisition was occurring in both jurisdictions simultaneously; and (5) the investigation began in the Southern District of Mississippi with the same district court judge reviewing and passing on the propriety of all four wiretap applications.

B. District Court

The district court began its opinion by setting forth the current state of the law in the Fifth Circuit, which held that jurisdiction for a wiretap order lies both (1) where the phone is then physically located and (2) where the communications will be overheard (i.e., the listening post).[18]

The district court continued by pointing out that the government's argument pertaining to certain factors that gave the court jurisdiction did not match up with the terms of the statute:

> By its very terms, the statute only grants jurisdiction to authorize or approve '*interception*' of wire, oral, or electronic communications *within the territorial jurisdiction of the court* in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction).[19]

The district court stated that a court does not have jurisdiction to authorize interception simply because the wiretap is sought as part of an investigation of criminal activity within the district or because a judge in that district had previously issued wiretaps of co-conspirators' phones or because the phone the government is seeking to tap is being used to facilitate the distribution of drugs into the district.[20] Although it did not explicitly say so, the district court seems to have been worried about a slippery slope, and it preferred to clearly draw a line on the slope by saying that "[t]erritorial jurisdiction is tied to the place of interception."[21]

The court declined to address what it deemed the government's best argument for finding territorial jurisdiction in this case—the mobility of cellular telephones. The government relied heavily on the Seventh Circuit's opinion in *Ramirez*, arguing that the federal judge in the Southern District of Mississippi who had authorized the wiretap in the *North* case was similarly situated to the federal judge from the Western District of Wisconsin in *Ramirez*. However, the court chose not to decide the issue of whether a district judge has jurisdictional authority to order a wiretap of a phone where neither the phone nor the listening post was in the judge's district.[22] Instead, the district court decided that, since it was finding that the issue of territorial jurisdiction is not a basis for suppression, there was no need to parse the definition of "mobile interception device."

According to the district court, the United States Supreme Court has said that not every violation of Title III requires suppression.[23] Rather, suppression is required where law enforcement fails to satisfy a statutory requirement that directly and substantially implements the congressional intention of the Act. The court found that "territorial jurisdiction was not central to the purposes of Title III."[24] The court based its decision to a large degree on the fact that, under Fifth Circuit precedent, territorial jurisdiction could be vested in a district judge based solely upon the fortuitous location of a listening post which could theoretically have nothing whatsoever to do with the criminal investigation.[25] "Given this, it can hardly be said that territorial jurisdiction is intended to play a central role in the statutory scheme. . . . Therefore, suppression is not required on jurisdictional grounds, regardless of whether the listening post or tapped cell phone was located within the court's territorial jurisdiction."[26]

C. Fifth Circuit's First Decision in North

North appealed the district court's decision and, on August 26, 2013, the Fifth Circuit issued its *per curiam* decision in *United States v. North*.[27] First, the court addressed the territorial jurisdiction question. The court held that:

> [E]xcept in the case of a mobile interception device, a district court cannot authorize interception of cell phone calls when neither the phone nor the listening post is present within the court's territorial jurisdiction. This, however, is exactly what the district court did in this case. . . . In short, the district court, located in the Southern District of Mississippi, lacked the authority to permit interception of cell phone calls from Texas at a listening post in Louisiana.[28]

The court expressly disagreed with the Seventh Circuit's holding in *Ramirez*, finding instead that the word "mobile" in "mobile interception device" from 18 U.S.C. § 2518(3) "appears to refer to the mobility of the *device used to intercept* communications, not the mobility of the tapped phone."[29] According to the Fifth Circuit, it was not the intent of Congress to enlarge the scope of a district court's authority to issue wiretap warrants in any jurisdiction in the United States when the device to be intercepted is a cell phone.

Next, the court turned to whether the lack of territorial jurisdiction requires suppression of evidence obtained from such a wiretap issued without jurisdictional authority. Referencing the remedy of suppression found in Section 2518(10)(a)(ii) for an authorization order which is "insufficient on its face[,]" the court recognized Supreme Court precedent limiting suppression to only a "failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device."[30] While the Eleventh and Second Circuits had found that territorial jurisdiction was not a "core concern" justifying suppression, the Fifth Circuit disagreed, holding that:

> Title III's territorial restrictions prevent forum manipulation by law enforcement, similarly preventing wiretap authorizations in cases where investigators would otherwise be able to obtain them. Limiting the number of district judges authorized to issue a wiretap warrant reduces the opportunity for the government to use forum manipulation to obtain a warrant that may not be approved elsewhere. We fail to see how this is not a significant protection of privacy. Territorial limitations on a district court directly implicate Congress's intent to guard against the unwarranted use of wiretapping.[31]

