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 *AMICUS CURIAE* MICROSOFT CORPORATION IN SUPPORT OF PETITIONER

Robert M. Loeb
Counsel of Record
Monica Haymond
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street N.W.
Washington, D.C. 20005
(202) 339-8400
rloeb@orrick.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

Microsoft Corporation is a leading innovator and provider of cloud computing services. Cloud technology provides substantial benefits to individuals and enterprises in the United States and around the world by improving efficiency and cybersecurity, and by providing access to the next-generation technologies necessary to innovate and compete. Those benefits dissipate, however, if the public and our foreign allies lose trust in cloud providers and services because key aspects of government surveillance laws are hidden from view.

Microsoft's primary mission is to promote the full potential of the global economy by creating technology that transforms the way people communicate, share, and use data, and that empowers even the smallest team. In pursuit of that goal, Microsoft works closely with the United States and foreign governments to ensure that its products and services are not used for international crime such as terrorism, child exploitation, and nation-state cyberattacks. In turn, Microsoft also serves as a leading advocate for the rights of its enterprise customers to control and make informed choices about their data. *See*, *e.g.*, *Microsoft Corp. v. U.S. Dep't of Just.*, 233 F. Supp. 3d 887 (W.D. Wash. 2017); *In re Application of the United States of*

---

[1] No counsel for a party authored any part of this brief, and no person other than Microsoft Corp. and its counsel made a monetary contribution intended to fund this brief's preparation or submission. Microsoft Corp. timely provided notice of intent to file this brief to all parties, and all parties have consented to the filing of this brief.

America for an Order Pursuant to 18 U.S.C. § 2703(d) at 3, No. 8:19-mc-00682 (D. Md. Feb. 21, 2020), Dkt. 19; *Microsoft's Appeal of Non-Disclosure Orders*, No. 1:20-mc-00349 (S.D.N.Y.) (20 Mag. 7329, 20 Mag. 10620).

In particular, Microsoft has pressed for greater transparency in the scope and meaning of government surveillance laws, and in how those laws are applied. Such transparency fosters both public trust and governmental accountability. To that end, Microsoft petitioned the U.S. Foreign Intelligence Surveillance Court (FISC) for an order permitting it to disclose aggregate statistics concerning orders and directives Microsoft received under the Foreign Intelligence Surveillance Act (FISA) or the FISA Amendments Act. 50 U.S.C. §§ 1805(c)(2)(B), 1881a(h); *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-4 (FISC June 19, 2013), https://tinyurl.com/zh9vh5rv.

Accordingly, Microsoft has a substantial interest in supporting a qualified right of access to the FISC's interpretations of surveillance laws.

INTRODUCTION AND SUMMARY OF ARGUMENT

Cloud services fuel the global economy. The cloud enables enterprises[2] large and small to manage, use, and store data efficiently and at scale. Cloud services provide access to the next-generation technologies (such as artificial intelligence, machine-learning, and quantum computing) necessary for enterprises to compete globally. And the cloud offers cutting-edge cybersecurity protections needed to rapidly spot, mitigate, and remedy cybersecurity attacks—including attacks from authoritarian nation states.

But for enterprises to invoke the full benefits of the cloud, they must be able to trust that they will retain control over their data in the cloud and that they are not putting their data at risk. That requires not just trust in Microsoft's technologies, but also in the legal systems that establish, interpret, and apply the rules limiting government access to data.

When the judicial body charged with interpreting U.S. surveillance laws does not disclose how it interprets key provisions of those laws, distrust mounts. Confusion around when, and of whom, the U.S. government may lawfully conduct electronic surveillance inspires speculation and fear of vast, unchecked powers and abusive practices. Such concerns can deter

---

[2] *See* Dep't of Justice, *Seeking Enterprise Customer Data Held by Cloud Service Providers* (Dec. 2017), https://tinyurl.com/42z7pppj (defining "enterprises" as "companies, academic institutions, non-profit organizations, government agencies, and similar entities").

individuals and enterprises from using cloud technologies and from taking full advantage of the most effective and efficient technologies. This, in turn, threatens to curtail innovation, blunt competitive edge, and stifle economic growth. If enterprises forego use of the cloud and the full panoply of cybersecurity benefits that cloud technology offers, the risk of harm by cyberterrorists and cyber-attacks from hostile nation states will increase.

