No. 17-2

In the Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

REPLY BRIEF FOR THE UNITED STATES

JEFFREY B. WALL
Acting Solicitor General
Counsel of Record
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Statutes:

Miscellaneous:

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 17-2

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

REPLY BRIEF FOR THE UNITED STATES

For decades, Microsoft and other providers of electronic communications services routinely complied with disclosure warrants issued under 18 U.S.C. 2703 without regard to where they stored the relevant communications. The panel upended that status quo by holding that Microsoft's business decision to place certain communications on a server in Ireland rendered a warrant seeking their disclosure impermissibly extraterritorial. That "unprecedented ruling" has "put the safety and security of Americans at risk" by severely limiting a critical law-enforcement tool. Pet. App. 125a & n.6 (Cabranes, J., dissenting). And every decision outside the Second Circuit to consider the issue has squarely rejected the panel's holding—a striking consensus that now includes eleven magistrate and district judges.

Microsoft does not deny that the question presented is critically important or that this case is an appropriate vehicle for resolving it. Microsoft nonetheless contends (Br. in Opp. 13-37) that this Court should deny review because, in Microsoft's view, the panel's decision was correct; because no circuit conflict yet exists; and because Congress may amend the Stored Communications Act (SCA), 18 U.S.C. 2701 *et seq.* To the contrary, the panel's decision is deeply flawed, and neither the absence of a circuit conflict nor the speculative possibility of eventual legislative action diminishes the acute and present need for this Court's review of a legally unsound decision that is frustrating important investigations around the country.

A. The Question Presented Is Exceptionally Important

This case presents a question of "exceptional importance to public safety and national security." Pet. App. 124a (Cabranes, J., dissenting). Section 2703 warrants are "an essential investigative tool used thousands of times a year." *Id.* at 125a (brackets and citation omitted). They are issued only if the government satisfies a standard "consistent with the highest level of protection ordinarily required by the Fourth Amendment": probable cause to believe that the relevant communications are evidence of a crime. *Id.* at 50a (Lynch, J., concurring). In holding that such evidence is categorically beyond the reach of a Section 2703 warrant whenever a provider chooses to place it abroad, the panel's decision "substantially burden[s] the government's legitimate law enforcement efforts" without serving "any serious, legitimate, or substantial privacy interest." *Id.* at 125a (Cabranes, J., dissenting).

Already, the panel's decision has frustrated "dozens of investigations" involving child exploitation, human

trafficking, and other serious federal crimes. *Statement of Brad Wiegmann, Deputy Assistant Att'y Gen., Before the Subcomm. on Crime and Terrorism of the Senate Comm. on the Judiciary* 6 (May 24, 2017) (Wiegmann Statement). Thirty-three States and Puerto Rico have likewise confirmed that the panel's decision "ha[s] had and will continue to have very real and detrimental impacts" on their ability "to protect the safety of their residents." Vermont Amicus Br. 3.

Although Microsoft acknowledges that the panel's decision severely restricts Section 2703 warrants, it asserts (Br. in Opp. 26) that "the Government does not deny that it can secure most of what it needs through [mutual legal assistance treaties (MLATs)] and other bilateral agreements." That is not so. In fact, as we explained (Pet. 30), the MLAT process is often "entirely futile." The United States does not have MLATs with most countries. Wiegmann Statement 6. Even where they exist, MLATs are of no help when, as is common, a provider stores the relevant communications in multiple countries, continuously shifts them from country to country, or is unable or unwilling to tell the government where they are stored. Pet. App. 127a-129a (Cabranes, J., dissenting). And even when the government seeks communications stored in a single, identifiable country with which the United States has an MLAT, the MLAT process can be too slow for "time-sensitive investigations and other emergencies." Wiegmann Statement 6. MLATs therefore cannot reliably substitute for Section 2703 warrants.

B. The Panel's Decision Is Wrong

The warrant in this case was based on a judicial finding of probable cause to believe that the relevant communications are evidence of a federal crime. It was

served in the United States on Microsoft, a U.S. provider. It requires Microsoft to disclose communications in the United States. And Microsoft's U.S.-based employees could make that disclosure without leaving their desks. Despite all that, Microsoft asserts (Br. in Opp. 25-34) that the warrant entails an impermissible extraterritorial application of Section 2703. That is incorrect.

