No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

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

REPLY BRIEF FOR THE UNITED STATES

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Cases—Continued: Page

Constitution, treaty, statutes, rules, and regulation:

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 17-2

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

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

REPLY BRIEF FOR THE UNITED STATES

Congress has provided that the government "may require the disclosure" of certain electronic information by obtaining "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. 2703(a); see 18 U.S.C. 2703(b)(1) and (c)(1)(A). Microsoft contends that the application of Section 2703 here is "extraterritorial" because Microsoft stores the requested information abroad.

This Court's extraterritoriality precedents do not sweep so broadly. The Court has rejected as extraterritorial actions involving foreign defendants, foreign plaintiffs, and foreign conduct. See *Kiobel* v. *Royal Dutch Petrol. Co.*, 569 U.S. 108 (2013); *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247 (2010). Here, by contrast, the U.S. government has required a U.S. service provider to disclose in the United States information that a neutral magistrate has found relates to a U.S. crime. Indeed, Microsoft's employees could prepare that disclosure without leaving their desks in the

United States. Yet under Microsoft's theory, that application of Section 2703 is impermissibly "extraterritorial" because Microsoft has unilaterally chosen to store the requested information in Ireland and would need to retrieve the information before disclosing it.

That incidental foreign activity would make a difference only if Section 2703 focused on the storage of electronic information. See *Morrison*, 561 U.S. at 266-267. But Section 2703 does not say anything about how or where information must be stored. Instead, it regulates the circumstances under which such information must be disclosed to the government. Microsoft's contrary position conflicts not just with the statute's text but with longstanding principles governing compulsory process. It also upends the status quo that Microsoft and other service providers followed for years before this litigation commenced, and that largely remains the status quo outside the Second Circuit.

A. Section 2703 Focuses On Domestic Conduct

Although Microsoft at times collapses them (Br. 2, 19, 44-45), this Court's extraterritoriality analysis comprises two distinct steps. See *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2101 (2016). The first step asks whether the presumption against extraterritoriality has been rebutted. *Ibid.* Because it is undisputed that Section 2703 lacks extraterritorial reach, Microsoft's discussion of that first step (Br. 14-18) is beside the point. This case concerns only the second step, which asks "whether the case involves a domestic application of the statute." *RJR Nabisco*, 136 S. Ct. at 2101. 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.* Here, because the conduct relevant to Section 2703's "focus"—disclosure to the government—occurs in the United States, this case involves a domestic application of the statute. That result is not "paradoxical," as Microsoft contends (Br. 19); it is a straightforward application of this Court's two-pronged analysis.

1. Section 2703 focuses on the disclosure of stored communications, not the storage of stored communications

Microsoft contends (Br. 20-32) that the colloquially named Stored Communications Act (SCA), 18 U.S.C. 2701-2712, focuses on protecting the privacy of stored communications at their place of storage. That contention rests on two key premises. First, Microsoft analyzes the focus of the entire SCA (Br. 20-25), rather than Section 2703 itself. Second, Microsoft assumes (Br. 25-29) that, because Section 2703 covers electronically *stored* communications, it must "seek[] to regulate" the *storage* of those communications, *Morrison*, 561 U.S. at 267 (citation and internal quotation marks omitted). Both premises are unsound.

a. Microsoft first attempts (Br. 20-25) to shift the analysis to the broader SCA. That approach conflicts with this Court's precedents, which dictate a provision-specific "focus" inquiry. See *RJR Nabisco*, 136 S. Ct. at 2102-2103, 2108-2111; *Morrison*, 561 U.S. at 265-267. Microsoft contends (Br. 25) that *RJR Nabisco* did not reach the second step of the extraterritoriality analysis. But it necessarily did: The Court held that the application of 18 U.S.C. 1964(c) was extraterritorial because the plaintiffs' claims involved "injury suffered abroad," *RJR Nabisco*, 136 S. Ct. at 2111—

indicating that the injury was the provision's focus. More generally, the Court cautioned that extraterritoriality principles "must be applied separately" to individual statutory provisions. *Id.* at 2108. As for *Morrison*, Microsoft acknowledges (Br. 25) that the Court assessed the focus of Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. 78j(b), though it looked to other provisions to bolster its conclusion that Section 10(b) focuses on domestic exchanges. See 561 U.S. at 266-268.

