[NOT YET SCHEDULED FOR ORAL ARGUMENT]

No. 18–5276

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

JASON LEOPOLD AND
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS,
Appellants,

v.

UNITED STATES OF AMERICA,
Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

No. 13-mc-00712 (Howell, C.J.)

BRIEF OF AMICI CURIAE FIRST AND FOURTH AMENDMENT SCHOLARS IN SUPPORT OF PETITIONERS-APPELLANTS AND IN SUPPORT OF REVERSAL

HANNAH BLOCH-WEHBA*
Assistant Professor of Law
Thomas R. Kline School of Law
Drexel University
3320 Market Street
Philadelphia, Pennsylvania 19143
(215) 571-4819
hbw@drexel.edu
**not admitted in this Court*

CHARLES S. SIMS, *Counsel of Record*
Floyd Abrams Institute for Freedom of Expression
Yale Law School
P.O. Box 208215
New Haven, Connecticut 06520
(203) 436-5831
charles.sims@yale.edu

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), *amici curiae* First and Fourth Amendment Scholars certify as follows:

A. Parties and Amici

All parties, intervenors, and amici appearing in the proceedings below and in this Court are listed in the Brief of Appellants.

B. Rulings Under Review

References to the rulings at issue appear in the Brief of Appellants.

C. Related Cases

This case has not previously been before this Court or any other court. Counsel are not aware of any related cases currently pending in this Court or in any other court within the meaning of Circuit Rule 28(a)(1)(c).

DISCLOSURE STATEMENT

Pursuant to Circuit Rule 26.1, *amici curiae* state that none of the *amici* is a corporate entity.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

INTEREST OF THE AMICI CURIAE

Amici curiae First and Fourth Amendment scholars submit this brief pursuant to Rule 29 of the Federal Rules of Appellate Procedure. *Amici curiae* are law professors whose work concerns privacy, technology, and constitutional law. They have an interest in seeing that the Electronic Communications Privacy Act (which includes the Stored Communications Act and Pen Register Act) is interpreted consistently with the right of access to judicial records under the First Amendment and the common law. A list of the *amici* legal scholars is provided in the Appendix. [1]

This brief is filed with the consent of all parties pursuant to Rule 29(a). Pursuant to Federal Rule of Appellate Procedure 29(c)(5), *amici* certify that no party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting this brief, and no person—other than *amici*, their members, or their counsel—contributed money that was intended to fund preparing or submitting this brief.

[1] This brief has been prepared and joined by individuals affiliated with various law schools, but it does not purport to represent any school's institutional views.

INTRODUCTION

Amici curiae legal scholars, whose research, teaching, and writing focus on privacy, technology, and constitutional law, write to assist the Court by providing important context for the petitioners' appeal. Materials related to court-authorized surveillance pursuant to the Stored Communications Act, 18 U.S.C. § 2703, and the Pen Register Statute, 18 U.S.C. § 3123, commonly remain under seal long after the criminal investigation to which they are related concludes. The petitioners seek to unseal the docket numbers, applications, and court orders authorizing such surveillance with respect to these concluded investigations. Even the Government has recognized that this secrecy frequently endures far longer than is necessary.

The district court correctly concluded that the materials at issue are judicial records. *Matter of Leopold to Unseal Certain Elec. Surveillance Applications & Orders*, 300 F. Supp. 3d 61, 92 (D.D.C. 2018), *reconsideration denied sub nom. Matter of Leopold*, 327 F. Supp. 3d 1 (D.D.C. 2018). The court erred, however, in concluding that the surveillance materials at issue are not analogous to "traditional search warrants," and therefore are not subject to the First Amendment right of access to judicial records. 300 F. Supp. 3d at 91. In deciding that the surveillance applications and orders sought in this case are "more akin to subpoenas," the district court mistakenly relied upon differences between the statutory framework that governs searches of records held by third-party communications service

providers and the framework for "traditional," physical searches and seizures of records held by a "first party." *Id.* The district court overlooked important statutory context and background that underscores a critical point of similarity with search warrants: all of the applications at issue in this case require *ex ante* review by a neutral magistrate before the Government can engage in surveillance. Reviewing this context makes plain that Congress intended to heighten judicial oversight and scrutiny of communications surveillance, not to water it down.

