No. 17-43

IN THE

Supreme Court of the United States

LOS ROVELL DAHDA,

Petitioner,

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 PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

December 7, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts in cases concerning privacy issues, new technologies, and constitutional interests. *See, e.g.*, *Carpenter v. United States*, No. 16-402 (2017) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data); *State v. Earls*, 214 N.J. 564 (2013) (same); *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); *Utah v. Streiff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that it is unreasonable to warrantlessly search a cell phone incident to an arrest); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (arguing that the government bears the burden of establishing the reliability of new investigative techniques used in establishing probable cause for a search); *United States*

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

v. Jones, 565 U.S. 400 (2012) (arguing that warrantless tracking of a car using a GPS device violates the Fourth Amendment); *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (same).

EPIC seeks to ensure that the statutory protections established by Congress to safeguard privacy are fully enforced by the courts. This case presents a fundamental question about the obligation of the courts to comply with the plain text of 18 U.S.C. § 2518(10)(a), the suppression remedy for an interception that is unlawful, supported by insufficient authorization, or not in conformity with authorization or approval. EPIC submits this *amicus* brief in support of petitioners.

SUMMARY OF THE ARGUMENT

In recent years, this Court has considered several important privacy cases, arising from new technologies, that present important constitutional questions. This is not such a case. This case is about the authority of Congress to enact statutes to safeguard privacy. The suppression and exclusion provisions in the Wiretap Act, 18 U.S.C. §§ 2515, 2518(10), are broad and unambiguous, and it is the responsibility of the courts to ensure they are enforced. Congress has made clear that wiretap orders cannot authorize surveillance beyond a court's jurisdictional boundary. Any order that does is facially invalid and triggers suppression of evidence under the plain text of § 2518(10). If the government wishes a different outcome, then it should go to Congress to revise the statute. It is not for the Court to undo the statutory provisions.

The Wiretap Act was enacted by Congress in 1968 to respond to this Court's rulings in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967). The purpose of the Act is to protect the privacy of communications, to strictly limit unauthorized and unlawful interception, and to ensure meaningful enforcement of statutory rights. Congress has subsequently amended the Wiretap Act on several occasions, and may choose to do so again to provide, for example, specific rules governing cell phone location information. But it is not for the courts to create atextual exceptions to the suppression and exclusion provisions in the Wiretap Act. The lower court's decision should be overturned.

ARGUMENT

I. Congress enacted broad and unambiguous suppression and exclusion provisions in the Wiretap Act to minimize unlawful or unauthorized surveillance and to ensure compliance with the Act.

The provisions for exclusion and suppression in Sections 2515 and 2518 are "integral" to the privacy regime established in the Wiretap Act. S. Rep. 90-1097, at 96 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2185 ["Senate Committee Report"]. The statutory provisions are intended to minimize unlawful or unauthorized interception and ensure compliance with the Act. There is no basis in the text, history, or purpose of the Wiretap Act for judicially manufactured limitations on the law's unambiguous provisions. In the privacy realm, the Court appropriately determines the bounds of the Fourth Amendment. But the Court should leave it to Congress to make changes to privacy protections established by statute.

The "core purpose" of the Wiretap Act is to strictly limit unlawful or unauthorized interception and to "protect the privacy of individuals by banning eavesdropping other than by duly authorized law enforcement officers who complied with the safeguards provided by the law." Edith J. Lapidus, *Eavesdropping on Trial* 7 (1974). The law accomplishes this in three distinct ways: (1) by generally prohibiting unauthorized interception and providing for civil remedies, 18 U.S.C. §§ 2511, 2520; (2) by criminally sanctioning both unlawful interception and the facilitation of unlawful interception through manufacture and distribution of "intercepting devices," 18 U.S.C. §§ 2511, 2512; and (3) by establishing specific procedures that courts and law enforcement officers must follow in order to be authorized to intercept communications in criminal investigations, 18 U.S.C. §§ 2516–18. In order to ensure that these rules would be enforced, Congress provided a full range of remedies: damages, criminal penalties, injunctive relief, and suppression of evidence derived from an unlawful or unauthorized interception. Congress also established an extensive reporting scheme to facilitate public oversight of the use of Wiretap authority. 18 U.S.C. § 2519. *See generally* EPIC, *Wiretapping* (2017).[2]

Congress made clear from the outset that the exclusionary rule is essential to the Wiretap Act's robust privacy protections and therefore should not be limited. The Senate Judiciary Committee described the broad exclusionary provision in § 2515 as "necessary and proper to protect privacy" and "an integral part of the system of limitations designed to protect privacy." Senate Committee Report, *supra*, at 96. Pri-

[2] https://epic.org/privacy/wiretap/.

or to 1968, the idea of authorizing interception of private communications was so controversial that Congress failed repeatedly to pass any statutes authorizing wiretapping. *See* Edward V. Long, *The Intruders* 153–54 (1967); Lapidus, *supra*, at 11.