Insofar as Microsoft contends that Section 2703's focus should be determined in the context of related statutory provisions (Br. 22-24)—and not that related provisions must share a single focus—the government agrees. Sections 2701, 2702, and 2703 regulate different actors and different actions, which reinforces Section 2703's particular focus on providers' disclosure to the government. Section 2701 forbids "access[] without authorization," 18 U.S.C. 2701(a)(1), including hacking, but exempts conduct authorized by a provider, 18 U.S.C. 2701(c)(1). Sections 2702 and 2703, by contrast, focus on providers' intentional disclosures. Section 2702 bars a provider from "knowingly divulg[ing]" the contents of electronic communications, 18 U.S.C. 2702(a), subject to exceptions, see 18 U.S.C. 2702(b). Section 2703, meanwhile, outlines when a provider must disclose information to governmental entities. 18 U.S.C. 2703(a)-(c). Thus, while Sections 2701 and 2702 *forbid* the transfer of data from a provider to other entities, Section 2703 *requires* it. Section 2703 alone focuses on the mandatory disclosure of information from a provider (which lawfully controls it) to the government (which lawfully requests it).

b. Microsoft offers little text to support its theory that Section 2703 focuses on data storage. Although it stresses (Br. 22-25) that Section 2703 applies to "communications in electronic storage," that does not answer what acts Section 2703 "seeks to regulate" or what interests it "seeks to protect." *Morrison*, 561 U.S. at 267 (brackets, citation, and internal quotation marks omitted). Saying that Section 2703 regulates "stored communications" is just as incomplete as saying that Section 10(b) of the Securities Exchange Act regulates "securities." To assess whether Section 10(b) had been applied extraterritorially, *Morrison* determined that the "objects of the statute's solicitude" were the "*purchases and sales of* securities in the United States." *Id.* at 266-267 (emphasis added). A similar inquiry is necessary here: Does Section 2703 regulate the *storage* of stored communications or the *disclosure* of stored communications? Microsoft fails to identify any language in Section 2703 that regulates storage—such as where, with what security, or under what other conditions a provider must store communications. Conversely, Section 2703's title, substantive commands, and legislative history all make clear that it regulates disclosure to the government. See U.S. Br. 22-25. Such disclosures are thus "the conduct relevant to the statute's focus." *RJR Nabisco*, 136 S. Ct. at 2101.

In addition, Microsoft's storage theory (Br. 20-29) overlooks that Section 2703 is not limited to "communications in electronic storage." For example, it also covers "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." 18 U.S.C. 2703(c)(1). The focus of Section 2703 cannot be the storage of stored communications, when Section 2703 regulates

the acquisition of information other than stored communications. By contrast, for all the varied types of electronic information, the statute sets forth the applicable disclosure requirements. See 18 U.S.C. 2703(a)-(c).

Faced with Section 2703's repeated references to disclosure, Microsoft points to (Br. 26-29) other textual features that purportedly foreclose a disclosure focus. Most are unrelated to the focus inquiry. For example, that Section 2703 does not extend to foreign governments (Br. 27) and that a separate statute covers foreign requests for assistance (Br. 18, 27) show only that Section 2703 regulates domestic investigations. Similarly, the statute's application to state and local governments (Br. 26-27) coheres with its focus on domestic disclosure, and Microsoft's pragmatic objections are unsupported. See p. 8, *infra*. And Section 2703's omission of disclosure requirements for entities not covered by the statute (Br. 28) demonstrates nothing about its focus.

