No. 17-43

IN THE

Supreme Court of the United States

LOS ROVELL DAHDA AND
ROOSEVELT RICO DAHDA,

Petitioners,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUIT

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF PETITIONERS

JEFFREY T. GREEN
Co-Chair Amicus Committee
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW
Washington, DC 20036
(202) 872-8600

JENNIFER LYNCH
ANDREW CROCKER
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

ILANA H. EISENSTEIN
Counsel of Record
JASON D. GERSTEIN
MARC A. SILVERMAN
DLA PIPER LLP (US)
One Liberty Place
Philadelphia, PA 19109
(215) 656-3300
ilana.eisenstein@dlapiper.com

Counsel for Amici Curiae

277252

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Cited Authorities

Page

Cited Authorities

STATUTES

Cited Authorities

Page

OTHER AUTHORITIES

Page

Page

INTEREST OF *AMICI CURIAE*[1]

Amici are organizations committed to ensuring constitutional rights continue to be protected as technology advances and include the Electronic Frontier Foundation and National Association of Criminal Defense Lawyers. These organizations have appeared previously as *amici* before this Court. Their individual organizational statements are contained in the Appendix following this brief.

SUMMARY OF THE ARGUMENT

I. Congress and this Court have long recognized that wiretapping poses a serious threat to privacy. Indeed, in 1934, Congress initially outlawed wiretapping outright. In 1968, after renewed and intense debate, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and permitted wiretapping, but only under the narrowest of circumstances and subject to restrictive requirements "carefully drawn to protect extremely sensitive privacy interests." *United States* v. *Ojeda Rios*, 495 U.S. 257, 268 (1990) (Stevens, J., dissenting).

The privacy concerns that animated Title III's strict limits on wiretapping have become only more acute with the proliferation of cellphones, smartphones, and Internet-based communications. Modern wiretaps

1. Pursuant to Supreme Court Rule 37.3(a), all parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, amici state that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than amici or their counsel made a monetary contribution to fund the preparation or filing of this brief.

frequently intercept far more information than monitoring a traditional phone call or even searching a home—the interception of our cell phones exposes to the government the digital records of "nearly every aspect of [our] lives—from the mundane to the intimate." *Riley* v. *California*, 134 S. Ct. 2473, 2490 (2014). But as communications have evolved, wiretaps have become only easier for the government. A wiretap no longer requires physical intrusion into the phone wires. Now, from the comfort of their office, government agents not only listen in on voice conversations, but also read texts and view data communications, pictures, and emails, sent from cellular phones located anywhere in the country.

Meanwhile, since Title III's passage, the number of wiretaps has ballooned. Last year, over 43 million conversations were intercepted, 93% of which were from "portable devices," largely cell phones. Meanwhile, only a small fraction of those conversations were incriminating, meaning that millions of personal and innocent conversations (and data communications) were monitored through court-ordered wiretaps. New technology thus has enhanced the already-acute privacy concerns posed by wiretapping.

II. The power and pervasiveness of new wiretapping technology makes Title III's territorial limits that much more important. Title III requires a wiretap to be authorized by a judge within the territorial location that the wiretap is placed or heard.

That territorial limitation is not a mere technicality—it is a critical component of the statute's privacy protections. Title III's territorial limits mean that the wiretap is

approved, monitored, and overseen by the court with the closest nexus to the investigation. Geographic restraints also curtail forum shopping and prevent prosecutors from seeking wiretap approval from only favorable jurisdictions.

Territorial limits further alleviate the substantial burden of review, approval, and supervision of wiretaps by dividing those duties among the various districts. Title III vests the district courts with discretion whether to issue a wiretap order, which may issue only after a robust and detailed wiretap application and affidavit that satisfies all statutory requirements. Once a wiretap commences, Title III imposes on the court rigorous supervisory responsibilities to monitor the progress of the wiretap, ensure the continued necessity of the wiretap, and confirm compliance with Title III's many strictures. If properly carried out, those statutory responsibilities require significant attention by the district court, which would be strained to the breaking point if a diminishing number of district courts became the centralized hubs for wiretaps nationwide.

Title III's territorial limits parallel similar geographic restrictions on the warrant power at common law and embodied in the Fourth Amendment, which recognized that a warrant reached only as far as the issuing official's authority. Those territorial limits persist in Federal Rule of Criminal Procedure 41, which, with few limited and enumerated exceptions, allow a magistrate judge to issue search warrants for persons or property within that judge's district. See Fed. R. Crim. P. 41(b). Our longstanding preference for geographically divided search authority is a guard against abuse that inheres in centralized power.

The government, however, has continued to dispute that Title III places any meaningful territorial limits on its authority to tap cellular phones anywhere in the country. That interpretation of Title III is incorrect and inconsistent with Title III's statutory scheme. The government's position that wiretaps of cell phones could issue from any court nationwide would drastically undercut Title III's carefully designed system of protections.

III. If law enforcement violates any of Title III's carefully drawn requirements, the statute *requires* suppression of the wiretapping evidence—a remedy that promotes compliance with Title III's extensive requirements and Congress's primary objective to limit and carefully regulate wiretaps' substantial intrusions on privacy.