In its recent decision in *Carpenter v. United States*, the Supreme Court declined to make constitutional protections contingent on the formalistic distinctions between search warrants and subpoenas. 138 S. Ct. 2206 (2018). In *Carpenter*, the Court considered—and rejected—an argument that searches of records held by third-party communications service providers do not require a search warrant because they are effectuated through subpoenas. *Carpenter* calls into question the validity of the district court's approach, which would condition the public's First Amendment right of access on the form of legal process rather than its substance.

The court compounded these errors by making sweeping generalizations regarding the need for secrecy of law enforcement surveillance. Contrary to the district court's suggestion, secrecy of judicial records concerning surveillance is neither required nor supported by the statute or by the Fourth Amendment. Indeed,

ECPA's secrecy provisions neither require nor permit long-term, indefinite secrecy. Nor does unsealing of the materials petitioners seek conflict with ECPA's privacy protections for subscribers and customers. Continued sealing is more properly achieved through limited, narrow, and tailored redactions than through wholesale secrecy. Finally, secrecy undermines ECPA's goal of promoting effective judicial oversight by hampering understanding of new surveillance technologies. The relief petitioners seek would promote needed transparency regarding surveillance practices that is essential to vindicating Fourth Amendment rights and values.

Amici applaud the court's adoption of new procedures that will increase transparency concerning the use of the surveillance authorities at issue in this case. 300 F. Supp. 3d at 103–05. But while the prospective changes the district court has adopted will make docketing information and statistical data concerning the use of surveillance authorities more widely available, they do not remedy the court's failure to recognize that the public interest requires transparency regarding surveillance applications and orders as well. *Amici* respectfully urge this Court to reverse the district court's categorical rejection of access to applications, warrants, and orders under the Electronic Communications Privacy Act.

ARGUMENT

I.
THE MATERIALS TO WHICH THE PETITIONERS SEEK ACCESS ARE ANALOGOUS TO RULE 41 SEARCH WARRANTS

The records to which Leopold seeks access—warrants and orders issued under the Stored Communications Act, 18 U.S.C. § 2703(a), (d), and court orders issued under the Pen Register Statute, 18 U.S.C. § 3123—bear all the hallmarks of judicial records to which a right of access attaches under the First Amendment and the common law. Indeed, the government assumed, and the district court agreed, that the materials at issue are judicial records. *Matter of Leopold*, 300 F. Supp. 3d at 92 ("PR/TT and SCA applications and any supporting materials, which the government submits to obtain the related orders and on which courts rely in deciding whether to enter such orders, undoubtedly meet this standard."). Nonetheless, the district court ruled that the petitioners lacked a First Amendment right of access to unseal these judicial orders because they failed to demonstrate the existence of a "tradition of openness" with respect to the materials. 300 F. Supp. 3d at 86.

The district court reached this determination by rejecting any analogy between "traditional" search warrants and the orders to which the petitioners seek access. *Id.* The court misconstrued the context in which these surveillance authorities were enacted: Congress chose to require heightened judicial oversight

and heightened scrutiny for electronic surveillance because it was convinced that judicial oversight was necessary to protect user privacy. The district court erred in suggesting that the electronic surveillance orders are "too functionally unlike search warrants in issuance, execution or challenge procedures" to be analogous to search warrants. *Id.* at 91. Its determination relies on a formalistic distinction between searches of records in the possession of third parties such as electronic surveillance providers and those of records in the possession of investigative targets. But the Supreme Court has recently rejected that distinction, leaving the district court's rationale without support.

A. SCA warrants, Section 2703(d) orders, and pen register/trap and trace orders require heightened judicial oversight and heightened scrutiny.

ECPA reflects a legislative effort to heighten privacy protections online. In enacting ECPA, Congress opted to require the government to obtain a court order or a search warrant before it could compel the disclosure of some types of user data or compel the installation of a pen register or trap and trace device. This requirement of review by a neutral magistrate, upon a heightened standard of scrutiny, renders SCA warrants, Section 2703(d) orders, and pen/register and trap and trace ("(PR/TT") orders more analogous to search warrants than to subpoenas in important respects.