Greater transparency into the rules that restrict when the government may lawfully access data from cloud service providers would mitigate such harms. If consumers and enterprise customers understand when the government may seek their data from cloud service providers, they can make informed judgments, and they can do so with confidence in cloud service providers and the legal systems that apply to them.

Such transparency is also vital to the proper functioning of our democracy. The public has a right to know the laws that govern the government's surveillance powers and how the FISC construes those laws. A qualified right of access to that information is necessary to hold the government accountable and to prevent government overreach.

Thus, this Court should grant review and recognize that the Constitution provides a qualified right of access to the FISC's interpretations of surveillance laws.

ARGUMENT

I. A Qualified Right Of Access To The Legal Rationale Of FISC Decisions Is Necessary To Promote Public Trust And Avoid Unwarranted Economic Harm.

This Court has recognized that a qualified First Amendment right of access attaches when that right would play a "significant positive role" in the functioning of the judicial system and in promoting public trust. *See Press-Enterprise Co. v. Superior Ct.*, 478 U.S. 1, 9-12 (1986) (*Press-Enterprise II*). A qualified right of access to FISC opinions is essential to promoting public trust in and understanding of the FISA system, as well as in the scope of the U.S. government's ability to surveil data in the cloud. Conversely, allowing the government to withhold how the FISC interprets key aspects of U.S. surveillance law, without any judicial review over the scope of that secrecy, risks jeopardizing trust in the U.S. technology sector and as a result, threatens to harm the economy and public good as a whole.

A. Withholding the FISC's interpretation of surveillance law fuels distrust.

The FISC's interpretations of surveillance law should rarely, if ever, be withheld from the public. Hiding the core legal regime and rules from public view does not serve any legitimate government interest and erodes public trust.

As this Court has long recognized, "[i]t is emphatically the province and duty of the judicial

department to say what the law is." *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 177 (1803). It is also true that the public has a corollary right to know how the judicial department interprets the law. After all, "[o]urs is a nation of laws." *United States v. Higdon*, 638 F.3d 233, 247 (3d Cir. 2011). The governed have a right to know what those laws are and how our judges interpret them.

Public access to judicial opinions interpreting the law is a long-established norm. It is a "fundamental element of the rule of law, important to maintaining the integrity and legitimacy of an independent Judicial Branch." *MetLife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 663 (D.C. Cir. 2017). "At bottom, it reflects the antipathy of a democratic country to the notion of 'secret law,' inaccessible to those who are governed by that law." *Leopold v. United States*, 964 F.3d 1121, 1127 (D.C. Cir. 2020).

Hiding how the FISC construes federal statutes, interprets constitutional provisions, or constructs legal standards creates secret law that is antithetical to our democracy. Lack of access to how the FISC applies the constitution and construes ambiguities in the FISA statute fosters distrust and leaves people to assume the worst.

Notably, the FISA statute contains significant ambiguities. For example, one provision permits the Attorney General and the Director of National Intelligence to electronically surveil communications for "foreign intelligence information," 50 U.S.C. § 1802(a)(1), (b). That provision in turn encompasses standards as broad as information that is necessary

to "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2)(B). The statute, however, does not explain the meaning or limits of the clause "conduct of foreign affairs of the United States." That type of statutory ambiguity necessarily requires judicial interpretation—interpretations that should be shared with the public.

Clarity as to how the FISC interprets "conduct of foreign affairs of the United States" is critical. Does it mean that anytime the Executive invokes those talismanic vague terms a court will defer and allow surveillance? Or has the FISC established meaningful limits and rules? The U.S. public and international enterprises and governments will assume the former absent disclosure of the interpretative aspects of the FISC opinions explaining how it construes that phrase.