ARGUMENT

I. Title III, Including Its Territorial Limitation, Was Expressly Designed To Limit Intrusion And Protect Privacy

A. Wiretaps Pose A Serious Threat To Privacy As Congress, States, And This Court Have Long Recognized

The privacy interest implicated by wiretapping is acute. Wiretaps have long been viewed as more intrusive than a physical search warrant. Wiretaps capture not only the target's words, but also any and all communications between the target and third-parties—whether or not those communications are criminal. Justice Brandeis expressed this very concern over 90-years ago in his familiar dissent in *Olmstead* v. *United States*:

> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.

277 U.S. 438, 475-476 (1928) (Brandeis, J., dissenting). Justice Brandeis further expressed concern that "discovery and invention" continually provides "subtle[]" and "far-reaching" means for the government to "obtain disclosure in court of what is whispered in the closet." *Id.* at 473.

Recognizing wiretaps' threat to privacy, as early as 1862, California "found it necessary to prohibit the practice by statute." See *Berger* v. *State of N.Y.*, 388 U.S. 41, 45 (1967). Other states, such as Illinois and New York, soon followed suit. *Ibid.*

Likewise, in 1934, "Congress outlawed the interception without authorization, and the divulging or publishing of the contents of wiretaps." *Berger*, 388 U.S. at 46; *Nardone* v. *United States*, 302 U.S. 379, 384 (1937) ("For years controversy has raged with respect to the morality of the practice of wire-tapping by officers to obtain evidence. It has been the view of many that the practice involves a grave wrong."). That statute made wiretapping a federal

criminal offense and made wiretap evidence inadmissible in court. Federal Communications Act of 1934, ch. 652, Title VI § 605, 48 Stat. 1064, 1103-04 (1934) (current version at 47 U.S.C. 605 (2000)).

Forty years after *Olmstead*, in *Katz* v. *United States*, 389 U.S. 347 (1967), and *Berger*, *supra*, this Court "accepted Justice Brandeis's logic" concerning the privacy and threat of wiretaps. S. Rep. No. 541, 99th Cong., 2d Sess. 2 (1986). In *Berger*, this Court recognized that "[b]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope." 388 U.S. at 56.

B. With Those Privacy Concerns At The Forefront, Congress Enacted Title III To Permit Wiretaps In Only Limited Circumstances

In 1968, Congress passed The Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90–351, 82 Stat. 197, codified at 42 U.S.C. 3711. Title III of the statute (the Wiretap Act), codified at 18 U.S.C. 2510-22, authorizes government interception of wire communications only "under carefully subscribed circumstances." See S. Rep. No. 541, at 3556. Congress passed Title III with two concerns in mind: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 1097, 90th Cong., 2d Sess. 2153 (1968). The "draftsman and sponsors of Title III" further intended to "establish a system of prior review of applications for surveillance orders." William H. Erickson, et al., Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping

and Electronic Surveillance 73 (1976) (1976 Wiretap Commission). Title III imposes stringent limitations on the use of wiretapping, requiring careful adherence to its requirements.

Congress understood that "[w]iretapping and other forms of eavesdropping are recognized by even their most zealous advocates as encroachments on a man's right to privacy * * * the most comprehensive of rights and the right most valued by civilized men." S. Rep. No. 1097, at 2231; see also *id.* at 2180 ("The right here at stake—the right of privacy—is a right arising under certain provisions of the Bill of Rights and the [D]ue [P]rocess [C]lause of the 14th [A]mendment."). As the D.C. Circuit recently observed:

> The deliberations leading up to the passage of Title III reveal deep unease over the risk to privacy interests inherent in granting wiretapping authority to law enforcement. With telecommunications technology—and alongside it eavesdropping technology—evolving rapidly, members of Congress feared that if [Title III] is successful, today's narrowing enclave of individual privacy will shrink to the vanishing point.

United States v. *Scurry*, 821 F.3d 1, 9-10 (D.C. Cir. 2016) (quoting S. Rep. No. 1097, at 2232) (internal citations and quotation marks omitted). For that reason, the statute's particular requirements were "carefully drawn to protect extremely sensitive privacy interests." *Ojeda Rios*, 495 U.S. at 268 (Stevens, J., dissenting).

In 1986, Congress amended Title III to extend its restrictions to electronic communications—*i.e.*, data, text messages, and email. See generally S. Rep. No. 541. Congress recognized that communication technology had again advanced significantly and that Title III's protections had "not kept pace with the development of communications and computer technology." *Id.* at 3556. The 1986 amendments to Title III expanded the statute to cover "electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing." *Ibid.* Congress further recognized that Title III failed to protect the "storage and processing of information" by computers, on which many Americans came to significantly rely to "lock away a great deal of personal and business information." *Id.* at 3557. Congress recognized that "[f]or the person or business whose records are involved, the privacy or proprietary interest in that information should not change." *Ibid.* As it did when it first passed Title III, Congress again made its privacy concerns paramount:

> Most importantly, the law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id. at 3559.

