No. 20-1499

IN THE
Supreme Court of the United States

AMERICAN CIVIL LIBERTIES UNION
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari to the United States Foreign Intelligence Surveillance Court of Review

BRIEF OF FORMER UNITED STATES MAGISTRATE JUDGES AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

JAMES ORENSTEIN
ZWILLGEN PLLC
183 Madison Ave.
Suite 1504
New York, NY 10016
(646) 362-5590

JESSICA RING AMUNSON
Counsel of Record
TALI R. LEINWAND
ANNA M. WINDEMUTH
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
jamunson@jenner.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*[1]

Amici are former federal magistrate judges. In their capacity as magistrate judges, *amici* frequently confronted government requests for authorization of surveillance and were at the frontlines of addressing novel legal issues arising from new technology. *Amici* have experience publishing opinions that explain the rationale for judicial decisions on surveillance methods without jeopardizing government interests. *Amici* write to urge the Court to grant the petition for certiorari because greater access to opinions issued by the Foreign Intelligence Surveillance Court ("FISC") would promote the orderly development of case law that ensures that the use of new surveillance technologies complies with statutory and constitutional law. This in turn would benefit judges across the country confronting comparable questions regarding the balance of security and privacy. *Amici* include the following:

David K. Duncan served as a United States Magistrate Judge for the District of Arizona from 2001 to 2018. He is a co-author of *The Rights of the Accused Under the Sixth Amendment: Trials, Presentation of Evidence, and Confrontation* (2d ed. 2016).

James C. Francis IV served as a United States Magistrate Judge for the Southern District of New York from 1985 to 2017. He is currently an arbitrator, mediator, and special master at JAMS. Among many other decisions, he authored an opinion of first

[1] All parties received notice of and consented to this filing. No party or party's counsel wholly or partially authored this brief. Only *amici* and counsel for *amici* funded its preparation and submission.

impression about the use of a warrant to access emails stored on servers in a foreign country, *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), as well as an opinion regarding the government's novel request for cell tower dumps, *In re Application of U.S. for an Order Pursuant to 18 U.S.C. §§ 2703 (c) & 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS, & Verizon Wireless to Disclose Cell Tower Log Info.*, 42 F. Supp. 3d 511 (S.D.N.Y. 2014).

James Orenstein served as a United States Magistrate Judge for the Eastern District of New York from 2004 to 2020. He is currently a Senior Legal Director at ZwillGen PLLC. He authored published decisions on location tracking, non-disclosure orders under the Stored Communications Act, and compelled decryption of mobile devices. *See In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010); *In re Grand Jury Subpoena to Facebook*, No. 16-MC-1300 (JO), 2016 WL 9274455 (E.D.N.Y. May 12, 2016); *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

Brian L. Owsley served as a United States Magistrate Judge for the Southern District of Texas from 2005 to 2013. He is currently an Assistant Professor of Law at the University of North Texas at Dallas College of Law. He has authored published decisions on novel law enforcement techniques including the use of cell site simulators, *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 (S.D. Tex. 2012), and cell tower dumps, *In re U.S.*

ex rel. Order Pursuant to 18 U.S.C. Section 2703(d), 930 F. Supp. 2d 698 (S.D. Tex. 2012). He is also the author of *To Seal or Not to Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Application Orders*, 5 Cal. L. Rev. 259 (2014).

Viktor V. Pohorelsky served as a United States Magistrate Judge for the Eastern District of New York from 1995 to 2015. Before his appointment as a magistrate judge, he had a fourteen-year career as a litigator both in private practice and as an Assistant United States Attorney in the Southern District of New York.

SUMMARY OF ARGUMENT

As the petition for certiorari explains, when determining whether the public has a qualified right of access to judicial documents, courts consider both "experience and logic." *Press-Enter. Co. v. Superior Court of Cal. for Riverside Cty.*, 478 U.S. 1, 8 (1986). *Amici* have a unique perspective on both factors. Like members of the FISC, magistrate judges routinely—and, in an age of rapidly advancing technology, with increasing frequency—rule on *ex parte* applications from the government to deploy innovative surveillance technologies. Drawing upon the judiciary's long history of public access to judicial opinions, magistrate judges have gained experience in making publication determinations regarding opinions on novel issues of law without sacrificing the compelling interest in the integrity of law enforcement investigations. As former magistrate judges, *amici* are in a unique position to explain why public access to such opinions is not merely logical, but critical to the development of the law.