Sometimes the Executive Branch tries to assuage concerns by making public statements about how it plans to use its powers. For instance, the Director of National Intelligence has announced that the United States does not "use [its] foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—US companies to enhance their international competitiveness or increase their bottom line." Dir. Nat'l Intel. James R. Clapper, *Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage* (Sept. 8, 2013), https://tinyurl.com/u6cmszew. But such statements do little to alleviate concerns of our foreign allies when the authoritative court interpretations of the laws authorizing electronic surveillance (including the power to collect

information necessary to "the conduct of the foreign affairs of the United States," 50 U.S.C. § 1801(e)(2)(B)) remain hidden from public view. Without a transparent legal regime setting out well-defined rules, those affected deem such assurances unreliable. Shrouding legal interpretations of facially ambiguous statutory language in secrecy will only continue fueling this distrust. *See*, *e.g.*, Edward Alden, *The U.S.-EU Spying Fiasco: Why Commercial Espionage is a Bad Idea for the United States*, Council on Foreign Relations (July 3, 2013), https://tinyurl.com/axebtmcc (noting that foreign leaders threatened to withdraw from negotiations over the Transatlantic Trade and Investment Partnership due to reports of alleged U.S. economic espionage).

There are, of course, compelling national security and public safety reasons for the government to collect intelligence from online sources in certain instances. And our foreign government allies share a mutual interest in investigating, detecting, and preventing terrorism and cyberattacks. *See* President of the United States, *National Strategy for Counterterrorism of the United States of America* 2 (Oct. 2018), https://tinyurl.com/3nxv6hk7. But a qualified right of public access to the FISC's core legal reasoning is a narrow one that will not hamper those efforts. It does not require disclosure of the identities of those targeted by surveillance. It does not require disclosure of the confidential sources who provided information to the government. And it does not require disclosure of the confidential methods the government used for intelligence gathering. It merely requires disclosing the rules of the road—not the tools of the trade.

B. Lack of transparency regarding the limits of U.S. surveillance laws harms the economy and the public good.

Lack of transparency in how the FISC interprets U.S. surveillance laws deters use of cloud technologies, which harms the economy, stifles innovation, and creates greater risks of cyberattacks from data hackers and hostile governments.

Cloud computing services drive today's global economy. Through cloud services, enterprises have streamlined, cost-effective access to highly sophisticated and secure applications and resources. This reduces the need for such enterprises to invest in internal infrastructure or hardware, freeing them to focus their resources on innovating, expanding, and increasing efficiency. More specifically, in 2017, cloud computing added $214 billion to the United States GDP and approximately 2.15 million jobs. Christopher Hooton, *Examining the Economic Contributions of the Cloud to the United States Economy*, Internet Assoc. (Mar. 5, 2019), https://tinyurl.com/yvbca7sb. Just between the United States and Europe, cross-border cloud data transfers "underpin the $7.1 trillion transatlantic economic relationship," making the cloud "indispensable" to how modern-day industry operates and grows. U.S. Dep't of Commerce Int'l Trade Admin., *Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision* (Sept. 2020), https://tinyurl.com/y4jva44r. These numbers are only set to grow, as 60% of the global economy is projected to be digitized by next year. *See* Daniel S. Hamilton & Joseph Quinlan, *The Transatlantic Economy* 2020 ch. 3 at 28 (2020), https://tinyurl.com/236zf7ts.

Every major economic sector—from manufacturing to energy to financial services to agriculture to retail—relies on cloud services to export goods, manage supply chains, and connect with customers. *See* Joshua P. Meltzer & Peter Lovelock, *Regulating for a Digital Economy*, Brookings Global Economy and Development Working Paper 113 (Mar. 2018), https://tinyurl.com/6devxyna. These traditional industries realize 75% of the value created by Internet commerce, enabled by the cloud. McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (May 2011), https://tinyurl.com/49ue45ka. As members of the global industry put it in a joint statement to the World Trade Organization earlier this year, "continued economic development, innovation, and employment depend upon cross-border access to digitally delivered services and technologies." *Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce* 1 (Jan. 26, 2021), https://tinyurl.com/yn9dzx3a.

But the cloud runs on trust. Companies must trust that their trade secrets stored on the cloud are secure. Public health organizations must trust that confidential patient information will not be vulnerable to data breaches and hacks. Foreign governments must trust that their sensitive decision-making and security will not be compromised by their use of cloud computing. And individuals must trust that their private information will remain as such.