Title III thus broadly prohibits electronic surveillance, providing for only narrow circumstances under which law

enforcement agents may use the technique. *United States* v. *Giordano*, 416 U.S. 505, 515 (1974) (Congress "evinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications. These procedures were not to be routinely employed as the initial step in criminal investigation."); see also *ibid.* (Congress sought to limit the use of wiretaps by "impos[ing] important preconditions to obtaining any intercept authority at all.").

Title III imposes a strict set of rules on the application, authorization, oversight, and termination of a wiretap. Title III's requirements go far beyond the procedures for a standard search warrant. A wiretap must first be authorized by the Attorney General or another specified high-level Department of Justice official before district court approval may be sought. 18 U.S.C. 2516(1). In addition to establishing probable cause, Title III also requires an applicant to establish the necessity of the wiretap, *i.e.*, wiretapping is a tool of last resort, to be only used when all less intrusive law enforcement techniques have failed or would be futile. 18 U.S.C. 2518(1)(c). During a wiretap, law enforcement must "minimize" the interception of irrelevant conversations. 18 U.S.C. 2518(5). Wiretap orders only may remain in place for as long as necessary, and for no more than 30 days.[2] 18 U.S.C. 2518(5). And the wiretap recordings must be immediately sealed by the district court upon the wiretap's conclusion. 18 U.S.C. 2518(8)(a).

2. Wiretap orders may be renewed or extended, but applications for extension are subject to the same requirements and standards as the original application, with the added requirement that the government report its results obtained so far or explain why its failure to obtain results. 18 U.S.C. 2518(1)(f).

The authorizing district court is responsible for oversight of the wiretap, and courts typically require frequent, periodic reports during the duration of the order. See 18 U.S.C. 2518(6). Those reports "contain the prosecutors' summaries of telephone conversations, theories of the case, and additional investigative leads," and help the authorizing court determine what progress has been made in a criminal investigation and the need for continued interception, if any. See, *e.g.*, *Scott* v. *United States*, 436 U.S. 128, 131-32 (1978) ("The order also required the agents to * * * report to the court every five days 'the progress of the interception and the nature of the communication intercepted.'").[3]

To allow for continued public and Congressional oversight of wiretapping activities, Title III requires judges and prosecutors to report to the Administrative Office of the United States Courts (Administrative Office) broad-ranging and detailed statistics that reflect the number of wiretaps and intercepts, their type and length, and the results of wiretap investigations. See 18 U.S.C. 2519(1)-(2). The Administrative Office is required under Title III to submit a "full and complete report" of that information to Congress, which it publishes in an annual report known as the "Wiretap Report." 18 U.S.C. 2519(3); see also, *e.g.*, Wiretap Report, Yearly Wiretap Reports from 1997 to 2016.[4]

---

3. In addition, to ensure data integrity, 18 U.SC. 2518(8) requires recording of intercepted communications to prevent editing, immediate sealing, and judicially supervised custody.

4. Available at https://tinyurl.com/YearlyWiretapReports.

C. The Privacy Concerns Animating Title III Have Become More Acute With Advancing Telecommunications Technology

New communication technology and advances in wiretapping techniques have made it increasingly possible to intercept communications from anywhere in the country. The potential for intrusions into privacy that led Congress to impose Title III's strict limits on wiretapping only have increased with the growth and innovation of new technologies—cellphones, smartphones, and internet-based communication—that are at once more pervasive and more personal than traditional landlines. Our cell phones frequently contain far greater information than a simple voice call or even the search of a home might reveal. Today, cell phones contain digital records of "nearly every aspect of [our] lives—from the mundane to the intimate." *Riley*, 134 S. Ct. at 2490. But, when the government wiretaps our cellphones, those private moments are exposed to a degree that was not possible, or imagined, at the time Title III was passed.

Until relatively recently, telephones used copper wires to carry an electric current representing the sound waves of your voice. Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* 131 (2007). Along the way, the signal was passed from the phone to the wall socket, and then through a series of wires to a local telephone exchange, where it was routed to the receiving phone. That signal was "vulnerable to wiretapping at every point along its path." *Id.* at 131. And traditional carrier-assisted wiretapping "once required that the interception take place near the target, such as at a call-switching center." Pell, 28 Harv. J.L. & Tech at 8 n.33.

The advent of "digital telephony" technology altered the transmission of communications from copper transmission to "digital transmission modes." H.R. Rep. No. 827(I), 103rd Cong., 2d Sess. (1994). Before, "intrinsic elements of wire lined networks presented access points where law enforcement, with minimum assistance from telephone companies, could isolate the communications associated with a particular surveillance target and effectuate an intercept." *Id.* at 3493-94. The digital technology, however, "complicated law enforcement's" ability to introduce a wiretap into the digital system. See *ibid.* As a result, Congress passed the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. 1001-1010, which required telephone companies to build "government-mandated interception capabilities * * * into their networks." Stephanie K. Pell, Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J.L. & Tech. 1, 9 (2014).

Communication again advanced with the invention of modern cellular phones, which facilitate mobile communications "over the air on a radio frequency to a cell site." S. Rep. No. 541, at 3563. Despite the inherent mobility of cellphones, however, with the right technology and the help of the carriers through CALEA, law enforcement need not leave the comfort of their police headquarters to tap a cellular phone. See Pell, 28 Harv. J.L. & Tech. at 8-9.