Microsoft also points to (Br. 27-28) Section 2703(g), under which an officer's presence is not required (though is not forbidden) "for service or execution" of a warrant. But that provision describes the warrant as one "requiring *disclosure* by the provider." 18 U.S.C. 2703(g) (emphasis added). That accords with Section 2703's description of a provider's disclosure duties. See 18 U.S.C. 2703(a)-(c). Consistent with that reading, the warrant in this case indicated that law enforcement officers would review information that Microsoft disclosed. See J.A. 24-25. Finally, Microsoft identifies (Br. 29) amendments to the SCA that allow for the nationwide service of warrants. If anything, however, the creation of broader jurisdictional rules for electronic data than for physical evidence, see 18 U.S.C. 2711(3)(A),

suggests that Congress focused less on the location of electronic data.

c. Left without a textual foothold, Microsoft relies on policy. It contends (Br. 29-32) that Congress could not have sought to regulate disclosure in Section 2703 because various undesirable results would ensue if U.S.-stored information could be disclosed abroad. As an initial matter, all of Microsoft's purported statutory gaps stem from the application of Sections 2701 and 2702, not Section 2703. This case concerns only Section 2703, and other provisions of the SCA need not share the same focus. See pp. 3-4, *supra*. Microsoft's policy concerns thus reflect its basic failure to adopt a provision-specific "focus" approach.

In any event, Microsoft's theory leads to the same results it attributes to the government's. If, as Microsoft believes, the SCA focuses on storage, it does not protect communications once moved outside the United States. Thus, "a U.S. service provider (or rogue employee)" would be free to provide "a U.S. citizen's U.S.-stored emails to a tabloid" outside the United States (Br. 30), so long as it first transfers those communications to its offices abroad. Or, if a U.S. provider builds its servers just beyond the U.S. border, then U.S. citizens' communications will escape all protection. Microsoft conceded as much in the court of appeals. See J.A. 138 ("There will be a gap regardless of what you identify as the focus of Congressional concern."); see also Resp. Br. 32 ("*[E]ither* interpretation will inevitably yield some gap in coverage in the digital era."). To the extent Microsoft now attributes its gaps in protection to changes in the global internet (Br. 30-31), the same observation applies to any gaps under the government's theory.

For similar reasons, the three hypotheticals that Microsoft offers (Br. 31-32) are either incorrect or overwrought:

(1) The provider that discloses a U.S. citizen's emails in China: This hypothetical assumes that Section 2702—not at issue here—focuses on disclosure. Assuming that it does, if a provider transfers data to servers in China, both the storage and the subsequent disclosure of the data would occur there and Section 2702 would not apply under either theory.

(2) The London hacker who accesses a U.S. server: This hypothetical assumes that Section 2701—also not at issue here—focuses on disclosure. Section 2701, however, regulates "access," which encompasses the U.S. destination of the attack. Cf. *United States* v. *Auernheimer*, 748 F.3d 525, 533-534 (3d Cir. 2014) (in analyzing venue of unauthorized access in violation of 18 U.S.C. 1030(a)(2)(C), concluding that access occurred at location of protected computer).

(3) The local sheriff who seeks Chinese officials' correspondence: Although Section 2703 theoretically authorizes the disclosure (assuming that a provider in the United States controls the relevant files), this hypothetical is implausible. State or local entities may obtain a Section 2703 warrant only upon a showing of probable cause that the requested records implicate a crime within their jurisdiction. As a result, such warrants typically involve state residents who commit state offenses. See States Amicus Br. 9-10, 15-16, 22-23. And if a case with international ramifications were to arise, the federal government could intercede and pursue a cooperative diplomatic resolution.

d. Ultimately, Microsoft contends (Br. 37) that treating disclosure as the focus of Section 2703 prioritizes "mechanical" domestic activities over more "significant" activities abroad. That is incorrect. Because Section 2703 governs disclosures from U.S. providers to U.S. governmental entities about U.S. crimes, those domestic disclosures are the heart of the statute and logically determine its reach. To use an analogy more apt than air travel (*ibid.*), consider a court-ordered fine: If a U.S. court has jurisdiction over a U.S. company and orders it to pay a fine pursuant to a federal statute, it does not matter that the company may need to transfer money or sell assets from around the world to pay that fine. The payment occurs here, and a company's internal preparation for payment does not transform the court order into an extraterritorial application of the statute. The same is true of disclosure orders under Section 2703.