Uncertainty in the legal rules for how and when the U.S. government may access data in the cloud erodes this trust. This erosion threatens to deter

consumers, companies (including those who deal with consumers), and our foreign allies from gaining the full benefits of the cloud. *See* Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://tinyurl.com/wj7zxsxx. For instance, some businesses may avoid the cloud without fully realizing that doing so places their data at increased risk of cybersecurity events. *See* Internet Society, *Internet Way Of Networking Use Case: Data Localization* (Sept. 30, 2020), https://tinyurl.com/j74p99zs. Microsoft has cutting-edge cybersecurity capabilities in its cloud, where it has visibility into its cloud platforms and services, enabling it to see over 8 trillion signals every 24 hours. *See* Testimony of Brad Smith, S. Select Comm. on Intel.: Open Hearing on the SolarWinds Hack 5-6 (Feb. 23, 2021), https://tinyurl.com/ax5z4tb8. But Microsoft lacks this level of visibility outside the cloud.

Another consequence of uncertainty in the legal rules governing U.S. surveillance is the risk of incentivizing foreign governments, including allied ones, to restrict cross-border data transfers out of sovereignty and privacy concerns. *See* Linxin Dai, *A Survey of Cross-Border Data Transfer Regulations Through the Lens of the International Trade Law Regime*, 52 N.Y.U. J. Int'l L. & Pol. 955, 958-60 (2019). Disruptions to cross-border data flows create additional harms. For instance, vital health research depends on the rapid transfer of information. Vaccine and other drug researchers rely on sharing research insights. So too, epidemiological research has benefited from near-instantaneous reports of new cases when tracking virus and disease outbreaks. Medical device

manufacturers also rely on cross-border data transfers for research, routine maintenance, and repairs. When that information flow is restricted, patients suffer. And when patients suffer on a large scale—such as during a pandemic—those harms ripple across the economy and nation.

Likewise, financial institutions seeking to identify financial fraud rely on the technology and speed that cloud computing offers. Without that, these institutions lack the tools necessary to recognize connections between transactions that could reveal bad-faith actors. So too, manufacturers would lose the benefits of seamless online communications with suppliers and customers around the world. Those harms, combined with many others, would stifle job growth and lead to economic stagnation, resulting in losses in community welfare. *See* U.S. Chamber of Commerce & Hunton & Williams, *Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity* (2014), https://tinyurl.com/3m2tmb5k.

More broadly, the current lack of transparency into the FISC's interpretations also threatens national security. It undermines the leadership of the U.S. technology sector to the benefit of global competitors, such as those in authoritarian legal regimes like Russia and China. The U.S. government itself has identified the grave security risks inherent in the United States losing its competitive edge and leadership in next-generation technologies.

The U.S. Director of National Intelligence has commented on national security risks caused by increasing flow of data "across foreign-produced

equipment and foreign-controlled networks." Dir. Nat'l Intel. Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, S. Select Comm. on Intel. 5, 16 (Jan. 29, 2019), https://tinyurl.com/hz8655x8 (discussing threats posed by Russia, China, Iran, and North Korea). That significantly "rais[es] the risk of foreign access" to data, meaning access by hostile governments and other bad actors, who may seek to use such access to cripple a company's or agency's computer system. *Id.* Bolstering trust in U.S. cloud services and technology is critical to combatting these risks. Today, the lack of transparency in how the FISC construes U.S. surveillance laws diminishes this trust.

C. Uncertainty in the rules governing U.S. government surveillance has spurred foreign government proposals restricting international data transfers.

The concern that lack of transparency in the rules governing U.S. surveillance law risks disrupting data flows is not an abstract concern. In July 2020, the European Union Court of Justice (ECJ) invalidated the EU-U.S. "Privacy Shield"—a framework that until then had governed cross-border transfers of data. *See Data Prot. Comm'r v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 (Schrems II), https://tinyurl.com/ab7y4k8f. The ECJ concluded that the Privacy Shield failed to adequately protect European citizens' personal data because, according to the ECJ, U.S. law does not guarantee judicial oversight of foreign intelligence surveillance or apply clear standards for when the government may lawfully target individuals' data. *Id.* ¶¶ 64, 198. In the ECJ's view, FISA and

Executive Order No. 12,333 could permit unjustified invasions of privacy without sufficient judicial redress. *Id*. Now companies that transfer data between the United States and countries in the EU must conduct an independent analysis of U.S. law and take sufficient supplemental safeguards to ensure compliance with EU law. *Id.*; *see also* U.S. Dep't of Commerce, et al., *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After Schrems II*, 1 (Sept. 2020).