First, for decades, magistrate judges have publicly grappled with government requests for evolving forms of surveillance technology, cognizant that transparency is especially important when addressing unsettled questions of personal liberty. To that end, magistrate judges—including *amici* when they were on the bench—have, over the years, published their reasoning when answering novel questions regarding surveillance requests. And they have managed to do so while simultaneously accommodating compelling governmental interests—separating legal analyses from the confidential facts of ongoing investigations, applying redactions, delaying publication, and consulting government officials along the way. These same tools are available to FISC judges, and the Court should grant this petition to recognize the public's qualified right of access to those judges' opinions.

Second, beyond conferring the democratic benefits addressed in Petitioner's request for certiorari, the Court's recognition of a qualified right of access to FISC opinions would have important implications for magistrate judges across the country. For example, qualified access to FISC opinions would provide magistrate judges with persuasive guidance from Article III judges, mitigating the current unevenness of surveillance law across districts—or, at a minimum, promoting a more efficient and uniform development of the law. This access could help counteract opportunities for forum shopping that arise when prosecutors can unilaterally take judges' duty rotations and perceived views into account in deciding when to submit

applications as well as whether, when, and where to seek review of magistrate judges' adverse rulings.

Petitioner's request for certiorari addresses an issue of extraordinary importance. Absent review by this Court, there is no other court that can articulate and confirm the existence of a qualified right of access to opinions that are likely to become even more relevant as government tracking technology multiplies and evolves. Transparency is especially important to maintaining public trust in this context given the constitutional rights and liberties at stake in a process that otherwise remains opaque and one-sided. To that end, access to significant FISC opinions not only is grounded in constitutional law but also is both feasible and necessary. The Court should therefore grant certiorari.

ARGUMENT

I. *Amici*'s Experiences Demonstrate That Publishing Decisions About Surveillance Technology Can Serve The Public Interest While Also Accommodating National Security Interests.

Amici collectively have decades of experience evaluating government surveillance requests in *ex parte* proceedings, applying both statutory and constitutional law to novel surveillance techniques in published memoranda and orders. In *amici*'s experience, the public's compelling interest in access to significant judicial decisions about surveillance technology can be vindicated without jeopardizing ongoing investigations or broader national security interests.

Amici's experience mirrors an important part of the work of FISC judges, who also assess law enforcement's

compliance with congressional mandates and constitutional requirements under the Fourth Amendment, often without the benefit of an adverse party to inform their decisions. To that end, both magistrate judges and FISC judges operate as gatekeepers, assessing novel search requests from government officials, often before responsive legislation is even on the horizon. *See, e.g.*, *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 475 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016) (holding that law enforcement has statutory authority to require the production of customer cloud data stored abroad years before Congress passed the CLOUD Act to explicitly address lawful uses of overseas data[2]); *In re Warrant to Search a Target Computer at Premises*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (concluding that approving a search warrant to hack a computer suspected of criminal use without location information would violate Federal Rule of Criminal Procedure 41(b)(1), prompting amendments to the rule[3]).

Indeed, Congress relied on similarities between magistrate and FISC judges to establish the constitutionality of the FISC under Article III. *See* Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence, 95th Cong. 26–31 (1978) (statement of John M. Harmon, Asst. Att'y Gen., Office

---

[2] *See* 18 U.S.C. § 2713.

[3] *See* Fed. R. Crim. P. 41(b)(6) & Committee Notes on 2016 Amendment.

of Legal Counsel) (concluding that the proposed FISC was likely constitutional given that its judges would preside over *ex parte* proceedings similar to those in "normal criminal cases"). To ensure public scrutiny and understanding of emerging law enforcement tools, magistrate judges have long publicly articulated or written about decisions of the kind Petitioner seeks—namely, those regarding "significant interpretations of statutory and constitutional law." Pet. at i. This practice of publishing decisions has become even more critical in light of the "bewildering pace" of surveillance technology innovation. *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 137, 144 (E.D.N.Y. 2013). Importantly, the same tools available to magistrate judges in publishing opinions on these issues—for example, redacting or avoiding any mention of highly sensitive facts—are equally available to FISC judges when making disclosure determinations.