2. Even if Section 2703 focuses on the privacy of stored communications, any privacy invasion occurs here

Even if Microsoft were correct (Br. 20-21) that the relevant statutory focus is protecting the privacy of stored communications, the Court still must determine where any invasion of privacy occurs. As Judge Cabranes explained in his dissent from the denial of rehearing en banc, "it is only when a provider *divulges* the content of a user's communications to a third party that the provider puts a user's privacy at risk." Pet. App. 135a. Under a Section 2703 warrant, that action occurs domestically. Microsoft's sole argument to the contrary appears to be (Br. 32-37) that a law-enforcement search or seizure, with a corresponding privacy invasion, oc-

curs where the data is stored. That argument misconstrues Section 2703, the nature of a search, and this Court's precedents.

a. Under a Section 2703 warrant, two critical acts occur in the United States: A provider discloses information to the government, and the government reviews that information. See, *e.g.*, J.A. 24-26. In Microsoft's view (Br. 32-33), Section 2703(g) instructs that the "execution of a search warrant" extends more broadly and encompasses a provider's collection of data for disclosure. But Section 2703(g) clarifies only that an officer need not be present for a provider's "execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider." In other words, it permits a provider to handle the disclosure component of a Section 2703 warrant; it does not declare that all of a provider's preparatory actions for the required disclosure constitute substantive searches.

In this case, at most one preparatory action occurs outside the United States: Microsoft repatriates an account that it had previously "migrated" to Ireland. J.A. 31. It does so by running a "database management program" from its U.S. offices, which allows U.S.-based employees to "collect the requested information from the server" in Ireland. J.A. 34; see Pet. App. 8a. But that process does not invade a user's privacy for several reasons. First, Microsoft chose to move the user's account to Ireland initially, and Microsoft is equally free to return it. See J.A. 30-31. Second, Microsoft's transfer of data does not expose the contents of any communications. See J.A. 24-25. And third, the SCA specifically contemplates that a provider may permissibly access and transfer users' data. See 18 U.S.C. 2701(c)(1); 18 U.S.C. 2702(b)(4)-(5) and (c).

b. Microsoft nevertheless contends (Br. 33-34) that the transfer is significant because Microsoft purportedly retrieves the data as a government agent. Its premise is mistaken. This Court has held that, when the government compels a private party to perform a search or seizure of a third party, the search or seizure may be attributed to the government. See *Skinner* v. *Railway Labor Execs. Ass'n*, 489 U.S. 602, 614-615 (1989). But Section 2703 does not require that Microsoft intrude on someone else's privacy by performing a search or seizure.

The Section 2703 warrant requires that Microsoft disclose certain information already within its "possession, custody, or control." J.A. 24. It does not demand that Microsoft seize goods in someone else's possession, as occurred in *Gambino* v. *United States*, 275 U.S. 310, 314-317 (1927) (state officers made seizures from private persons "on behalf of the United States"). Nor does it demand that Microsoft acquire information about someone—such as by entering a person's hotel room and photographing his private papers (Br. 33-34). The Section 2703 warrant simply requires Microsoft to gather information in its control, wherever stored, and disclose it to the government. That is what any subpoena or summons requires, and Microsoft cites no decision holding that a person performs a "search" or "seizure" as a government agent when responding to a subpoena or summons. See Pet. App. 144a-145a (Raggi, J., dissenting from denial of rehearing en banc). To the contrary, compliance with such compulsory process has long been treated as a basic duty of citizenship. See *United States* v. *Dionisio*, 410 U.S. 1, 9-10 (1973); *Kastigar* v. *United States*, 406 U.S. 441, 443 (1972).