The court pointed out in a footnote that its holding created a strange result in this case, since the district court that had the strongest investigative nexus—and therefore the ability to best balance privacy concerns with the appropriateness of the wiretap—lacked territorial jurisdiction to issue the wiretap. Recognizing its role as interpreter and not creator of laws, the court stated that "[i]t is for the United States Congress to determine whether, in light of technological advances, the statute should be amended."[32]

D. Fifth Circuit's Sua Sponte Withdrawal of Its First North *Decision and Its New Decision Avoiding the Jurisdiction Question*

On October 24, 2013, almost two full months after its initial decision in *North*, the Fifth Circuit sua sponte withdrew its previous opinion and issued a new, superseding opinion.[33] Curiously, the court's opinion was stripped of any direct holding on the issue of territorial jurisdiction or necessity. Instead, the court only ruled on the issue of minimization, finding that the government had failed to comply with the minimization requirements and that evidence from the wiretap should therefore be suppressed.

Judge DeMoss wrote a concurring opinion stating that he would have reached the territorial jurisdiction question and would have ruled as the Court had done previously. He then proceeded to retype the previous opinion on this question almost verbatim.[34] Judge DeMoss's statement towards the end of his concurrence might give some insight into why the court withdrew and superseded its prior opinion: "Although application of the plain language may create a circuit split and potentially reduce the efficiency of the government to intercept communications from any available listening post, this is not a reason for our court to apply the law in contravention of the plain language of the statute."[35]

These recent opinions by the Fifth Circuit have raised questions anew in the minds of many as to whether there are in fact jurisdictional limitations on the authority of federal judges to issue wiretaps under Title III—questions that were previously presumed to have been answered by the Seventh Circuit in *Ramirez*. Shortly after the *North* decisions, the D.C. Circuit entered these murky waters and added further commentary to this percolating debate.

III. The D.C. Circuit's Decision Concerning Jurisdictional Limitations on Planting Bugs in Private Places in United States v. Glover

The United States Court of Appeals for the District of Columbia Circuit recently addressed another part of Title III in *United States v. Glover*, a case involving the recording of oral communications via a bug installed in a defendant's truck.[36] In *Glover*, the defendant was suspected of dealing drugs, so the FBI obtained a warrant to tap his cell phone. Because Glover was careful and spoke only in code while on his cell phone, the FBI secured a warrant from a district court judge in Washington, D.C. to install an audio recording device in Glover's truck, which was parked at an airport in Baltimore, Maryland. In fact, the warrant specifically authorized the FBI to forcibly enter the truck, regardless of whether the vehicle was in D.C., Maryland, or Virginia. The bug was successful, capturing evidence of Glover's drug dealing, whereby he was thereafter indicted and convicted for conspiracy to distribute cocaine.[37]

The defendant appealed, arguing that the warrant was insufficient on its face because it was signed by a district court judge in D.C. authorizing the FBI to place an electronic bug in Glover's truck parked in Maryland – outside the district court's jurisdiction. The government countered by arguing that a district court judge was in fact authorized to approve the placement of such an electronic listening device on a vehicle anywhere in the United States.[38]

The court began by reminding the parties that Section 2515 of Title 18, United States Code, states that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any . . . proceeding . . . if the disclosure of that information would be in violation of this chapter." The statute further states that an:

> [A]ggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is *insufficient on its face*; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[39]

The court held that the United States Supreme Court had "read paragraph (i) as requiring a broad inquiry into the government's intercept procedures to determine whether the government's actions transgressed the "core concerns" of the statute, whereas (ii) is a mechanical test; either the warrant is facially sufficient or

it is not."[40] Without limiting paragraph (i) by applying a "core concerns" test to it, a broad, unlimited reading of paragraph (i) would make the other two paragraphs redundant, since an authorization which is "insufficient on its face" would necessarily be "unlawfully intercepted."[41]

But the court disagreed with the interpretations of the Third, Fifth, and Sixth Circuits, all of which applied the "core concerns" test to paragraph (ii), stating that such interpretations were contrary to the plain text of the statute and elevated policy over text.[42] According to the court, the Supreme Court had turned to congressional policies *only after* it had first applied traditional tools of statutory construction to paragraph (i), which indicated that a limiting construction was necessary in order to avoid rendering the other two paragraph "surplusage."[43] The court went on to state that a facially invalid warrant should be mandatorily suppressed, as there was no room for judicial discretion in such a circumstance.[44]

The court next turned to the jurisdictional language of Title III, which states that a judge may "authoriz[e] or approv[e] interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)."[45] The court nonetheless concluded that the language could apply either to the jurisdiction in which the judge was sitting (in this case D.C.) or to the jurisdiction in which the mobile interception device was installed (in this case Maryland). The court stated that:

> Under either reading, the parenthetical makes clear that a judge cannot authorize the interception of communications if the mobile interception device was not validly authorized, and a device cannot be validly authorized if, at the time the warrant is issued, the property on which the device is to be installed is not located in the authorizing judge's jurisdiction. A contrary reading would render the phrase "authorized by a Federal court within such jurisdiction" completely superfluous.[46]

Next, the court recounted the government's argument, based on cases from the Second, Fifth, and Seventh Circuits, that an "interception" under Title III takes place at both (1) the location of the listening post and (2) the location of a tapped phone.[47] According to the government, this language and its interpretation gives an issuing court "the power to authorize covert, trespassory entries onto private property, anywhere in the country, for purposes of placing surveillance equipment. The only jurisdictional limitation the government acknowledges is that the listening post must be located in the issuing court's jurisdiction."[48] The court noted, however, that the statute does not refer to a "listening post," that the cases cited by the government all addressed phone taps (rather than installing bugs in places), and that none of the cases cited by the government addressed the jurisdictional issue of an issuing court authorizing law enforcement to covertly place a listening device on private property.[49]

Finally, the court construed Rule 41 of the Federal Rules of Criminal Procedure in conjunction with the provisions of the Wiretap Act, which appears to be the first time a federal appellate court has used Rule 41 to provide clarity and certainty to the provisions of the Act. Rule 41 states that "a magistrate judge with authority *in the district* has authority to issue a warrant for a person or property outside the district if the person or property is located *within the district when the warrant is issued* but might or be moved outside the district before the warrant is executed."[50] Stating that Rule 41 partially implements the statute and that its language is crystal clear, the court held that the warrant issued in this case appears on its face to violate the rule and the statute.[51]

The government also argued the same holding from the district court in *United States v. North*—that territorial jurisdiction is not a "core concern" of Title III and that therefore suppression is not the appropriate remedy for a violation of such jurisdiction in this case. The court responded to the government's argument by reiterating that the Supreme Court's position that the "core concerns" test does not apply to paragraph (ii), and that even if it did, the court would agree with the Fifth Circuit's recent decision in *North*, holding that territorial jurisdiction *is* a core concern of Title III.[52] The court concluded that the jurisdictional problem with the warrant could not be excused as a "technical defect," which some circuit courts have allowed to slide. Rather, the court held that "a blatant disregard of a district judge's jurisdictional limitation" was more than just a technical violation.[53]

Finally, the court shot down what it called the government's "last refuge" argument—a request to import a "good faith" exception to Title III's remedy of suppression.[54] The court held however that the government's actions could not have been in good faith because they so blatantly violated Rule 41 and, in any event, Congress was clear in declaring that suppression is required when evidence has been gathered pursuant to a facially insufficient warrant.[55] Finding that the district court's failure to preclude the truck bug evidence was plain error, the court reversed appellants' convictions.

IV. Fallout from *North* and *Glover* and the Future of Electronic Surveillance

In light of these recent appellate decisions addressing jurisdictional questions pertaining to Title III, it is unclear whether there are jurisdictional boundaries on federal judges' ability to authorize orders for electronic surveillance and whether evidence emanating from such orders is suppressible. It appears that law enforcement can usually avoid these issues by simply setting up listening posts in the jurisdictions where the issuing courts are located (although, judging from dicta in *Glover*, that may not work in the District of Columbia).[56] Of course, this tactic could be viewed as an opportunity for arbitrage, as it effectively allows the government to choose the districts and judges from whom they will seek authorization orders to conduct electronic surveillance, irrespective of their connection to the underlying criminal investigation. Ironically, while not the exact type of forum manipulation about which Judge DeMoss was concerned in his concurring opinion in *North*, it is effectively the same and could continue unabated even if Judge DeMoss's concurring opinion had remained the majority in the Fifth Circuit.

Hopefully, just as federal prosecutors did in the *North*

case, the government will continue to seek wiretaps from "the jurisdiction having the strongest investigative nexus to the object in which the monitoring device is installed."[57] This seems to best serve the public interest, and it limits forum shopping and jurisdictional arbitrage, about which the appellate courts have recently been greatly concerned. However, to get to this point, Congress will need to step in and update Title III to catch up with today's technology and challenges. That will be no easy task.

Endnotes

1 18 U.S.C. §§ 2510 *et seq* (2014).

2 18 U.S.C. § 2510(9)(a) (2014).

3 18 U.S.C. § 2518(3) (2014).

4 18 U.S.C. § 2515 (2014).

5 18 U.S.C. § 2518(10)(a)(2014).

6 112 F.3d 849 (7th Cir. 1997).

7 *Id.* at 851.

8 *Id.*

9 *Id.* at 852.