1. Microsoft repeatedly invokes (Br. in Opp. i, 4, 13-16, 32-33, 37) the presumption against extraterritoriality. But it is undisputed that Section 2703 "lacks extraterritorial reach." Pet. App. 120a (Jacobs, J., dissenting). This case thus involves only the second step of this Court's "two-step framework for analyzing extraterritoriality issues," which asks "whether the case involves a domestic application of the statute." *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2101 (2016). That question turns not on the presumption against extraterritoriality, but on "the statute's 'focus.'" *Ibid.* "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *Ibid.*

2. Echoing the panel, Microsoft contends (Br. in Opp. 27-32) that the "focus" of Section 2703 is the privacy of stored communications and that the conduct relevant to that focus occurs exclusively where the communications are stored. Both steps of that argument are unsound.

First, the text and structure of Section 2703 make clear that it focuses on disclosures to the government. Section 2703 prescribes the circumstances under which "[a] governmental entity may require *the disclosure* by a provider" of communications. 18 U.S.C. 2703(a) (emphasis added). Those mandated disclosures are what "the statute seeks to 'regulate.'" *Morrison* v. *National*

Australia Bank Ltd., 561 U.S. 247, 267 (2010) (citation omitted). Those disclosures are thus "the conduct relevant to [Section 2703]'s focus." *RJR Nabisco*, 136 S. Ct. at 2101; see Pet. 14-17. And because the warrant at issue here requires Microsoft to disclose communications to the government in the United States, it is a permissible domestic application of the statute.[1]

Microsoft does not seriously dispute that Section 2703 concentrates on disclosure. Like the panel, however, it asserts (Br. in Opp. 27-28) that courts must be guided by the focus of the SCA as a whole rather than the focus of Section 2703 in particular. But different provisions of a statute may "regulate" different conduct or "protect" different interests—and thus have different focuses. *Morrison*, 561 U.S. at 267 (brackets and citations omitted). In *RJR Nabisco*, for example, this Court held that the private right of action in 18 U.S.C.

---

[1] That understanding is consistent with the settled rule governing subpoenas. Half a century ago, the Second Circuit observed that it was "no longer open to doubt" that a subpoena may "require the production of documents located in foreign countries" so long as "the court has *in personam* jurisdiction of the person in possession or control of the material." *United States* v. *First Nat'l City Bank*, 396 F.2d 897, 900-901 (1968). Microsoft asserts (Br. in Opp. 33-34) that the subpoena rule is distinguishable because Section 2703 uses the term "warrant" rather than "subpoena" and because it requires the production of user communications rather than a provider's "own corporate records." Neither distinction is relevant to the extraterritoriality analysis. The subpoena cases reflect the principle that a court order requiring a person to produce information in the United States is not extraterritorial even if the person must retrieve that information from abroad. So too here. Indeed, it would be bizarre if a probable-cause-based Section 2703 warrant afforded the government less ability to reach material stored abroad than an ordinary subpoena gives to any civil litigant.

1964 focuses on domestic injuries even though the underlying substantive provisions reach conduct occurring abroad. 136 S. Ct. at 2111. The "focus" inquiry thus requires a "provision by provision" analysis, Pet. App. 151a (Droney, J., dissenting)—not an attempt to infer the focus of the SCA as a whole from its colloquial name (Br. in Opp. 6, 27) or from provisions not at issue here (*id.* at 27-29).

Second, even if Microsoft were right that Section 2703's focus is "privacy," "the conduct relevant to [that] 'focus' * * * is a provider's *disclosure* or *nondisclosure* of emails to third parties." Pet. App. 132a (Cabranes, J., dissenting). Microsoft's contrary argument (Br. in Opp. 31-32) rests on the premise that the conduct relevant to privacy would occur exclusively in Ireland, where it would gather emails to be transmitted to the United States. But Microsoft "already ha[s] possession of, and lawful *access* to, the targeted emails." Pet. App. 136a (Cabranes, J., dissenting). Its ability to gather those emails and transfer them from a Microsoft server in Ireland to a Microsoft server in the United States does not implicate user privacy. Instead, "[o]nly Microsoft's *disclosure* of the emails to the government" implicates a privacy interest and would be "unlawful under the SCA absent a warrant." *Ibid.* That disclosure in the United States is thus the conduct relevant to Section 2703's asserted privacy focus.