Once the cellular phone carrier receives a signed wiretap order, the phone carrier simply transmits the signal both to the receiving phone and to the police

listening post simultaneously. See *United States* v. *Reed*, 575 F.3d 900, 916 (9th Cir. 2009) ("[T]he data was compiled in real time by the telephone company and transferred to the federal agents monitoring the wiretap via wire."); *United States v. McLee*, 436 F.3d 751, 764 (7th Cir. 2006) (describing how calls for "all ongoing wiretap investigations" were "initially directed to a single computer hard drive located in" the Chicago office of the Drug Enforcement Administration).[5]

Wiretaps have become even more invasive as they focus increasingly on cell phones. See 2016 Annual Report to Congress Concerning Intercepted Wire, Oral, or Electronic Communications as Required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (2016 Wiretap Report) (93% of all wiretaps are cell phones).[6]

Communication continues to evolve with the proliferation of smartphones and the expansion of Internet-based communication. Now, "hundreds of millions" of people are communicating through smartphone "apps," such as Microsoft's Skype, Apple's FaceTime and iMessage, Google's Hangouts, and Facebook's WhatsApp. Pell, 28 Harv. J.L. & Tech. at 72. Those apps

5. Law enforcement also has the ability to capture signals "as they are transmitted over the air," or through active surveillance, using a device called an International Mobile Subscriber Identity (IMSI) Catcher, also known as a "cell site simulator." Pell, 28 Harv. J.L. & Tech. at 9, 11. The cell site simulator "trick[s] the target's phone into connecting to it" instead of a phone company's cell tower. *Ibid.* Cell site simulators can identify and locate all nearby phones—not just the target's phone—and can be configured to intercept outgoing calls and text messages. *Ibid.* (citing sources).

6. Available at https://tinyurl.com/2016WiretapReport.

use internet protocols to transmit data over "cellular data network[s], rather than the wireless carriers' legacy voice and text message systems." *Ibid.* The evolution of those new technologies, which allow many more ways to communicate, has only enhanced the privacy concerns addressed by Title III.

As this Court observed in *Riley*, "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives." *Riley*, 134 S. Ct. at 2490. It is no surprise, therefore, that this Court recognized that cell phones are quantitatively and qualitatively different than physical searches and that cell phones "hold for many Americans 'the privacies of life.'" *Id.* at 2494-2495 (citing *Boyd* v. *United States*, 116 U.S. 616, 625 (1886)).

D. Since Title III's Passage, Wiretapping Has Drastically Expanded

Since Title III's inception, the number of wiretaps has exploded. In 1968, just 174 wiretaps were authorized. Electronic Privacy Information Center, Title III Wiretap Orders – Stats, Title III Electronic Surveillance 1968-2015.[7] By 2016, that number had ballooned to 3,168 wiretaps, according to the 2016 Wiretap Report, and potentially far more than that according to "Transparency Reports" published by telephone carriers themselves.[8]

---

7. Available at https://epic.org/privacy/wiretap/stats/wiretap_stats.html.

8. A large discrepancy exists between the wiretaps reported in the recent Wiretap Reports and the number reported in telephone carriers' transparency reports. For

The number of interceptions has likewise exploded from 400,000 in 1968 to over 43 million interceptions in 2016. Diffie, *supra*, at 213; 2016 Wiretap Report, Table A1.

The ratio of intercepted communications to incriminating communications is not encouraging. According to the Administrative Office, on average, only about 20% of intercepted conversations are incriminating. See 2016 Wiretap Report, Wire Table 4.[9] Hence, 80% of intercepted communications do not advance a criminal

---

example, the 2016 Wiretap Report identifies 3,168 wiretaps, while the telephone carriers reported 11,868. *Compare* 2016 Wiretap Report *with* AT&T Transparency Report First Half of 2016 (1,229 wiretaps), available at https://tinyurl.com/ATTWireReport1stHalf2016; AT&T Transparency Report Second Half of 2016 (1,219 wiretaps), available at https://tinyurl.com/ATTWireReport2dHalf2016, Sprint Transparency Report (2,359 wiretaps), available at https://tinyurl.com/SprintWireReport; Verizon Transparency Report (1,306 wiretaps), available at https://tinyurl.com/VerizonWireReport; T-Mobile/Metro PCS Transparency Report for 2016 (5,836 wiretaps), available at https://tinyurl.com/TMobileWireReport. Similar large discrepancies have been noted in 2014 and 2015. See Albert Gidari, Stanford Law School, *Wiretap Numbers Still Don't Add Up*, available at https://tinyurl.com/WiretapNumbersDontAddUp ("[Administrative Office] reported 3554 wiretaps in 2014, the four major U.S. carriers reported 10,712 wiretaps implemented for the same period"); *Ibid.* ("[Administrative Office] now reports that 4,148 wiretaps were authorized in 2015 * * * [and] [t]he four major carriers (AT&T, Sprint, Verizon and T-Mobile) reported a total of 11,633 wiretaps in 2015").