1. SCA Warrants

When Congress enacted ECPA, existing caselaw suggested that a user retained no expectation of privacy in information sent to third parties, even the contents of emails. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). A separate line of caselaw suggested that the government could, consistent with the Fourth Amendment, compel those third parties to disclose user communications in response to a subpoena. *See, e.g.*, *Newfield v. Ryan*, 91 F.2d 700, 702–03 (5th Cir. 1937) (upholding use of subpoena to compel disclosure of telegrams in the possession of a telegraph company); *United States v. Gross*, 416 F.2d 1205, 1213 (8th Cir. 1969) (upholding use of subpoena to compel disclosure of Western Union records). The Supreme Court had also repeatedly found that eavesdropping on the contents of telephonic communications was a Fourth Amendment "search" that required a warrant. *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967).

As the use of electronic communications began to increase, policymakers raised numerous questions about whether, and to what extent, they were subject to privacy protections. In 1985, the Office of Technology Assessment (OTA) published a report noting that "innovations in electronic surveillance technology have outstripped constitutional and statutory protections, leaving areas in which

there is currently no legal protection against, or controls on the use of, new surveillance devices." Office of Technology Assessment, *Federal Government Information Technology, Electronic Surveillance and Civil Liberties* 12 (Oct. 1985), https://bit.ly/2MBhLDX. The OTA noted that much electronic surveillance required no judicial authorization or other approval. *Id.* Moreover, the OTA observed, "given the unobtrusive nature of surveillance activities, it may be difficult to detect when one's rights have been violated." *Id.*

Congress was likewise concerned that the use of new technologies for electronic surveillance would outstrip constitutional protections. *See* S. Rep. No. 99-541, at 3 (1986) (expressing concern that information in the possession of third party communication services "may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties"). Despite the complete absence of caselaw, Congress predicted—rightly—that the Fourth Amendment likely would apply to email searches. H.R. Rep. No. 99-647, at 22 (Jun. 19, 1986) ("It appears likely, however, that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required.").

In response, Congress enacted ECPA, amending the existing Wiretap Act and creating the two further statutes at issue in this proceeding: the Stored Communications Act (SCA) and Pen Register Act (PRA). P.L. 99-508 (1986). In

1994, it further expanded protections against the compelled disclosure of some forms of online communications metadata, requiring the government to demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." Communications Assistance for Law Enforcement Act, P.L. 103-414 (1994) at § 207(2).

This legislative history underscores important context overlooked by the district court. First, the district court's decision that SCA warrants are "functionally unlike" other search warrants ignores Congress's determination that the constitutional warrant requirements should apply in the SCA. 300 F. Supp. 3d at 88. Under the Stored Communications Act, the government may compel disclosure of the contents of communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703. The SCA explicitly refers to the Rule 41 warrant procedures in the statutory text. As the Department of Justice's guide to searching and seizing computers points out, "investigators must draft an affidavit and a proposed warrant that complies with Rule 41." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*,

Department of Justice Criminal Division Computer Crimes and Intellectual Property Section, 255–262, available at https://bit.ly/2FMX5s2.

Moreover, the requirements for SCA warrants mirror those of the Fourth Amendment in multiple respects. Search warrants must be "issued by neutral, disinterested magistrates," demonstrate probable cause, and describe the items to be searched with particularity. *Dalia v. United States*, 441 U.S. 238, 255 (1979). An SCA warrant cannot be issued on a standard lower than probable cause. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (requiring the government to obtain a "warrant based on probable cause" prior to executing a search of the contents of emails). Nor can an SCA warrant be so broad as to violate the Fourth Amendment's particularity requirement. *See In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 401 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (holding that the government's application for an SCA search warrant complied with the Fourth Amendment's particularity requirement); *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157, 164 (D.D.C. 2014) (same).

The district court's distinction between SCA and so-called "traditional" search warrants rests on two grounds: the "method of execution and opportunity

for pre-disclosure challenge." 300 F. Supp. 3d at 88. But the court overlooks that these differences exist because of Congress's decision to heighten the standards for compelled disclosure of user data held by third parties. If third-party searches were executed like ordinary computer searches—if, in other words, the government could *seize* a communications service provider's entire server in order to conduct a search—they would be profoundly disruptive to business. *See* S. Rep. No. 99-541 at 39 ("This specific standing for the service provider to contest an overly broad order is intended to protect the service provider from unduly burdensome requirements and to permit an impartial judicial officer to evaluate the appropriateness of the government's request."); *see also Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 443 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994) (finding that physical seizure of company computers "virtually eliminated the safeguards contained in" ECPA, and awarding damages to company). In light of these potential burdens, Congress permitted service providers to move to modify or quash a court order if the demand requests records that are "unusually voluminous" or if compliance "otherwise would cause an undue burden" on the provider. 18 U.S.C. § 2703 (West).