In the wake of that decision, several nations have proposed policies or amplified earlier measures to restrict international data transfers. Countries in the European Union, for instance, have continued to support proposals for a European-based cloud service, Gaia-X, that would prevent data from being shared with cloud providers who are subject to ambiguous government surveillance laws. *See* Catherine Stupp, *European Cloud Project Draws Backlash From U.S. Tech Giants*, WSJ (Nov. 1, 2019), https://tinyurl.com/e6fk7u3p. Other measures include blocking companies from using cloud computing to aggregate and analyze data, preventing companies from offering services on the global market, limiting the flow of financial services information (and thereby restricting online payments), hampering global supply chains that rely on blockchain, and limiting artificial intelligence by preventing entities from collecting large data sets. *See* Rachel F. Fefer, Cong. Rsch. Serv., R45584, *Data Flows, Online Privacy, and Trade Policy* 4 (Mar. 26, 2020), https://tinyurl.com/eeuwzr8w.

These proposals all restrict use of cloud services, and they do so in no small part due to a lack of clarity in how the FISC is interpreting U.S. laws limiting government surveillance. Disclosure of the interpretative aspects of these FISC rulings would ameliorate many of the concerns motivating such proposals, and, more generally, would promote trust in the U.S. legal system.

II. A Qualified Right Of Access To The FISC's Key Legal Reasoning Will Support Public Accountability And Prevent Governmental Overreach.

This Court should recognize a qualified right of access to the FISC's core legal rationale for the additional reason that such a right would play a "significant positive role" in the functioning of the FISA system. *Press-Enterprise II*, 478 U.S. at 9-12. Disclosing the FISC's interpretations of the key terms of U.S. surveillance laws would ensure that the public has the information necessary to keep the government democratically accountable and to prevent overreach.

The Constitution provides a qualified right of access when such a right would "play[] a particularly significant role in the functioning of the judicial process and the government as a whole." *Globe Newspaper Co. v. Superior Ct.*, 457 U.S. 596, 606 (1982). There is no piece of information more critical to the public's trust in the judiciary than the reasons the court provides for authorizing or limiting government action. "Confidence in a judge's use of reason underlies the public's trust in the judicial institution. A public statement of those reasons helps provide the public

with the assurance that creates that trust." *Rita v. United States*, 551 U.S. 338, 356 (2007); *see also Nat'l Labor Rels. Bd. v. Sears, Roebuck & Co.*, 421 U.S. 132, 161 (1975) (recognizing that the public has an "interest in knowing the reasons for a policy" adopted by its government).

Further, fundamental to this democracy is the concept that governmental power comes from the "consent of the governed." Dec. of Independence. The Constitution's "Bill of Rights denies those in power any legal opportunity to coerce that consent." *West Virginia Bd. of Educ. v. Barnette*, 319 U.S. 624, 641 (1943). Here, the government's use of secrecy subverts those protections: without transparency into the rules of the road, the public can neither ensure sufficient oversight nor give free consent.

More pointedly, the public cannot engage in an informed debate, pass legislation correcting the FISC's interpretation of a statute, or exercise oversight over abusive government surveillance practices if the public lacks information about how the FISC has interpreted U.S. surveillance law. Indeed, information is the cornerstone to being able to "vote intelligently or to register opinions on the administration of government." *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 492 (1975). Denied that, the people have little ability to evaluate the powers being exercised by their own government.