A. Magistrate Judges Have a History of Safely Providing Public Access to Opinions on Emerging Surveillance Technology.

The right of access is "qualified" precisely to accommodate countervailing interests. *Amici* and their colleagues have put this principle into practice by publishing opinions on novel surveillance issues while protecting governmental interests. Judges have a variety of tools at their disposal when contemplating publication that they can use to balance competing interests in law enforcement and access. In particular, and when warranted, they may redact identifying information, seal underlying government applications, delay publication, seek input from government actors,

and structure opinions to focus broadly on the statutory and constitutional questions at issue rather than the specific factual nuances that give rise to them. These measures enable expedient and efficient public access without threatening law enforcement aims.

Illustrations of how magistrate judges, including *amici*, have utilized these tools abound in the history of government requests for cellular telephone data. Nearly three decades ago, a magistrate judge issued an opinion on the government's use of a digital analyzer to detect telephone numbers. *In re Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digit. Analyzer*, 885 F. Supp. 197 (C.D. Cal. 1995). The judge concluded that such surveillance did not require a court order under the Fourth Amendment, the so-called "Pen/Trap Statute," 18 U.S.C. § 3122, or the All Writs Act, 28 U.S.C. § 1651, but nonetheless denied the government's proposed order as improperly broad, 885 F. Supp. at 202. The magistrate judge published his reasoning to that effect but sealed the government's application and other filings for 90 days, thus accounting for the potential investigative interference that could have resulted from publication. *Id.*

Subsequently, magistrate judges across a variety of jurisdictions, including certain *amici*, have issued opinions on matters of first impression regarding government requests for cell phone location data. For example, one of these opinions, published by a magistrate judge in the Western District of Pennsylvania, centered on a government request for historical and prospective cell phone subscriber data that the government claimed to have shown was based

on an "articulable, reasonable belief" that such tracking was "relevant to" a criminal investigation, and thus obtainable under the Stored Communications Act, 18 U.S.C. § 2703, and the Pen/Trap Statute. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).[4] The magistrate judge denied the request, finding that the government actually needed to show probable cause under the Fourth Amendment. *Id.* at 585–86. The court reasoned that "law enforcement's investigative intrusions on our private lives, in the interests of social order and safety, should not be unduly hindered," but that those intrusions "must be balanced by appropriate degrees of accountability and judicial review." *Id.* at 587. Recognizing the spectrum of relevant issues, each of which cut differently with respect to publication, the judge redacted the underlying government application "in order not to jeopardize an ongoing criminal

[4] Further examples of publicly issued opinions regarding government requests for cell phone location data include *In re Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info.*, No. 6:08-6038M (REW), 2009 WL 8231744 (E.D. Ky. Apr. 17, 2009); *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134 (D.D.C. 2006); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info.*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

investigation," but issued a public opinion to shine a light on the "issues concerning the statutory and Constitutional regulation of electronic surveillance," the disclosure of which would not "hinge on the particulars of the underlying investigation." *Id.* at 616.

Similar publication practices have become even more prevalent as technology has evolved. In another instance, a magistrate judge in the Southern District of New York grounded his decision to publish an opinion regarding a government request for cell tower data in the emergence of competing—and novel—law enforcement questions. *In re Application of the U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435, 436 (S.D.N.Y. 2005). The court disagreed with other courts that had confronted similar issues, and pointed to such disagreement as a reason why publishing its analysis was particularly important. *Id.* The magistrate judge released an opinion while remaining mindful of law enforcement's investigation; the judge maintained the government's application under seal and focused the analysis on the law rather than on factual nuances specific to the request. *Id.* at 437.

Magistrate judges have published decisions on countless other novel law enforcement technologies and requests using similar publication techniques—omitting identifying information, maintaining certain filings under seal, and focusing their analyses on the broader legal questions at issue. Select examples include opinions analyzing law enforcement's use of:

- Geofiltered data searches—or "geofences"—surrounding particular locations to help identify suspects using cell phone data. *See In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 757 n.17 (N.D. Ill. 2020) (noting that the memorandum opinion and order were initially filed under seal, but were unsealed following consultation with the government); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 349 n.2 (N.D. Ill. 2020) (noting that the warrant remained under seal and that "the Court . . . only generally described the crime and its suspects");