If anything, this practical accommodation of service providers' business needs renders SCA warrants *more* similar to "traditional" search warrants in some respects. For example, Rule 41(e)(2) of the Federal Rules of Criminal Procedure

explicitly provides that a warrant may authorize law enforcement to seize or copy electronic records for "later review" at an off-site location. This "two-step" process reflects a need to accommodate a practical reality: as the Advisory Committee's notes to the 2009 amendments reason, computers "commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location." Fed. R. Crim. P. 41(e)(2) advisory committee note. The disclosure of information pursuant to an SCA warrant often poses the same practical hurdle. Accordingly, numerous courts have granted SCA warrants that compel the disclosure of electronic content for a *later* search, reasoning that these searches pose issues analogous to the physical seizure of electronic information. *See, e.g.*, *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d at 165–66; *In the Matter of Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023, 1036–37 (D. Kan. 2016) (analogizing the particularity requirement for SCA warrants to other searches for electronically stored information under Rule 41(e)(2)); *United States v. Deppish*, 994 F. Supp. 2d 1211, 1219–20 (D. Kan. 2014) (comparing SCA search warrant to other Rule 41 warrants authorizing computer searches).

2. PR/TT and 2703(d) Orders

The district court equally failed to appreciate the implications of ECPA's broader statutory context, set forth above, for judicial oversight of the government's use of pen registers, trap and trace devices, and compelled disclosure of non-content user data. The decision below emphasizes that PR/TT and 2703(d) orders do not require probable cause, 300 F. Supp. 3d at 91, but ignores what these provisions actually show: through ECPA, Congress *heightened* the standards for the government to obtain user data. Take the example of the Pen Register Statute. In *Smith v. Maryland*, the Supreme Court held that warrantless pen register surveillance did not constitute a search, and therefore did not trigger Fourth Amendment protections. 442 U.S. 735, 745–46 (1979). In that case, the police had simply "requested" that the telephone company install the pen register, and the company complied. *Id.* at 737 ("The police did not get a warrant or court order before having the pen register installed."). In response, Congress enacted the Pen Register Statute, requiring the government to obtain a court order in order to install a pen register. 18 U.S.C. §§ 3121–27. Likewise, as Professor Kerr has pointed out, the Stored Communications Act also "require[s] the government to obtain a statutory court order to order an ISP to conduct monitoring even without Fourth Amendment protection." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1033 (2010).

ECPA reflects Congress's intention to expand judicial oversight of government surveillance, not unduly constrain it. In each of these contexts, Congress opted to require judicial oversight and approval despite caselaw holding that a subpoena—or even an informal demand, as in *Smith*—would have been constitutionally sufficient. Indeed, the text of the SCA makes plain that Congress was relying upon distinctions between warrants, court orders, and administrative or grand jury subpoenas in conferring different degrees of protections for different types of user information. *See, e.g.*, *In re United States for an Order Pursuant to 18 U.S.C. § 2705(b)*, 289 F. Supp. 3d 201, 207 (D.D.C. 2018) (describing the SCA's provisions as "a sliding scale of protections, such that the legal mechanism law enforcement utilizes and the showing required depend on the kind of information sought"); § 2703(b) (permitting disclosure of communications content *without* notice if the government obtains a warrant, but permitting disclosure *with* notice if the government obtains a court order, administrative subpoena, or grand jury subpoena).

The district court overlooked that the requirement of *ex ante* judicial approval set forth under § 2703(d) and the PRA is common to a warrant regime but distinct from subpoenas. That Congress opted to require neutral magistrates to review and approve surveillance under 2703(d), rather than permitting government to compel disclosure using only a subpoena, underscores its desire to heighten

oversight of these surveillance techniques.[2] Congress's determination that judicial oversight was sound policy—albeit not required by the Constitution—is the basis for the important role that the courts play today in monitoring, overseeing, and facilitating surveillance. That court orders under these authorities do not entirely mirror the substantive requirements for search warrants is of no moment. Without that vital judicial oversight, the statute is clear: no surveillance under either Section 2703(d) or the PRA may take place.