9. Available at https://tinyurl.com/2016WiretapReportWire4Table. A substantial number of wiretap orders lack prosecutor's reports that contain information on, *inter alia*, the percentage of incriminating intercepts. *Ibid.*

investigation at all. See *ibid.* Some jurisdictions have lower, even dramatically lower, rates of incriminating intercepts. In 2016, for example, the federal wiretap with the most intercepted communications occurred in the Middle District of Pennsylvania involving a total of "3,292,385 cell phone conversations or messages over 60 days." 2016 Wiretap Report. But the total number of incriminating interceptions identified from that order was zero. 2016 Wiretap Report, Wire A1, Line 2685.[10] While that may be the starkest example, it is by no means the only one. There are numerous other wiretaps that intercepted tens of thousands of conversations without logging a single incriminating conversation. See, *e.g.*, 2016 *Wiretap Report*, Wire Table A1 at Rows 1600 (14,459 interceptions, zero incriminating), 1853 (13,789 interceptions, zero incriminating), 1905 (12,490 interceptions, zero incriminating), 2266 (20,667 interceptions, zero incriminating), 2686 (12,421 interceptions, zero incriminating), 2697 (12,990 interceptions, zero incriminating). The Wiretap Reports also contain many examples where the number of interceptions far exceeds the incriminating conversations. For example, in the District of Columbia, a wiretap intercepted 497,437 communications and only 807 were deemed incriminating—indicating that fully 98% of the intercepted communications were innocent communications. 2016 *Wiretap Report*, Wire Table A1 at Row 1068.

10. Available at https://tinyurl.com/2016WiretapReportWireA1Table.

II. Title III's Territorial Limitation Is An Important Component Of The Statute's Restrictive Framework

The power and pervasiveness of new wiretapping technology underscores the critical importance of Title III's territorial limits. Title III requires a wiretap to be authorized by a judge within the territorial location that the wiretap is placed or heard.[11] In other words, either the cell phone, the place of interception, or both, must be in the district for a wiretap to be valid under Title III. See Pet. App. 16a-17a; *United States* v. *Jackson*, 849 F.3d 540, 551-552 (3d Cir. 2017) (citing the uniform view of the courts of appeals). Title III's territorial limitation works in concert with Title III's other statutory restrictions to carry out the statute's guiding purpose: "protecting the privacy of wire and oral communications." See S. Rep. No. 1097, at 2153.

A. Title III's Territorial Limits Are Critical To The Function Of Its Statutory Scheme

Title III's territorial limitation provides important privacy protection and is crucial to the proper function of the statutory scheme, which features intensive district court and prosecutorial oversight at its core.

---

11. Title III provides that a wiretap order "authorizing, or approving the interception of wire, oral, or electronic communications" may be issued "*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)." 18 U.S.C. 2518(3) (emphasis added).

Adherence to Title III's strict procedures is best assured when "the jurisdiction having the strongest investigative nexus to the object in which the monitoring device is installed" oversees each intensive part of the process. See Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, U.S. Dep't of Justice, *Electronic Surveillance Manual Procedures and Case Law* 15 (2005).[12] Stripping the territorial limitation also would undermine, if not eliminate entirely, oversight by a local, issuing court.

One way that territorial limits improve judicial oversight is by preventing the concentration of wiretaps in a few districts, which could easily become overloaded and unable to discharge the weighty review functions that Title III imposes. Those oversight functions require that the authorizing judge review the affidavit and application for probable cause, necessity and other Title III requirements, supervise the wire throughout the investigation to ensure compliance with statutory requirements,[13] approve any extensions,[14] and immediately seal wire recordings at the wiretap's conclusion.[15] Those reporting, renewal, and

12. Available at available at https://tinyurl.com/USDOJElecSurManual.

13. See 18 U.S.C. 2518(6) (progress reports must be submitted to the court at regular intervals).

14. 18 U.S.C. 2518(1)(f).

15. 18 U.S.C. 2518(8)(a) (When an interception period expires, the "recordings shall be made available to the judge issuing such order and sealed under his directions."). The seal must be placed according to the issuing court's directions "immediately." 18 U.S.C. 2518(8)(a). Some judges have required the sealing to be done in their presence. *E.g.*, *United States* v. *Vazquez*, 605 F.2d

sealing procedures all require careful supervision and cooperation between the district court, prosecutors, and investigators.

Geographic dispersion also ensures that district court judges are able to exercise their discretion whether to approve a Title III application or not. Congress specifically declined to make mandatory the issuance of a Title III order,[16] and that discretion is a critical feature of the statute's privacy protections. Discretion only can be properly exercised if the district court has the time and attention to fully review and consider lengthy and detailed wiretap applications and affidavits with the rigor that Title III demands.

Territorial limits also promote investigators' and prosecutors' compliance with Title III's requirements. Title III has "been found to be most effective" when experienced prosecutors are "working closely with experienced investigators" and in "close cooperation." 1976 Wiretap Commission at xiv. In particular, it is important to have close monitoring between the teams to ensure that minimization requirements, ongoing necessity, and any proper investigative action (including responses to threats) are promptly and carefully carried out. Local oversight and execution of a wiretap helps fulfill those

---

1269, 1278 (2d Cir. 1979); *United States* v. *Martin*, 618 F.3d 705, 709 (7th Cir. 2010), as amended (Sept. 1, 2010). The purpose of the sealing requirement, bolstered by an in-presence requirement, is to "ensure the reliability and integrity of evidence obtained by means of electronic surveillance." See *Ojeda Rios*, 495 U.S. at 263.