Not surprisingly, Congress has expressed concern with the level of secrecy afforded to attributes of the FISC's legal opinions. In 2015, Congress passed the USA Freedom Act, which requires that the Director of

National Intelligence, in consultation with the Attorney General, conduct a "declassification review" of FISC decisions "that include[] a significant construction or interpretation of any provision of law" and to "make publicly available to the greatest extent practicable" that order or opinion. 50 U.S.C. § 1872(a). But that statute fails to provide for any judicial review of the government's classification decisions. Instead, courts must blindly accept the government's designations, even when those designations include the FISC's interpretations of key aspects of U.S. surveillance laws.

Recognizing a qualified right of access to the FISC's legal interpretations of U.S. surveillance laws would allow courts to scrutinize the propriety of maintaining these aspects of FISC decisions secret. This sort of regime is not out of the ordinary. In fact, the judicial branch already exercises similar oversight over government attempts to prevent disclosure of national security information under the Freedom of Information Act (FOIA). 5 U.S.C. § 552. FOIA exempts from disclosure information that is deemed classified "under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy" and that has been "in fact properly classified pursuant to such Executive order." *Id.* § 552(b)(1). Courts accord "*substantial weight*" to the government's explanation of classification decisions when reviewing challenges in FOIA litigation. *Osen LLC v. United States Cent. Command*, 969 F.3d 102, 114 (2d Cir. 2020) (quoting *Am. Civ. Liberties Union v. Dep't of Just.*, 681 F.3d 61, 69 (2d Cir. 2012)); *see also Krikorian v. Dep't of State*, 984 F.2d 461, 464 (D.C. Cir. 1993). But giving substantial weight to the

government's expertise on national security matters does not mean withdrawing review altogether. Instead, FOIA provides for effective oversight of government classifications by requiring judicial scrutiny of the government's reasons for withholding information.

Without such judicial review, over-classification by the government will remain unchecked, perpetuating continued secrecy of the FISC's legal interpretations of U.S. surveillance laws. As the former U.S. Solicitor General Erwin Griswold explained: "It quickly becomes apparent to any person who has considerable experience with classified material that there is massive over-classification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another." Erwin N. Griswold, *Secrets Not Worth Keeping*, Wash. Post (Feb. 15, 1989), https://tinyurl.com/3xuhz6yt. Similarly, current Deputy Attorney General Lisa Monaco recently acknowledged, "over classification is a big problem." Cafe Insider, *United Security: Bounties, Bolton and COVID-19* (July 10, 2020), https://tinyurl.com/6nh73x9h.

As detailed in the ACLU's petition (Pet. 4), the FISC has released highly redacted opinions that show that the government continues to withhold information critical to understanding the legal bases for its decisions to authorize electronic surveillance. Those opinions have concerned significant surveillance programs, including the government's practice of accessing international communications between people in the United States and foreign targets, and the

government's access to international databases to target people in the United States. *See, e.g.*, [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011), https://perma.cc/L4YQK2MB; [Redacted], 402 F. Supp. 3d 45 (FISC 2018).

This is not to say that sources of government intelligence and methods of electronic surveillance should be revealed—that information is critical to the investigations the government conducts and is often properly classified. But judicial oversight of the reasons cited by the government for classifying the FISC's legal interpretations of surveillance laws is necessary to "afford[] proper respect to the individual rights at stake." *McGehee v. Casey*, 718 F.2d 1137, 1148 (D.C. Cir. 1983). Importantly, this judicial oversight would still recognize that the government has the "expertise and practical familiarity with the ramifications of sensitive information." *Id.*

Recognizing a qualified right of access will ensure that the government may not unduly restrict the public's understanding of the rules governing lawful surveillance. The resulting increased transparency about these rules will, in turn, foster trust in the U.S. legal and judicial systems. And it will enhance confidence in the U.S. cloud services and technology sector, ensuring individual and enterprise customers that they can have confidence in the safety and security of services that provide unmatched speed, opportunity, and protection.

CONCLUSION

For the foregoing reasons, and those set out by the ACLU in its petition, this Court should grant the petition for writ of certiorari.

Respectfully submitted,

Robert M. Loeb
Counsel of Record
Monica Haymond
ORRICK, HERRINGTON & SUTCLIFFE LLP
1152 15th Street N.W.
Washington, D.C. 20005
(202) 339-8400
rloeb@orrick.com

Date May 27, 2021