Congress intended section 2518(10)(a)—the provision that provides standing to file a motion to suppress—to provide "the remedy for the right created by section 2515." Senate Committee Report, *supra* at 106. The Senate Committee Report cautioned that "[o]nly by striking at all aspects of the problem can privacy be adequately protected." *Id.* at 69. Accordingly, the law provides for criminal, civil, and evidentiary remedies. *Id*. These three remedies were intended "to guarantee that the standards of the new chapter will sharply curtail the unlawful interception of wire and oral communications." *Id*. at 96.

Congress also intended the exclusionary rule to be a sanction for those law enforcement officers that engaged in unlawful wiretapping. The report describes section 2515's exclusionary rule as an "evidentiary sanction." *Id*. The Senate report also states that the "perpetrator must be denied the fruits of his unlawful action in civil and criminal proceedings." *Id*. at 69. This indicates that Congress intended the provision to have a deterrent effect on officers, preventing future unlawful wiretapping. These strict limitations on the use of wiretap evidence are consistent with the law that existed post-*Olmstead*. *See* Samuel Dash, *The Eavesdroppers* 387–400 (1959) (discussing Section 605 of the Federal Communications Act and the early post-*Olmstead* cases interpreting the exclusionary rule).

When Congress ultimately adopted sections 2515 and 2518(10), it used unambiguous language that prohibits the use of evidence obtained in violation of Title III; those provisions should be applied broadly and without exception. The Senate indicated "that *all* unauthorized interception of such communication should be prohibited, as well as the use of the contents of unauthorized interceptions as evidence in courts and administrative hearings." Senate Committee Report, *supra*, at 89 [emphasis added]. Indeed, the only limitation on the broad exclusionary rule is the requirement that the movant be an "aggrieved person" under 18 U.S.C. § 2510(11). As the Senate Committee Report explained, they did not intend "to change the general rule" governing grand jury proceedings or "to grant jurisdiction to Federal courts over Congress itself," but provided that "[o]therwise the scope of the provision is intended to be comprehensive." Senate Committee Report, *supra*, at 106. Judicially crafted exceptions to the exclusionary rule on the basis of a change in technology would be inconsistent with this intent for a comprehensive scope.

The meaning of the exclusion and suppression provisions in the Wiretap Act are also informed by the cases that preceded their adoption. Although members of the Court have subsequently disagreed over the scope of the constitutional exclusionary rule, the statutory rule in the Wiretap Act should be interpreted based on both its text and the law as it existed in 1968. In the decade leading up to the Act's passage, the Court in *Mapp v. Ohio*, 367 U.S. 643 (1961), established that "the exclusionary rule is an essential part of both the Fourth and Fourteenth Amendments." *Mapp*, 367 U.S. at 657. Justice Black's concurring opinion in *Mapp* noted that "when the Fourth

Amendment's ban against unreasonable searches and seizures is considered together with the Fifth Amendment's ban against compelled self-incrimination, a constitutional basis emerges which not only justifies but actually requires the exclusionary rule." *Id.* at 662 (Black, J., concurring). The Court had previously recognized this right as stemming from a combination of Fourth and Fifth Amendment protections. *See Agnello v. United States*, 269 U.S. 20, 33–34 (1925) ("It is well settled that, when properly invoked, the Fifth Amendment protects every person from incrimination by the use of evidence obtained through search or seizure made in violation of his rights under the Fourth Amendment.").

As Justice Stewart explained in his seminal lecture, the exclusionary rule serves an important deterrent function that is not matched by other remedies—criminal prosecutions, injunctions, and civil damages—which have a limited application in the law enforcement context. *See* Potter Stewart, *The Road to Mapp v. Ohio and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 Colum. L. Rev. 1365, 1386–89 (1983). Criminal prosecutions are seen as a severe penalty for law enforcement officers, and thus are limited to "willful" violations. *Id*. at 1386. Injunctions require proof of widespread constitutional violations to establish likelihood of a future violation. *Id*. at 1389. And civil damages are both expensive to pursue and difficult to prove due to deference given to law enforcement officers. *Id*. at 1387–88.