B. The Supreme Court has rejected rigid distinctions based on how a search is executed.

The decision below rested in large part on the district court's distinctions between the procedural requirements of compelled disclosure and of a so-called "traditional search." 300 F. Supp. 3d at 89. According to the district court, two attributes render the electronic surveillance authorities at issue in this case fundamentally distinct from ordinary searches: the method of execution and potential for *ex ante* challenges. Neither of these distinctions, however, support the district court's reasoning. And both exemplify a highly formalist approach to understanding the differences between compelled disclosure and "traditional"

[2] Writing in dissent in *Carpenter v. United States*, Justice Kennedy also echoed that surveillance under the SCA is distinct from an ordinary subpoena: "Here the Government did not use a mere subpoena to obtain the cell-site records. It acquired the records only after it proved to a Magistrate Judge reasonable grounds to believe that the records were relevant and material to an ongoing criminal investigation." 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

searches that is in tension with the Supreme Court's recent decision in *Carpenter*. 138 S. Ct. 2206 (2018).

First, the district court overemphasized a key difference between physical searches and searches of electronic data stored by a third party: unlike a search conducted directly by law enforcement agents, the SCA simply compels the recipient to *disclose* the records sought. 300 F. Supp. 3d at 89–90. But in *United States v. Carpenter*, decided after the district court issued its opinion in this matter, the Supreme Court expressly declined to adopt such a formalistic understanding of the differences between third-party and "traditional" searches. 138 S. Ct. 2206 (2018). *Carpenter* involved a § 2703(d) order seeking to compel the disclosure of over five months of cell-site records for Timothy Carpenter, who was later charged with robbery and weapons offenses. 138 S. Ct. at 2212.

Carpenter undermines the district court's contention that the differences between "traditional searches" and compelled disclosure make them categorically distinct and nonanalogous for constitutional purposes. The *Carpenter* Court rejected the argument, advanced by Justice Alito in dissent, that "compulsory production of records" under § 2703 is categorically not subject to the warrant requirement. *Id.* at 2221; 138 S. Ct. at 2255 (Alito, J., dissenting) (characterizing the compelled disclosure of Carpenter's cell site location records as "at most… a figurative or constructive search") (internal quotation marks omitted). Instead, the

Court analogized the demand for historical cell site location information at issue in that case—a demand that was made under Section 2703(d) of the Stored Communications Act—to other information to which a reasonable expectation of privacy attaches, and held that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party." *Id.* at 2222.[3] Indeed, the Court in *Carpenter* disagreed that the warrant requirement simply does not apply when the Government acquires records using compulsory process." 138 S. Ct. at 2221. In short, the *Carpenter* Court was unconvinced that the formal differences between searches and compelled disclosure of user data were sufficiently significant to overcome any expectation of privacy.

The district court compounded its error when it determined that the statutory motion to quash provided for in Section 2703(d) rendered SCA orders and warrants fundamentally dissimilar from search warrants. Section 2703(d) provides that a service provider may move to quash or modify a court order for disclosure

[3] Nor did the *Carpenter* Court provide any basis for distinguishing between a so-called "traditional search warrant" and the "warrant" provided for in § 2703. The district court attributed significance to the fact that § 2703 "uses the term 'warrant' rather than 'search warrant' in all but one instance." 300 F. Supp. 3d at 90. *Amici* note that the *Carpenter* Court likewise uses the term "warrant" rather than "search warrant," but that there is no apparent meaning to this choice. *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a *warrant supported by probable cause* before acquiring such records.") (emphasis added).

only "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Id.*

Contrary to the district court's suggestion, the SCA does not provide *targets* of a SCA order with notice and the "*ex ante* opportunity to quash," 300 F. Supp. 3d at 89, but rather provides *recipients* with an opportunity to challenge the "appropriateness of the government's request." S. Rep. No. 99-541 at 39 (conferring "specific standing for the service provider to contest an overly broad order"); *see also In re Search of Google Email Accounts*, 99 F. Supp. 3d 992, 996 (D. Alaska 2015) (modifying a search warrant that required Google to review content for relevance before disclosing it to the government). Nor does the SCA's motion to quash provide the target of a search with prior notice, as the district court erroneously suggested. 300 F. Supp. 3d at 89. Indeed, pursuant to Section 2705(b), the government may obtain a "preclusion-of-notice order" that prevents a communications service provider from notifying any person of the existence of a subpoena or order compelling disclosure under the SCA. 18 U.S.C. § 2705(b); *see also Microsoft Corp. v. United States Dep't of Justice*, 233 F. Supp. 3d 887, 908 (W.D. Wash. 2017) (concluding that Microsoft had alleged a "facially plausible" claim that § 2705(b) orders pose an "impermissible burden" on its First Amendment rights). These secrecy orders do not, however, diminish the rights of

the recipients to move to modify or quash unnecessarily burdensome government requests.