10 *Id.* (citing *United States v. Denman*, 100 F.3d 399, 403 (5th Cir. 1996); *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992)).

11 *Id.*

12 *Id.* at 853 (emphasis added).

13 728 F.3d 429 (5th Cir. 2013), *withdrawn and superseded by*, 735 F.3d 212.

14 Brief of the United States, *United States v. Richard North*, Fifth Circuit Case No. 11-60763 (filed May 7, 2012).

15 Defendant Richard North's Motion to Suppress Title III Intercept and Its Fruit, Criminal No. 3:09cr92TSL-FKB, Court Docket Number 147 at 5 (May 24, 2010).

16 *Id.* at 3-4.

17 This was important because prosecutors had to distinguish this case from the 5th Circuit's *United States v. Denman* precedent. 100 F.3d 399, 403 (5th Cir. 1996)

18 *United States v. North*, Crim. No. 3:09cr92TSL-FKB (S.D. Miss. 2011) at 5-6 (on file with the author) (citing *United States v. Denman*, 100 F.3d at 403).

19 *Id.* at 9-10.

20 *Id.* at 10.

21 *Id.*

22 *Id.* at 11. Interestingly, although not directly addressing the statutory definitional issue in *Ramirez*, the district court in *North* stated that it was "dubious that Congress intended 'mobile interception device' to include cellular telephones." *Id.*

23 *Id.* at 12 (*citing United States v. Chavez*, 416 U.S. 562, 575 (1974)).

24 *Id.* at 15 (*citing United States v. Giordano*, 416 U.S. 505, 527 (1974)).

25 *Id.* at 16 (*citing Ramirez*, 112 F.3d at 853).

26 *Id.* at 16-17.

27 728 F.3d 429 (5th Cir. 2013), *withdrawn and superseded by*, 735 F.3d 212. A copy of this decision is on file with the author and will be referred to herein as "*North*, Fifth Circuit Case No. 11-60763." The sum and substance of the opinion relating to territorial jurisdiction is reprinted almost verbatim in Judge DeMoss' concurring opinion in the superseding *North* opinion.

28 *North*, Fifth Circuit Case No. 11-60763 at 5.

29 *Id.* at 6.

30 *Id.* at 7 (*citing United States v. Donovan*, 429 U.S. 413, 433-34 (1977) (*quoting Giordano*, 416 U.S. at 527)).

31 *North*, Case No. 11-60763, at 8.

32 *Id.* at 6, n.1.

33 *United States v. North*, 735 F.3d 212 (5th Cir. 2013).

34 *Id.* at 216-219 (DeMoss, J., concurring).

35 *Id.* at 219.

36 736 F.3d 509 (D.C. Cir. 2013).

37 *Id.* at 510-511.

38 *Id.* at 511.

39 18 U.S.C. § 2518(10)(a) (2013) (emphasis added).

40 736 F.3d at 513.

41 *Id.*

42 *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)).

43 *Id.* at 513-14.

44 *Id.* at 513.

45 18 U.S.C. § 2518(3) (2013).

46 736 F.3d at 514. The court also points out the legislative history of the Act, which states that "the objective of the language was to ensure that warrants remain effective in the event of a target vehicle is moved out of the issuing judge's jurisdiction *after* a warrant is issued, but before a surveillance device can be placed in the vehicle." *Id.*

47 *Id.* at 514 (*citing United States v. Luong*, 471 F.3d 11097, 1109 (9th Cir. 2006); *Ramirez*, 112 F.3d at 852-53; *Denman*, 100 F.3d at 403; and *Rodriguez*, 968 F.2d at 136).

48 736 F.3d at 514.

49 *Id.* at 514-15.

50 Fed.R.Crim.P. Rule 41(b)(2) (2014) (emphasis added).

51 736 F.3d at 515.

52 *Id.* Interestingly, the original *North* decision was issued by the Fifth Circuit on August 26, 2013. *See* 728 F.3d 429 (5th Cir. 2013). On October 24, 2013, the Fifth Circuit withdraw its August decision in *North*, replacing it with a new decision as recounted above that avoided the jurisdictional issue (except in a concurring opinion), focusing instead on the issue of minimization. The

Glover decision, which purports to rely on the original *North* decision addressing the jurisdictional question, was decided on November 8, 2013, *after* the Fifth Circuit had withdrawn its previous opinion.

53 *Id.*

54 *Id.* at 515-16.

55 *Id.* at 516.

56 The opinion in *Glover* is a potential intellectual baton the D.C. Circuit has laid before the other appellate courts, from which they can scoop up and run with their own opinions, thus further limiting the jurisdictional reach of federal judges to issue wiretaps or bugs.

57 U.S. Department of Justice Electronic Surveillance Manual, DOJML Comment § 9-7.000.