3. Microsoft asserts (Br. in Opp. 29) that, "under the Government's construction," the privacy protections in 18 U.S.C. 2702 "would not bar a U.S. service provider from disclosing to a foreign tabloid a U.S. citizen's U.S.-stored communications" so long as the disclosure occurred abroad. But this case concerns only Section

2703, not Section 2702. Section 2703 authorizes the government to compel disclosures, and it is thus unsurprising that it focuses exclusively on disclosures in the United States (that is, to domestic authorities). Under this Court's provision-by-provision approach to extraterritoriality, however, other provisions of the SCA need not have the same focus.

In any event, Microsoft's interpretation suffers from the same problem it attributes to the government. As Microsoft acknowledges (Br. in Opp. 29), the necessary implication of its position is that *no* provision of the SCA applies to any "communications in electronic storage abroad." If that were right, a U.S. provider would be free to "disclos[e] to a foreign tabloid a U.S. citizen's U.S.-stored communications" (*ibid.*) so long as it first moved those communications outside the United States. Judge Raggi highlighted precisely that concern, emphasizing that Microsoft's interpretation could allow a provider "to flout not only [Section] 2703(a) warrants but also [Section] 2702(a) protections simply by moving materials abroad." Pet. App. 148a.

4. Microsoft also asserts (Br. in Opp. 15-17) that Section 2703 warrants requiring the disclosure of communications stored abroad could conflict with the laws of other countries. That concern appears to be largely hypothetical. Although Microsoft and other providers "routinely complied" with Section 2703 warrants seeking data "stored outside the United States" before the panel issued its decision, the Department of Justice "is not aware of any instance in which a provider has informed the Department or a court that production * * * would place the provider in conflict with local law." Wiegmann Statement 10-11. Here, too, Microsoft has

not asserted that production of the relevant communications would violate Irish law.[2]

Nor does the settled understanding that Section 2703 warrants can require the disclosure of information a provider has stored abroad place the United States at odds with the practices of other nations. "Countries including Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, the United Kingdom, and others already assert the authority to compel production of data stored abroad." Wiegmann Statement 12.

C. This Court's Review Is Warranted Now

Microsoft notes (Br. in Opp. 35-37) that the question presented is not yet the subject of a circuit conflict. But the exceptional importance of that question and the ongoing deleterious effects of the panel's decision warrant this Court's review even absent a circuit split. See Pet. 26-31. The need for this Court's review has only become clearer since the petition was filed. Microsoft continues to rely on the panel's decision nationwide, refusing to produce communications that previously would have been disclosed as a matter of course. At the same time,

---

[2] Microsoft repeats its claim (Br. in Opp. 17 & n.3) that the European Union's General Data Protection Regulation (GDPR) will prohibit compliance with Section 2703 warrants when it goes into effect in 2018. But the provision cited by Microsoft expressly specifies that it is "without prejudice to other grounds for transfer." Commission Regulation 2016/679, art. 48, 2016 O.J. (L 119) 64. Other GDPR provisions would allow providers to transfer communications to the United States to comply with a Section 2703 warrant. See, *e.g.*, *id.* art. 49(1)(d) and (e), 2016 O.J. (L 119) 64 (authorizing transfers that are "necessary for important reasons of public interest" or to establish legal claims).

eleven magistrate and district judges, sitting in five different circuits, have uniformly rejected the panel's holding in litigation involving Section 2703 warrants issued to Yahoo! and Google.[3]

In the wake of those decisions, Google has reversed its previous stance and informed the government that it will comply with new Section 2703 warrants outside the Second Circuit (while suggesting that it will appeal the adverse decisions in one or more existing cases). Consequently, the government's ability to use Section 2703 warrants to obtain communications stored abroad—which may contain evidence critical to criminal or national-security investigations—now varies depending on the jurisdiction and the identity of the provider.

Particularly given the unanimity of views in other courts and the compelling dissents from the denial of rehearing en banc, it is unlikely that all of the decisions rejecting the panel's holding will be reversed on appeal.