In any event, the district court offered no reason why recipients' ability to challenge SCA warrants and 2703(d) orders should diminish, rather than enhance, the petitioners' claim of a right of access to the related materials. The challenges brought by recipients of SCA orders are frequently quite public.[4] Indeed, these cases illustrate a longstanding norm of open disputes regarding the application of the SCA, during which the district court frequently makes available precisely the same information petitioners seek in this case: case numbers, case names, docket

[4] *See, e.g.*, *In re Search of Information Associated with Facebook Accounts DisruptJ20, Lacymacauley, and Legba.Carrefour that is Stored at Premises Controlled by Facebook, Inc.*, No. 17 CSW 658, 2017 WL 5502809, at *10 (D.C. Super. Nov. 09, 2017) (denying, in public opinion, accountholders' motion to intervene and quash warrants for Facebook accounts in investigation related to Inauguration Day protests); Rachel Kurzius, *Prosecutors Are Demanding Facebook's Data On Inauguration Protesters. The ACLU Is Trying To Stop Them*, DCIst (Sept. 28, 2017, 1:49 P.M.), https://bit.ly/2sJuniS; Kate Conger, *Justice Department Drops Request for Names of People Who 'Liked' Anti-Trump Facebook Page*, Gizmodo (Oct. 13, 2017, 6:30 P.M.), https://bit.ly/2OJOeLD; *see also In re United States for an Order Pursuant to 18 U.S.C. § 2705(b)* ("*Airbnb*"), 289 F. Supp. 3d 201, 211 (D.D.C. 2018) (concluding that Airbnb is a provider of "electronic communication services" subject to the SCA); *In re United States for an Order Pursuant to 18 U.S.C. §2703(d)* ("*Royal Caribbean Cruise Lines*"), No. MC 17-2682 (BAH), 2018 WL 1521772, at *6 (D.D.C. Mar. 8, 2018) (concluding that Royal Caribbean Cruise Lines is a provider of "electronic communication services" subject to the SCA).

information, and assigned magistrate judges.[5] Far from undermining the petitioners' right of access, current practice in the district court appears to illustrate the modest nature of the relief petitioners seek, and the value of disclosure to an ongoing public debate about electronic surveillance.

II.
POST-HOC SECRECY OF JUDICIAL RECORDS CONCERNING SURVEILLANCE IS UNNECESSARY AND UNWISE

The district court misconstrued ECPA as a "statutory framework that broadly prioritizes law enforcement's need for secrecy over the public's interest in transparency." 300 F. Supp. 3d at 87. This sweeping generalization misreads the statutory text and betrays common sense. No provision of ECPA requires secrecy after an investigation has concluded. Nor does the relief petitioners seek either conflict with or undermine the statute's protections for customer and subscriber privacy.

A. ECPA neither requires nor permits long-term, indefinite secrecy.

Contrary to the district court's sweeping interpretation, the secrecy provisions relevant to this matter are narrow and specific. Under the SCA, the Government may obtain an order delaying or precluding notice to a target. 18

[5] *See, e.g.*, *Royal Caribbean Cruise Lines*, Misc. No. 17-mc-2682 (Nov. 29, 2017), Dkt. 2 (unsealed opinion of Magistrate Judge Robinson); *Airbnb*, Misc. No. 17-mc-2490 (Oct. 11, 2017), Dkt. 2 (unsealed opinion of Magistrate Judge Robinson).

U.S.C. § 2705. Under the PRA, a PR/TT order shall be "sealed until otherwise ordered by the court." 18 U.S.C. § 3123(d)(1). The statutory text explicitly anticipates that, at a later point in time, secrecy will no longer be necessary or appropriate. *See* 18 U.S.C. § 2705(a)(4), (b) (providing for extensions of the delayed-notice timeframe, but only if the court determines that disclosure would result in one of the serious harms enumerated in the statute);
18 U.S.C. § 3123(d)(1) (sealing endures "until otherwise ordered by the court").