- Biometric data to unlock cell phones. *See In re Search Warrant No. 5165*, 470 F. Supp. 3d 715, 720 (E.D. Ky. 2020) (discussing the "nascent question concerning the constitutionality of compelled biometrics" without disclosing identifying information about the suspect or crime); *United States v. Warrant*, No. 19-mj-71283 (VKD), 2019 WL 4047615, at *1 n.1 (N.D. Cal. Aug. 26, 2019) (specifying that the underlying request remained sealed and inaccessible to amicus); *In re the Search of a Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1018 (N.D. Cal. 2019) (sealing a warrant application and accompanying exhibits regarding the compelled use of biometric data but making the court's analysis "a matter of public record"); *In re Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523, 527 n.3 (D.D.C. 2018) (explaining

why the government's warrant was sufficiently particularized under applicable legal standards without unsealing the warrant);

- Cell phone tracking to identify unknown individuals near a particular place at a certain time through a "tower dump." *See In re U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 2:17-mc-51662 (SW), 2017 WL 6368665, at *2 (Dec. 12, 2017) (noting that the opinion and order were initially sealed); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless to Disclose Cell Tower Log Info.*, 42 F. Supp. 3d 511, 512 n.1 (S.D.N.Y. 2014) (noting that *amici* "were unable to review the actual application at issue," which was "not publicly available"); *In re U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F. Supp. 2d 698, 699 (S.D. Tex. 2012);

- Cell-site simulators or "stingrays" to determine a mobile phone's location. *See In re the Application of the U.S. for an Order Relating to Tel. Use by Suppressed*, No. 15 M 0021 (IJ), 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015) (noting that "the requirements outlined in [the] opinion have not interfered with effective law enforcement"); *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register and Trap & Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

This robust history of magistrate judges publishing opinions on emerging law enforcement techniques shows

that judges have the necessary tools to disclose their own analyses on surveillance-related statutory and constitutional questions while still accommodating law enforcement interests and other related concerns.

B. The Same Tools Available to Magistrate Judges in Weighing Competing Interests, Making Access Determinations, and Ultimately Ordering Appropriate Disclosures, Are Available to FISC Judges.

FISC judges are similarly equipped to issue their own opinions (or redacted versions thereof) without harming law enforcement interests. Although FISC opinions on significant interpretations of law are sometimes declassified under the USA Freedom Act, 50 U.S.C. § 1872(a), such declassification is insufficient to vindicate the public's qualified right of access: it has only been applied to opinions post-dating 2015 and is performed by the executive branch rather than the judges who actually wrote the decisions. It is therefore inherently an insufficient substitute for a judicial determination of the First Amendment's requirements.[5] By contrast, the experiences of *amici* and other magistrate judges illustrate that the judiciary is well-positioned to disclose its own opinions fairly and efficiently on a regular basis.

By their very nature, significant FISC opinions affect more than just the individual(s) involved in a given

[5] Vesting authority to approve the release of decisions solely in the executive branch, given its status as an interested party, may also risk frustrating the law's development for reasons discussed below in Part II.B.

case (whose identities of course can be redacted). Instead, such opinions focus on questions of statutory and constitutional authority that do "not [necessarily] hinge on the particulars of the underlying investigation." *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 748 (S.D. Tex. 2005). Magistrate judges and FISC judges address many of the same legal issues under surveillance statutes and the Constitution. And like magistrate judges, FISC judges are capable of publicly expounding on relevant legal principles without threatening ongoing law enforcement efforts.

Like magistrate judges, FISC judges can initially issue sealed orders and publish opinions at a more appropriate time to explain their reasoning. Similar to magistrate judges presiding over detailed surveillance applications, FISC judges can time the publishing of their decisions to allow for government consultation and minimize the risk of interference. Moreover, to the extent FISC judges are unsure whether publishing certain information would threaten national security, they can seek input from government officials.

It also bears noting that courts—including this Court, the U.S. Foreign Intelligence Surveillance Court of Review ("FISCR"), and federal district courts—have long published opinions describing emerging surveillance technology. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001) (discussing how thermal imagers "detect infrared radiation" and convert such radiation into images based on relative warmth, thus operating "somewhat like a video camera showing heat images"); *In re Certified Question of Law*, 858 F.3d 591,

593–94 (FISA Ct. Rev. 2016) (explaining the government's interception of post-cut-through digits to determine a suspect's dialed telephone number); *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d at 137 (explaining the use of geolocation technology). The automatic sealing of opinions implicating surveillance technology is therefore an over-inclusive and unwarranted approach. To the extent that significant legal decisions implicate technical details unsuitable for publication, such details can be redacted if and when they arise.