16. Upon application a "judge *may* enter" a wiretap order. 18 U.S.C. 2518(3) (emphasis added).

goals by forging close communications and links between the physical surveillance teams and investigators posted in the wireroom who monitor the communications.[17]

In short, the intensive procedural requirements that are imposed to minimize intrusions on individual's privacy require close involvement between the investigators on the ground and the overseeing court. A centralized wiretapping jurisdiction or a wiretap issued from a jurisdiction far removed from the on-the-ground investigation team threatens that carefully circumscribed congressional framework.

B. Title III's Territorial Limitation Protects Privacy By Limiting Forum Shopping

Title III's territorial limitation further promotes Congress's intent to protect privacy by dissuading forum shopping to preferred judges (or even one preferred judge).

Stripping the territorial limitation would allow law enforcement "to use forum manipulation to obtain a warrant that may not be approved elsewhere." *United States* v. *North*, 735 F.3d 212, 219 (5th Cir. 2013) (DeMoss, J., concurring). For that reason, compliance with the territorial limitation is "a significant protection of privacy." *Ibid.*

---

17. During a wiretap, investigators are typically located at a listening post often referred to as a "wireroom." A wireroom is the place where the investigators monitor the communications in real time. See, *e.g.*, *United States* v. *Gordon*, 871 F.3d 35, 42 (1st Cir. 2017); *United States* v. *Emmanuel*, 565 F.3d 1324, 1327 (11th Cir. 2009).

The 1976 Wiretap Commission noted "the dangers that judge shopping presents to the fair disposition of a case may be substantial." 1976 Wiretap Commission at 73. The Commission found that it is "apparent that judge shopping with surveillance applications occurs in several jurisdictions." *Id.* at 74. Prosecutors, moreover, acknowledged to the Wiretap Commission that the "classic reason" that they sought to maneuver to a different court was to "avoid a court likely to take unfavorable action on the [wiretap] application." *Ibid.* Responding to the suggestion to limit wiretap authority to a particular judge, the Commission found that "there is a danger that the judge will come to consider himself a member of the prosecution team, with the result that the quality of judicial review will be diminished." *Ibid.*

Nonetheless, wiretap authorizations are not evenly distributed around the United States. For example, for the past three years, the District of Arizona authorized the most federal wiretaps—between 7 to 9 percent of the applications approved by federal judges over the last three years. 2016 Wiretap Report; 2015 Annual Report to Congress Concerning Intercepted Wire, Oral, or Electronic Communications as Required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (2015 Wiretap Report);[18] 2014 Annual Report to Congress Concerning Intercepted Wire, Oral, or Electronic Communications as Required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (2014 Wiretap Report).[19] In state courts, 82% of wiretaps were authorized in just six states, with California and New York accounting for 54% of all state wiretaps. 2016 Wiretap Report.

18. Available at https://tinyurl.com/2015WiretapReport.

19. Available at, https://tinyurl.com/2014WiretapReport.

Without a territorial limitation, there is nothing stopping any district from becoming a centralized wiretap district for the entire country. That outcome would undermine Title III's restrictive statutory scheme designed to protect privacy and to promote careful oversight of any government wiretaps.

C. Territorial Limitations Have Long Been Central To Our Nation's Laws

History teaches "that territorial restraints on the powers of magistrate judges are nothing new." *United States* v. *Krueger*, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring); *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 201 (2d Cir. 2016), cert. granted sub nom. *United States* v. *Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017) ("Warrants traditionally carry territorial limitations."). Above all, the placement of a territorial limitation in a statute "evinces a deeply rooted historical concern for limiting the territorial reach of magistrate judges' powers." *Krueger*, 809 F.3d at 1123. A centralized wiretapping forum is not in accord with this Nation's governing principles and threatens the privacy of all Americans.

Territorial limits on search warrants have deep roots in the common law and the Fourth Amendment. At common law, a "warrant issued for a search or seizure beyond the territorial jurisdiction of a magistrate's powers * * * was treated as no warrant at all." *Krueger*, 809 F.3d at 1125. The principle "animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official."

Id. at 1124. In particular, when this Court spoke of the requirement that a warrant be issued by "magistrates empowered to issue warrants," *United States* v. *Lefkowitz*, 285 U.S. 452, 464 (1932), state and circuit courts have "[t]ime and again" interpreted that to mean that "a warrant issued in defiance of positive law's restrictions on the territorial reach of the issuing authority will not qualify as a warrant for Fourth Amendment purposes." *Krueger*, 809 F.3d at 1124 (collecting cases); *Weinberg* v. *United States*, 126 F.2d 1004, 1006 (2d Cir. 1942) (warrant issued by the Eastern District of Michigan for property in the Southern District of New York was invalid because "constitutional provisions" prohibit a district court from issuing "search warrants [that] may be used anywhere in the country").