Recent changes in Department of Justice policy regarding Section 2705 nondisclosure orders also confirm that the district court's overly broad interpretation of ECPA's secrecy provisions is unwarranted. In recent litigation in the 9th Circuit, Microsoft challenged the constitutionality of Section 2705, claiming that it had received over 3,250 secrecy orders over a twenty-month period. First Am. Compl. ¶ 5, *Microsoft Corp. v. U.S. Dep't of Justice*, No. 2:16-cv-00538-JLR (W.D. Wash. 2017), Dkt. 28. In response, the Department of Justice adopted a new policy stating that each nondisclosure order "should extend *only as long as necessary to satisfy the government's interest.*" U.S. Dep't Of Justice, Office of the Deputy Attorney Gen., Policy Regarding Applications For Protective Orders Pursuant To 18 U.S.C. § 2705(B) (2017), https://perma.cc/4VLZ-CXSE (emphasis added).

In short, both the statutory text and Department of Justice policy confirm that ECPA's secrecy provisions are narrow, not broad. No provision of ECPA requires secrecy after an investigation has concluded.

B. Unsealing of materials related to SCA warrants, 2703(d) orders, and PR/TT orders does not conflict with ECPA's subscriber privacy protections.

ECPA's regime for protecting the privacy interests of subscribers and customers neither requires nor permits indefinite, permanent sealing of the information sought by petitioners. In the only case to address the issue, Judge Wilson opined that transparency regarding § 2703(d) orders conflicted with ECPA's "essential purpose" of protecting user privacy. *In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D)* ("*Appelbaum*"), 707 F.3d 283, 295 (4th Cir. 2013) (Wilson, District J., concurring).

This Court should reject Judge Wilson's reasoning. ECPA's privacy-protective goals simply do not conflict with the petitioners' request for access to PR/TT, Section 2703(d), and SCA warrant materials. As an initial matter, the petitioners have agreed that *any* personally-identifiable information—even that not covered by ECPA—may be redacted. *See* Supp. Mem., Dkt. 47, at 19. Furthermore, by their very nature, the applications and orders at issue in this matter reflect requests to compel the disclosure of information covered by ECPA; they are unlikely to contain information that has already been disclosed. Unsealing the

records that petitioners seek would not reveal the contents of communications, dialing, routing, addressing, or signaling information, or customer or subscriber records. Indeed, most applications reveal no sensitive information about communications content or customer records at all. *See, e.g.*, *Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(D),* No. 1:15-mc-01028-AK (D.D.C. filed Aug. 6, 2015), Dkt. 1. In the rare case in which unsealing would conflict with the privacy protections set forth in ECPA, redaction of the records is more than sufficient to address that need.

Finally, *amici* note that courts around the nation have successfully grappled with the challenge of balancing the competing objectives articulated by the district court in the decision below. Many district courts have adopted rules or practices that provide for routine eventual unsealing of search warrants, including SCA warrants. *See, e.g.*, E.D. Mo. R. 83–13.05(3); S.D. Ala. L. R. 5.2(d)(5) (providing for routine unsealing of all sealed documents after 120 days). Others, such as the District of Minnesota, appear to routinely unseal dockets for electronic surveillance applications.[6] The inconsistent approaches adopted by district courts merely highlight that there is more than one way for courts to accommodate law enforcement needs, subscriber and customer privacy, and the public's right of

[6] *USA v. Electronic Investigation*, 0:13-mj-00720-LIB (D. Minn. filed Nov. 1, 2013); *USA v. Search Warrant*, No. 0:16-mj-00088-SER (D. Minn. filed Mar. 1, 2016), Dkt. 1.

access. *See* Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93 Wash. L. Rev. 145, 162–63 (2018) (describing the different approaches adopted by different districts).

C. Transparency regarding surveillance practices is critical to upholding Fourth Amendment values.

Long-term secrecy is not only unnecessary to effectuate ECPA's privacy protections, but also impedes ECPA's goal of promoting judicial oversight by preventing judges from keeping pace with evolutions in surveillance technology. Cell site simulators, colloquially known as "stingrays," provide a powerful example. Stingrays are portable devices that act as cell phone towers, connecting with nearby cell phones and collecting information about incoming and outgoing traffic. For decades, law enforcement routinely entered into nondisclosure agreements with Stingray manufacturers, and failed to disclose that they were using Stingrays when they applied for court orders to conduct communications surveillance. *See* Barry Friedman, *Secret Policing*, 2016 U. Chi. Legal F. 99, 103–04 (2016). As a result, few cases discussed how Stingrays worked, and whether law enforcement should seek a PR/TT order or a search warrant in order to use one. *See, e.g.*, *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) ("Based on the statutory language and the limited case law analyzing this issue, a pen register does not apply to this type of electronic