In sum, there is already a robust history of disclosing judicial opinions on significant surveillance law questions. FISC judges are part of this same tradition and are well-suited to uphold it.

II. The Court's Review Is Necessary Because Without Access To FISC Precedent, Courts Across Jurisdictions Will Be Deprived Of Relevant Analytic Examples And Will Continue To Decide These Legal Issues In Non-Uniform Ways.

This Court's review is also necessary to bring more uniformity to the law. Surveillance law is replete with conflicting magistrate judge opinions across districts, subjecting the targets of surveillance efforts to widely divergent outcomes that essentially turn on geography or the magistrate judge who happened to be on criminal duty on a given day. Although this irregularity stems in part from disparate approaches to new technology, it also reflects prosecutors' power to effectively shop for magistrate judges and selectively appeal decisions, thus shaping the law as they so choose. By granting a

qualified right of access to FISC opinions, the Court would provide magistrate judges with additional authority on surveillance law issues and reduce the impact of prosecutorial discretion on the law's trajectory.

A. Enshrining a Qualified Right of Access to FISC Opinions Would Provide Judges Deciding Emerging Surveillance Law Issues with Crucial Guidance.

As it stands, the law surrounding government surveillance technology varies significantly across districts. Judges often reach conflicting decisions regarding surveillance questions left unaddressed by Congress. The quickening pace of technological developments is likely to exacerbate that variation, as is the fact that a variety of considerations can cause this Court's resolution of legal issues surrounding novel technology to take years.[6] A qualified right of access to FISC opinions would temper the non-uniformity of

[6] For example, while lower courts confronted the constitutional status of seizures of cell phone location data as early as 2005, *see, e.g.*, *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 756–57, this Court did not provide a uniform ruling on the matter until 2018. *See Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018); *see generally City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

surveillance law by providing rulings from Article III judges that magistrate judges could follow.

An example of surveillance law's irregularity emerged in the face of government requests for post-cut-through dialed digits ("PCTDD") collected under the Pen/Trap Statute, a technique also repeatedly analyzed by FISC judges. *See, e.g.*, *In re Application of the U.S. for Orders (1) Authorizing Use of Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Info.*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007). PCTDD are numbers dialed after a call is initially connected. *Id.* at 328. Sometimes such numbers merely include dialing information, such as extension numbers. *Id.* In other instances, however, such numbers transmit more substantive information such as bank account numbers, Social Security numbers, or prescription numbers. *Id.* In one case before a magistrate judge in the Eastern District of New York, government officials argued that the Pen/Trap Statute authorized the collection of any PCTDD digits, including those with substantive content, so long as law enforcement minimized the collection of such content using reasonably available technology. *Id.* The court determined—as a matter of first impression in the Second Circuit—that government access to PCTDD under the Pen/Trap Statute would violate the Fourth Amendment where there is any chance that content information could be intercepted. *Id.* at 339. A magistrate judge in the Southern District of Texas similarly declined the government's request for PCTDD, but limited his decision to issues of statutory interpretation and applied the constitutional avoidance doctrine. *In re the Application of the U.S. for an Order*

Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 836–37 (S.D. Tex. 2006). Yet another magistrate judge determined that all PCTDD constitute content information and that it was therefore unconstitutional for the government to collect PCTDD (as opposed to the other two judges, who found that only certain types of PCTDD contain content information and therefore raise a constitutional problem). *In re Application of the U.S. for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device on Wireless Tel. Bearing Tel. No. [Redacted], Subscribed to [Redacted], Serviced by [Redacted]*, No. 08 MC 0595 (JO), 2008 WL 5255815, at *3–*4 (E.D.N.Y. Dec. 16, 2008).