Congress likewise has "repeatedly displayed a preference for geographically divided power," and with good reason: "ours is not supposed to be [a] government * * * with power centralized in one district, but a government of diffused and divided power, the better to prevent its abuse." *Krueger*, 809 F.3d at 1125.

Those concerns have long been present in the rules governing physical searches and seizures under the Federal Rules of Criminal Procedure. Under Rule 41, a search warrant must be issued by a "magistrate judge with authority in the district * * * to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). When it was adopted in 1944, Rule 41 was a "codification of existing law and practice." Fed. R. Crim. P. 41, Advisory Committee Notes. There are only a few exceptions to that rule. Each

exception bears a nexus to the magistrate's territory[20] and each was added within the last decade and a half.[21]

---

20. The exceptions to Rule 41's territorial limitation allow a magistrate judge to issue a warrant outside the district if: (b)(2) "the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (b)(3) "terrorism may have occurred" in that district; (b)(4) if a tracking device is installed within the district, then "the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both"; (b)(5) if a crime occurs in the district, a judge may issue a warrant for property outside of the jurisdiction within a U.S. territory, possession or commonwealth, a premises of a U.S. diplomatic or consular mission in a foreign state, or a residence owned or leased by the U.S. and used by a diplomatic or consular mission in a foreign state; or, (b)(6) a judge may "issue a warrant to use remote access to search electronic storage media" outside the jurisdiction in two limited situations: (A) if the location was "concealed through technological means," or, (B) in an investigation of fraud or related activity in connection with computers, the "media are protected computers that have been damaged without authorization and are located in five or more districts." Fed. R. Crim. P. 41(b).

21. Subsection (b)(3) was adopted in 2002 in response to the terror attacks of September 11, 2011 as part of the USA Patriot Act of 2001. Subsection (b)(4) was adopted in 2006 to address the use of tracking devices. Subsection (b)(5) was adopted in 2008 to cover parts of United States jurisdiction that are "outside any State or any federal district." Subsection (b)(6) was adopted in 2016 to address "two specific circumstances" where "a magistrate judge in a district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information even when that media or information is or may be located outside of the district." Fed. R. Crim. P. 41, Advisory Committee Notes.

See *Krueger*, 809 F.3d at 1121 ("[T]hat rule grants to magistrate judges the power to do certain specified things—but only if they first have 'authority within the district.'").

D. The Government Is Incorrect That Title III Imposes No Territorial Limits On Cell Phone Wiretaps

The Government nonetheless has continued to dispute that Title III places meaningful territorial limitations on cellular or mobile phone interceptions—which constitute 93% of all interceptions last year. In the court of appeals, the Government argued that the wiretap order in this case was not facially deficient because the cellular telephones were "mobile interception devices" not subject to Title III's territorial limits. Brief of Appellee, 2016 WL 4492935 at *22 (2016). Under the government's view of the statute, a federal district court or state court[22] could authorize surveillance on cell phones located anywhere in the country without any meaningful limits.

The Tenth Circuit correctly rejected that position and concluded that the term "mobile interception device" means a "listening device that is mobile." Pet App. 17a-20a. Applying the plain language of the statute, the court found that the government's interpretation, which would "treat the cell phones themselves as 'mobile interception devices'" is "impossible to square with Title III." *Id.* at

22. Title III sets a floor for any state wire, and preempts more lenient wiretap authority. Title III's jurisdictional limits therefore also prevent states from exercising nationwide authority to tap phones outside their geographic limits.

18a. The Court explained that the "cell phone is the thing being intercepted, not the thing being used to intercept the call." *Id.* at 18a-19a.

Beyond being antithetical to the language and purpose of Title III, the Government's position for nationwide jurisdiction to wiretap cellphones is simply impractical. Just last year, there were 43 million intercepted calls. A central wiretapping forum in only a handful of federal district or state courts could not appropriately handle such a volume of interceptions consistent with Title III's rigorous oversight duties including monitoring reports, minimizing innocent interceptions, ensuring continuing necessity, extensions, and sealing.

III. Congress Imposed The "Automatic Remedy" of Suppression To Enforce the Statute as a Whole

Critically, *suppression is the exclusive statutory remedy for any violation of Title III*. See 18 U.S.C. 2515 ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial * * * if the disclosure of that information would be in violation of this chapter."); 18 U.S.C. 2518(10)(a).[23] As the legislative history of Title III

23. Section 2518(10) provides in pertinent part:

> Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to

makes clear, that statutory suppression remedy is distinct from and in addition to Fourth Amendment protection, and it "is necessary and proper to protect privacy." S. Rep. No. 1097, at 2185; see also *United States* v. *Vest*, 813 F.2d 477, 482 (1st Cir. 1987) ("[W]e believe that if Congress had intended to commit to the courts general authority to create exceptions to section 2515 in the same manner as the court might develop future exceptions to the [F]ourth [A]mendment exclusionary rule, Congress could certainly have said so more clearly."); *United States* v. *Amanuel*, 615 F.3d 117, 125 (2d Cir. 2010) (Title III provides the remedy of suppression for violations of the act that do not amount to constitutional violations).