---

[3] See *In re Search Warrant to Google, Inc.*, No. 17-mj-532 (N.D. Ala. Sept. 1, 2017), slip op. 23; *In re Search Warrant No. 16-960-M-1 to Google*, No. 16-960, 2017 WL 3535037, at *11 (E.D. Pa. Aug. 17, 2017), aff'g 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), aff'g 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017), aff'g 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search of Information Associated with Accounts Identified as [redacted]@gmail.com*, No. 16-mj-2197, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017); *In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3.

No sound reason exists for this Court to tolerate the present disuniformity, uncertainty, and harm to public safety while it awaits the development of a circuit conflict. That is particularly true because the Court has the benefit of detailed opinions by six appellate judges, which thoroughly analyze the relevant issues—including all of the issues Microsoft identifies in arguing (Br. in Opp. 35-37) that more percolation is needed.

D. The Possibility Of Amendments To The SCA Provides No Sound Reason To Deny Review

Microsoft places greatest emphasis (Br. in Opp. 14-26) on its assertion that even if the question presented otherwise warrants this Court's review, the Court should deny the petition because proposals to amend the SCA have been introduced in Congress. But in light of the importance of the question presented and the uncertainty and ongoing harms caused by the panel's decision, the speculative possibility of congressional action is not a sound reason to deny review.

Microsoft confidently predicts (Br. in Opp. 26) that "Congress likely will resolve the issue" in a matter of months because there is widespread agreement that the SCA should be "update[d]." But consensus on the need for *some* update is not the same thing as consensus on *how* the statute should be revised—much less a guarantee of prompt congressional action.[4] Indeed, analogous bills failed to pass when they were introduced in the last

---

[4] For example, the government has recommended legislation reinstating the status quo, Wiegmann Statement 10, but Microsoft has supported a different approach, see Brad Smith, President & Chief Legal Officer, Microsoft, *ICPA: A Much-Needed Legislative Path to Modernize Outdated Digital Data Laws* (July 31, 2017), https://blogs.microsoft.com/on-the-issues/2017/07/31/icpa-much-needed-legislative-path-modernize-outdated-digital-data-laws.

Cognress. See H.R. 283, 114th Cong., 1st Sess. (2015); H.R. 5323, 114th Cong., 2d. Sess. (2016); S. 356, 114th Cong., 1st Sess. (2015); S. 512, 114th Cong., 1st Sess. (2015); S. 2986, 114th Cong., 2d Sess. (2016). The prospects and timing of a legislative remedy thus remain "entirely speculative." Pet. App. 137a n.37 (Cabranes, J., dissenting).

More fundamentally, Microsoft errs in asserting (Br. in Opp. 21) that this Court would "disrupt the ongoing legislative process" if it granted certiorari. "If Congress wishes to revisit the privacy and disclosure aspects of [Section] 2703, it is free to do so when it chooses to do so." Pet. App. 154a (Droney, J., dissenting). But unless and until Congress acts, it is the responsibility of the Judiciary—and, ultimately, of this Court—to determine the correct interpretation of existing law. The Court thus often grants certiorari to decide important questions of statutory interpretation despite a respondent's contention that pending legislative proposals would be "preferable vehicles" for addressing the relevant issues. Br. in Opp. at 41, *Highmark Inc.* v. *Allcare Health Mgmt. Sys., Inc.*, 134 S. Ct. 1744 (2014) (No. 12-1163); see, *e.g.*, Franklin Pls.' Br. in Opp. at 23, 31-32, *Puerto Rico* v. *Franklin Cal. Tax-Free Trust*, 136 S. Ct. 1938 (2016) (Nos. 15-233 and 14-255); Br. in Opp. at 33, *Microsoft Corp.* v. *i4i Ltd. P'ship*, 564 U.S. 91 (2011) (No. 10-290). And immediate review is particularly appropriate where, as here, "a decision of [one] court" has upset an established status quo and "created serious, on-going problems for those charged with enforcing the law and ensuring our national security." Pet. App. 137a n.37 (Cabranes, J., dissenting).

* * * * *

For the foregoing reasons and those stated in the petition for a writ of certiorari, the petition should be granted.

Respectfully submitted.

JEFFREY B. WALL
Acting Solicitor General

SEPTEMBER 2017