Public access to FISC reasoning eventually provided more clarity to judges faced with such requests when the FISCR published its decision on the matter. *See In re Certified Question of Law*, 858 F.3d 591. Contrary to the preceding magistrate decisions, the FISCR determined that the pen/trap provision under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA"), authorizes such requests for PCTDD despite the risk of government access to content information, and that surveillance of this type may, in certain cases, be constitutionally reasonable under the Fourth Amendment without establishing probable cause. *Id.* at 593. Even though FISC judges had been issuing orders that authorized the acquisition of PCTDD "[s]ince at least 2006," magistrate judges were only given access to FISCR's reasoning ten years later when this particular opinion was published. *Id.* at 594. Regular exposure to FISC opinions on such significant interpretations of law

would thus provide greater clarity to judges when first confronting such novel questions, thereby facilitating more uniform application of key surveillance statutes.

Other FISC decisions provide helpful authority for judges outside of the foreign intelligence context by, for example, examining First Amendment questions, *see In re Application of the Fed. Bureau of Invest. for an Order Requiring the Prod. of Tangible Things From [Redacted]*, No. BR 13-25 (JB) (FISA Ct. Aug. 27, 2014), and providing further guidance on what constitutes a Fourth Amendment search in light of novel surveillance technologies, *see In re Application of the Fed. Bureau of Invest. for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 13-158 (MM) (FISA Ct. Oct. 11, 2013).

FISC guidance is additionally important in light of the good-faith exception to the exclusionary rule under the Fourth Amendment. In particular, when law enforcement conducts a search in "objectively reasonable reliance" on a warrant later held invalid, evidence from the search is not excluded. That is because "the exclusionary rule," prohibiting the use of evidence collected in violation of a person's constitutional rights, is "designed to deter police misconduct rather than to punish the errors of judges and magistrates." *United States v. Leon*, 468 U.S. 897, 916–26 (1984). As a result, if a magistrate judge erroneously authorizes a surveillance method that in fact violates a subject's rights, the good-faith doctrine will typically preclude a remedy and thus allow the government to use illegally obtained evidence against a defendant at trial.

The following examples offer useful illustrations of this point. In 2016, a magistrate judge in the Eastern District of Virginia issued a warrant allowing the Federal Bureau of Investigation to search any computers whose users logged into an illegal website. *See* Application for a Search Warrant, *In re Search of Computers that Access upf45jv3bziuctml.onion*, No. 1:15-SW-89 (TB) (E.D. Va. Feb. 20, 2015). The decision spurred "nationwide litigation, producing largely divergent opinions" on its validity. *United States v. Dzwoncyzk*, No. 4:15-CR-3134 (JG), 2016 WL 7428390, at *4 (D. Neb. Dec. 23, 2016) (citing cases). Even though several circuits concluded that the magistrate judge had exceeded her jurisdictional authority[7] and committed a fundamental constitutional error under the Fourth Amendment, they found that the associated evidence would not be suppressed because the good-faith exception applied. *See, e.g.*, *United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017); *United States v. Werdene*, 883 F.3d 204, 218 (3d Cir. 2018); *United States v. McLamb*, 880 F.3d 685, 690–91 (4th Cir. 2018); *United States v. Henderson*, 906 F.3d 1109, 1120 (9th Cir. 2018). The good-faith exception has also prevented defendants from suppressing cell phone location data despite the Court's decision in *Carpenter* that government acquisition of historical location data is a search that requires a showing of probable cause under the Fourth Amendment. *See, e.g.*, *United States v. Carpenter*, 926 F.3d 313, 318 (6th Cir. 2019); *United States v. Hammond*,

[7] Federal Rule of Criminal Procedure 41(b) was amended in 2016 to allow for the issuance of warrants pertaining to computers located in multiple districts. *See* Fed. R. Crim. P. 41(b)(6)(B).

No. 19-2357 (AS), 2021 WL 1608789, at *20 (7th Cir. Apr. 26, 2021); *United States v. Pritchard*, 964 F.3d 513, 529 (6th Cir. 2020); *United States v. Beverly*, 943 F.3d 225, 234–35 (5th Cir. 2019), *cert. denied*, 140 S. Ct. 2550 (2020). The availability of FISC opinions on such issues would have an important impact by providing Article III guidance on the law at an earlier stage of a proceeding, thus reducing the risk that defendants will be convicted and jailed on the strength of evidence that judges should never have authorized the government to collect.

B. Disclosing Significant FISC Decisions Would Reduce the Impact of Prosecutorial Discretion in Shaping Surveillance Law.