The 1976 Wiretap Commission found that "the exclusionary evidence rule provided by Title III has been effective in constraining potentially overzealous investigators to conduct their electronic surveillances carefully within the limits of the statute's procedural requirements." 1976 Wiretap Commission at 11-12. The Commission wrote that the chance of a motion to dismiss succeeding "and an entire investigation may thereby be ruined causes investigators seeking convictions to conduct their electronic eavesdropping with the careful procedural limits of Section 2518." *Ibid.* The Commission concluded that the "exclusionary evidence rule has special impact with respect to these searches" and the Commission "believe[d] it should be retained in Title III." *Id.* Indeed,

---

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.

in interpreting the 1934 federal wiretapping statute, this Court in *Nardone* v. *United States*, 302 U.S. 379, 383 (1937), "employed an exclusionary rule to deter [] violations" of the federal wiretap statute. *United States* v. *Patane*, 542 U.S. 630 n.4 (2004) (discussing *Nardone*). The Court in *Nardone* stated that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty." 302 U.S. at 383.

This Court has strictly applied the suppression remedy, noting that "Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures." See *Giordano*, 416 U.S. at 527-528 (suppressing wiretap because law enforcement agents failed to obtain authorization from the required high-level Department of Justice personnel); see also, *e.g.*, *Scurry*, 821 F.3d at 11 (citing to *Giordano* and ordering suppression in light of order's failure to provide identity of authorizing person); *United States* v. *Glover*, 736 F.3d 509, 513 (D.C. Cir. 2013) (citing to *Giordano* and stating that "[s]uppression is the mandatory remedy when evidence is obtained pursuant to a facially insufficient warrant. *There is no room for judicial discretion*." (emphasis added)).

The Tenth Circuit incorrectly held that Title III's territorial limitation was not a "core concern" of Title III, and therefore that suppression was not an appropriate remedy. See *United States* v. *Dahda*, 853 F.3d 1101, 1114 (10th Cir. 2017). Assuming the "core concern" test even applies, the territorial limitation is not just surplusage

or a mere technicality; it is part of the set of carefully subscribed rules devised by Congress to govern and protect privacy. See *North*, 735 F.3d at 218 (DeMoss, J., concurring) (agreeing with defendant that "the district court's lack of territorial jurisdiction 'is not a mere 'technical defect' but is in fact a central and functional safeguard underlying [Title III].'"); *Glover*, 736 F.3d at 515 ("Nor do we think that the jurisdictional flaw in the warrant can be excused as a 'technical defect.'"). As such, suppression is not only an appropriate remedy, it is *the only* appropriate remedy.

* * * *

Wiretapping presents a significant infringement of an individual's right to privacy. That concern continues to grow as wiretapping focuses almost exclusively on cell phones, which carry an individual's most private information along with them. Even more than a search of a home, a wiretap of one's phone can reveal intimate details never imagined by the Founders of this country. Title III balances the privacy concerns against law enforcement needs by allowing wiretaps in narrow situations that are closely monitored by local judges in tandem with the local prosecutors and investigators. Territorial limitations have been recognized for centuries in the common law and the Fourth Amendment as a critical protection against unwarranted government intrusions. Congress carried forward the long-held tradition of decentralized search authority into Title III. The territorial limitation in Title III protects against government overreach by promoting judicial oversight by a local judge in the jurisdiction having the strongest investigative nexus to the monitored device, limiting forum shopping, and dispersing the burdens

and duties of wiretap supervision among the various district courts. This Court should not allow lower courts or prosecutors to disregard the territorial limitation Congress placed in Title III. A wiretap order that lacks those limits is facially invalid, and the evidence collected pursuant to that order must be suppressed under the statute.

CONCLUSION

For the reasons stated above, this Court should reverse the judgments of the United States Court of Appeals for the Tenth Circuit.

Respectfully submitted,

JEFFREY T. GREEN
Co-Chair Amicus Committee
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW
Washington, DC 20036
(202) 872-8600

ILANA H. EISENSTEIN
Counsel of Record
JASON D. GERSTEIN
MARC A. SILVERMAN
DLA PIPER LLP (US)
One Liberty Place
Philadelphia, PA 19109
(215) 656-3300
ilana.eisenstein@dlapiper.com

JENNIFER LYNCH
ANDREW CROCKER
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Counsel for Amici Curiae

APPENDIX

APPENDIX — LIST OF *AMICI CURIAE*

The Electronic Frontier Foundation (EFF) is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF has served as amicus in multiple cases before this Court addressing Fourth Amendment protection for data and communications, including in *Carpenter* v. *United States*, 137 S. Ct. 2211 (2017) (granting certiorari), *Rios* v. *United States*, No. 16-7314 (petition for a writ of certiorari pending), *City of Los Angeles* v. *Patel*, 135 S. Ct. 2443 (2015), *Riley* v. *California*, 134 S. Ct. 2473 (2014), *Maryland* v. *King*, 133 S. Ct. 1958 (2013), *United States* v. *Jones*, 565 U.S. 400 (2012), and *City of Ontario* v. *Quon*, 560 U.S. 746 (2010).

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state

courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.