Justice Stewart, writing for the Court in *Elkins v. United States*, 364 U.S. 206 (1960), found that the exclusionary rule "compel[s] respect for the

constitutional guaranty in the only effectively available way—by removing the incentive to disregard it." *Elkins*, 364 U.S. at 217. The exclusionary rule is constitutionally required not as a right "but as a remedy necessary to ensure that those prohibitions are observed in fact." Stewart, *supra*, at 1380. Whether the exclusionary rule is understood as a right enshrined in the Constitution or as a remedy that is constitutionally required to make the Fourth Amendment meaningful in practice, it was well established by 1968 that an exclusionary remedy was necessary to preserve privacy.

Congress enacted the broad exclusionary rule in the Wiretap Act following the expansion of the remedy in *Mapp v. Ohio* and prior to any of the subsequent limitations imposed in the constitutional context. After *Elkins*, *Mapp*, and *Miranda v. Arizona*, 384 U.S. 436 (1966), the broad scope and application of the suppression remedy was solidified. That is the broad principle that Congress embraced in Title III. As Professor Murphy explained, "the exclusionary rule was effectively mandated as regards Title III, because *Katz v. United States* and *Berger v. New York* had already made it clear that improper wiretapping violated the Constitution." Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485, 522 (2013).

The Court has had occasion since that time to qualify somewhat the availability of exclusion as a pure constitutional remedy. *See* Aziz Z. Huq, *Judicial Independence and the Rationing of Constitutional Remedies*, 65 Duke L.J. 1, 17–20 (2015). But it is not necessary to impose new limits or qualifications on

the statutory remedy in the Wiretap Act, which have been clearly set out by Congress.

Title III is not the only statute where Congress has chosen to create a suppression remedy. In the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, Congress also enacted a broad and unambiguous exclusionary rule like the one in the Wiretap Act.

> Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

18 U.S.C. § 2710(d). *See* Murphy, *supra*, at 522–26.

It would raise substantial separation of powers concerns for the courts to narrow Congress' authority to enact statutory suppression remedies based on a judicial determination as to the statute's "core" purpose where there is no support in the text or history of the Act to reach such a result.

II. Where Congress has provided a broad and unambiguous suppression remedy, courts should not create atextual exceptions.

The Wiretap Act provides detailed rules that limit the government's ability to intercept private communications. Congress has since updated the law to carry forward the purpose of the 1968 Act and to reflect significant changes in the technology. As Jus-

tice Alito has explained, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *United States v. Jones*, 565 U.S. 400, 427–28 (2012) (Alito, J., concurring) (internal citations omitted). This process of technological refinement in statutory privacy law, where Congress defines protections and courts apply those definitions to emerging technologies, is ongoing and important.

Congress also has the ability to conduct detailed fact-finding and develop clear rules set out in public law. Professors Gray and Citron write, "the law enforcement and privacy interests at stake can be explored in a more expansive and timely manner in the context of legislative or executive rule making processes than they can be in the context of constitutional litigation." David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 110 (2013). Professor Murphy has stated, "Congress has proven more adept than the courts at implementing mechanisms for systemic oversight of privacy practices, as well as for reform of noncompliant institutions." Murphy, *supra*, at 535.

Congress looks to the Court's constitutional guidance to enact privacy legislation "that draws reasonable distinctions based on categories of information or [] other variables." *Riley v. California*, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring). As Justice Alito explained in *Riley,* "The regulation of electronic surveillance provides an instructive example" of Congress's complementary role in defining

privacy protections. *Id.* In 1967, the Court struck down a New York statute because it permitted electronic eavesdropping "without requiring belief that any particular offense ha[d] been or [was] being committed" and without requiring that the "conversations [sought] be particularly described." *Berger v. New York*, 388 U.S. 41, 58-59 (1967). Later that term, the Court held that warrantless eavesdropping on a telephone booth violated the Fourth Amendment because it intruded on the caller's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 358-59 (1967); *id.* at 360 (Harlan, J., concurring).