Granting the public a qualified right of access to FISC decisions also would reduce the impact of prosecutorial discretion on surveillance law. When government officials need judicial authority under FISA to engage in certain surveillance practices, they can only turn to one court: the FISC. 50 U.S.C. § 1803(b). By contrast, prosecutors seeking approval from magistrate judges for certain surveillance practices pursuant to other statutes can place and time their requests to ensure review by only those judges they subjectively believe will be most sympathetic to their demands. *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 Nw. L. Rev. 1609, 1645 (2012) (proposing the randomization of magistrate judges to prevent law enforcement from seeking out magistrate judges perceived to be sympathetic to government requests). These incentives, which are ripe for manipulation, are exacerbated by prosecutors' unilateral right of appeal in such *ex parte* proceedings. *See* Fed. R. Crim. P. 41(d);

Fed. R. Crim. P. 58(g)(2). In other words, a prosecutor who is dissatisfied with one magistrate judge's order may decline to appeal it if the corresponding circuit is perceived to be unfavorable to law enforcement requests; the prosecutor could instead simply seek out a different magistrate judge for the next request. If confronted with an unfavorable decision in a circuit deemed more likely to side with law enforcement, however, the prosecutor can seek appeal and try to set favorable law.

This scenario played out when the Eastern District of New York upheld a magistrate judge's decision that historical location tracking requires a warrant. *See In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, No. 10-MC-0897 (JO), 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010), *aff'd*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011). The government declined to appeal the decision, thereby avoiding the possibility of an adverse decision that would be controlling law throughout the Second Circuit. Instead, prosecutors pursued surveillance requests from other magistrate judges. By contrast, when a magistrate judge issued a similar adverse ruling in Texas, prosecutors pursued a successful appeal in the Fifth Circuit. *See In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *vacated and remanded*, 724 F.3d 600 (5th Cir. 2013). This pattern indicates that surveillance law, and its prospective trajectory, is particularly vulnerable to the whims of prosecutorial decision-making and strategic objectives rather than judicial review.

Expanded access to FISC opinions could blunt prosecutors' ability to shape the development of the law in this way. In the FISA context, prosecutors do not have the same range of choices they enjoy in traditional courts: when they need the FISC's authorization to use a surveillance method, there is only one judge to whom they can apply. 50 U.S.C. § 1803(a)(1). Further, the greater likelihood that applications will be time-sensitive given the demands of intelligence investigations may make it harder for prosecutors to wait for a judge they subjectively believe may be more agreeable to their view of the law. *Cf.* 50 U.S.C. § 1803(e)(1). In addition, the limited number of FISC judges and the fact that there is only a single court to review FISC rulings means that prosecutors faced with an adverse FISC ruling cannot be strategic in deciding whether to appeal. Unless they are willing to wholly abandon the surveillance method denied by one FISC judge, they must pursue an appeal to the FISCR and risk the adverse appellate ruling. 50 U.S.C. § 1803(a)(1).

Further access to FISC opinions also would allow magistrate judges to cite decisions from a specialized Article III court in support of their reasoning. Instead of having to wait for their circuit court to decide a particular issue—a process subject to the delays described above—magistrate judges could more uniformly draw from FISC authority, thus reducing disparate outcomes across circuits. Granting a qualified right of access therefore would limit the power of prosecutors to shape the law and provide magistrate judges with guidance from Article III judges to support their decisions.

CONCLUSION

Access to significant FISC opinions currently depends on a discretionary and limited declassification process controlled by the executive branch. Yet a history of disclosure on issues of importance by magistrate judges demonstrates that broader access to FISC reasoning through the judiciary is eminently feasible, would mirror past practices of judges in other contexts, and need not come at the expense of national security. The cost of shielding such opinions from public scrutiny, by contrast, remains great. The integrity of criminal proceedings, the uniformity of federal law, and public confidence in our judicial process all hinge on transparency. Access will only become more important as new surveillance technologies, along with novel legal questions, multiply. *Amici* therefore respectfully urge the Court to grant Petitioner's request for certiorari.

May 27, 2021

Respectfully submitted,

JAMES ORENSTEIN
ZWILLGEN PLLC
183 Madison Ave.
Suite 1504
New York, NY 10016
(646) 362-5590

JESSICA RING AMUNSON
Counsel of Record
TALI R. LEINWAND
ANNA M. WINDEMUTH
JENNER & BLOCK LLP
1099 New York Ave., NW
Washington, DC 20001
(202) 639-6023
jamunson@jenner.com