surveillance."). One magistrate judge in the Northern District of Illinois, issuing an order imposing minimization requirements for the use of stingrays, noted that the "dearth of case law discussing these devices" prevented the court from even being aware of whether "judges may be allowing the use of cell-site simulators without possessing a complete understanding of the device and how it works." *United States*, 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015). Other novel techniques pose the same question: what is the appropriate statutory vehicle for law enforcement to seek judicial authorization to engage in surveillance?

Widespread sealing prevents judges from fully understanding how new technologies operate and how they should apply existing law in a rapidly changing ecosystem. As former magistrate judge Brian Owsley has written, "Even magistrate judges have a difficult time ascertaining how other judges are addressing these issues. Instead, we must rely on word-of-mouth and caucusing with various colleagues." The Honorable Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 41 (2013).

By preventing the free flow of information, sealing also threatens to hinder the development of sound caselaw. As early as 1928, Justice Brandeis raised concerns that an "unduly literal construction" of the Fourth Amendment would be

insufficient to respond to the evolution of new surveillance methods. *Olmstead v. United States*, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting). More recently, the Court recognized that if Fourth Amendment doctrine failed to keep pace with law enforcement innovation, citizens would be left "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001); *see also United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) ("The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). Secrecy compounds these concerns by shielding new surveillance methods from view even by those whom Congress has tasked with oversight.

Hampering judicial understanding—and public debate—regarding these technologies has pernicious effects. As this Court has recognized, the right of public access to judicial proceedings and records reassures the public that "standards of fairness are being observed." *Dhiab v. Trump*, 852 F.3d 1087, 1101–02 (D.C. Cir. 2017) (Rogers, J., concurring) (citing *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984)). That interest is no less important with respect to law enforcement's use of surveillance than with respect to other kinds of proceedings relating to the criminal process.

CONCLUSION

For the aforementioned reasons, *amici* urge the Court to reverse the district court's decision.

Dated: January 25, 2019

Respectfully submitted,

/s/ Charles S. Sims
CHARLES S. SIMS,
Counsel of Record
Floyd Abrams Institute for Freedom of Expression
Yale Law School
P.O. Box 208215
New Haven, Connecticut 06520
(203) 436-5831
charles.sims@yale.edu

HANNAH BLOCH-WEHBA
Assistant Professor of Law
Thomas R. Kline School of Law
Drexel University
3320 Market Street
Philadelphia, Pennsylvania 19143
(215) 571-4819
hbw@drexel.edu

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because it contains 5,945 words, excluding the portions of the brief exempted by Fed. R. App. P. 32(f).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

/s/ Charles S. Sims
CHARLES S. SIMS
Counsel for *amici*

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 25th day of January 2019, he caused the foregoing Notice of Intent to File an *Amicus Curiae* Brief to be electronically filed using the Court's CM/ECF system, which served a copy of the document on all counsel of record appearing in the case.

/s/ Charles S. Sims
CHARLES S. SIMS
Counsel for *amici*

APPENDIX (List of Amici Curiae)[7]

Jack Balkin
Knight Professor of Constitutional Law and the First Amendment
Yale Law School

Hannah Bloch-Wehba
Assistant Professor of Law
Drexel University, Thomas R. Kline School of Law

Kiel Brennan-Marquez
Associate Professor & William T. Golden Research Scholar
University of Connecticut School of Law

Barry Friedman
Jacob D. Fuchsberg Professor of Law & Affiliated Professor of Politics
New York University School of Law

Heidi Kitrosser
Robins, Kaplan, Miller & Ciresi Professor of Law
University of Minnesota Law School

Lyrissa Lidsky
Dean & Judge C.A. Leedy Professor of Law
University of Missouri School of Law

Jonathan Manes
Assistant Clinical Professor
University at Buffalo School of Law

Justin Marceau
Professor of Law
University of Denver, Sturm College of Law

Katherine Strandburg
Alfred Engelberg Professor of Law
New York University School of Law

[7] Amici's law school affiliations are stated for purposes of identification only.