This Court has recognized the importance of judicial deference and treading carefully so as not to usurp the role of Congress. Chief Justice Roberts emphasized that, "in every case we must respect the role of the Legislature, and take care not to undo what it has done." *King v. Burwell*, 135 S. Ct. 2480, 2495 (2015). Justice Scalia cited Justice Brennan in cautioning "judges [] to refrain from substituting their own interstitial lawmaking." *City of Arlington, Tex. v. FCC*, 569 U.S. 290, 304–05 (2013) (citing *Ford Motor Credit Co. v. Milhollin*, 444 U.S. 555, 568 (1980)). Where Congress has gone through the effort of creating a broad and unambiguous suppression remedy, as it has done in the Wiretap Act, the Court should heed deference to Congress.

Since Title III was enacted in 1968, Congress has passed several amendments to the Wiretap Act, including the Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 ["ECPA"], and the Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994) ["CALEA"]. Congress passed ECPA to "update and

clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. Eight years later, Congress again amended the law, in part, to extend protections "to cordless phones and certain data communications transmitted by radio." H.R. Rep. 103-827, at 10 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3490. In both instances, Congress made the determination that changes in technology had altered the communications landscape in a way that required legislative action.

But Congress has not amended the Wiretap Act to provide for authorization of interception across jurisdictional boundaries. The district court's attempt to do so was a direct violation of the statute, making the order facially invalid. Congress clearly knew how to provide authority for cross-jurisdictional wiretapping where it determined that such authorization was proper. In ECPA, Congress both extended Wiretap Act protections to electronic communications and provided specific authority for the interception of oral communications across jurisdictional boundaries in a specific, narrow context: where law enforcement sought to use a "mobile tracking device." 18 U.S.C. § 2518(3).

The "mobile tracking device" provision was enacted for a specific purpose: to enable the authorization to use "a tap" that is "installed on a vehicle." S. Rep. 99-541, *supra*, at 30. Congress recognized that "[i]n certain cases . . . a device authorized for installation in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation." *Id*. Congress decided in

ECPA that, with an appropriate court order, the government has the authority to complete "installation in the district to which the vehicle has been moved." *Id*. This is precisely the type of narrow solution to a specific problem that Congress is capable of enacting when necessary.

But if a court simply ignores the jurisdictional limitation altogether by refusing to enforce the exclusionary rule when it is violated, then Congress would never have the occasion to review and update the law. Indeed, it is directly contrary to Congress' intent for the court to deny the remedy outlined in the statute (suppression of evidence) even when the jurisdictional limitation provision was violated. Suppression of evidence acquired in violation of Title III is not optional, it is required under the statute. 18 U.S.C. § 2515. Accordingly, the courts should defer to Congress to make any changes to the statutory scheme in response to emerging technologies, rather than adopt an atextual exemption by judicial fiat.

The Court and Congress have long worked together to determine the scope of the right to privacy. Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, Hum. Rts., March 2013, at 7, 10. ("Both courts and Congress share responsibility for safeguarding individuals' privacy from advancing technology and overzealous government surveillance."). The Wiretap Act was drafted in response to this Court's opinions in *Berger* and *Katz*. The drafters considered the cases to be authoritative pronouncements of the necessary procedures for constitutional wiretaps. *See* S. Rep. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (asserting "[i]n the course of the [*Berger*] Opinion the

Court delineated the constitutional criteria that electronic surveillance legislation should contain. Title III was drafted to meet these standards").

In drafting Title III, Congress expressly relied on the factors that the Court set out in *Berger*. S. Rep. 90-1097, 73-75 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2161–63 ("Working from the hypothesis that any wiretapping and electronic surveillance legislation should include . . . constitutional standards, the subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III."). "It was the Court's decision in 1967 that set the course for the modern right to privacy, but it was the congressional legislation the following year that gave meaning to that right." Rotenberg & Brody, *supra*.

It is for the Court to determine the scope of the Fourth Amendment. Congress has codified these decisions into statutes. Title III, for example, "authorizes but imposes detailed restrictions on electronic surveillance." *Riley*, 134 S. Ct. at 2497; *see* 18 U.S.C. § 2510.

Since the enactment of the Wiretap Act, "electronic surveillance has been governed primarily, not by decisions of this Court, but by the statute." *Riley*, 134 S. Ct. at 2497. If Congress has chosen a broad and unambiguous suppression remedy for violations of the Wiretap Act, then it is not for the courts to create atextual exceptions.

CONCLUSION

For the foregoing reasons, EPIC respectfully asks this Court to reverse the decision of the U.S. Court of Appeals for the Tenth Circuit.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

December 7, 2017