c. Microsoft's response is twofold. It first contends (Br. 35) that it must search private customer communications, not just its own business records. Critically, though, the government did not compel Microsoft to review customers' communications to identify particular content. Microsoft would arguably act as the government's agent in performing a search if the Section 2703 warrant commanded it to review the contents of emails and alert the government to suspicious activity. The Section 2703 warrant, however, authorizes only the government to examine the contents of emails after Microsoft discloses the entire account. See J.A. 24-25. By way of analogy, the Section 2703 warrant does not ask Microsoft to open and rummage through a safe-deposit box (Br. 33) or to open and read a paper letter (Br. 35). Rather, it requires Microsoft to hand over the stack of sealed letters or the locked safe-deposit box in its possession and control. The government then reviews the contents (pursuant to a warrant)—in the United States.

Microsoft next contends (Br. 35-36) that its asserted "copying" of data in Ireland constitutes an extraterritorial seizure. That theory has at least three flaws. First, a Section 2703 warrant, like a subpoena, simply requires disclosure. The government exercises no control over how Microsoft prepares for disclosure, including whether it repatriates a user's account or whether it leaves data on an Irish server and makes a copy. Second, few courts, including in the decisions that Microsoft cites (Br. 35), have assessed whether the government seizes data when it makes a copy. The copying of electronic data, unlike the seizure of a physical letter, does not "meaningful[ly] interfere[] with an individual's possessory interests." *United States* v. *Jacobsen*, 466 U.S. 109, 113 (1984); see *Arizona* v. *Hicks*, 480 U.S. 321, 324

(1987). That may explain why, contrary to Microsoft's characterization (Br. 35), Federal Rule of Criminal Procedure 41 refers to "the seizure or copying of electronically stored information" in the disjunctive. Fed. R. Crim. P. 41(e)(2)(B). Third, assuming that copying data constitutes a seizure to the extent the copy impairs a user's "right to exclude," Resp. Br. 36 (quoting *Rakas* v. *Illinois*, 439 U.S. 128, 143 n.12 (1978)), Microsoft's copying does not impair that right. A user has no right to exclude *Microsoft* from copying or relocating her communications, which Microsoft does as a matter of course. See J.A. 31 (explaining that Microsoft creates "several copies of the email content and non-content information," does so "on a continuous basis," and stores the copies in various locations). A user's right to exclude is therefore implicated only when the *government* receives a copy of her communications—in the United States.

B. Section 2703 Reflects The Common-Law Principle That Subpoena Recipients Must Produce Documents Within Their Control

Section 2703's focus on disclosure aligns with background common-law rules about compulsory process. At the time Congress enacted the SCA, it was "no longer open to doubt that a federal court ha[d] the power to require the production of documents located in foreign countries" if a party had "possession or control of the material." *United States* v. *First Nat'l City Bank*, 396 F.2d 897, 900-901 (2d Cir. 1968). Microsoft nevertheless contends (Br. 45-51) that Congress intended to depart from that background rule, that the rule does not cover "custodians," and that this Court has never endorsed it. All three contentions lack merit.

1. Microsoft suggests that Section 2703 is incompatible with the common-law rule in favor of production. To start, it observes (Br. 45) that warrants are distinct from subpoenas. As previously explained, however, see U.S. Br. 34-39, both Section 2703 warrants and subpoenas impose identical disclosure requirements on providers, see 18 U.S.C. 2703(a), (b)(1), and (c)(1). Microsoft responds (Br. 45-46) that Section 2703 warrants alone cover the contents of a user's communications, but that is incorrect. The government may require the disclosure of communications in a remote computing service, or in electronic storage in an electronic communication service for more than 180 days, through either a warrant or a subpoena (with notice to the user). See 18 U.S.C. 2703(a) and (b)(1).[1] Regardless, the fact that a *user* might have privacy interests that require a warrant (or notice) to search the contents of communications has no bearing on a *provider's* disclosure obligations.

Next, Microsoft asserts (Br. 46) that Section 2703(a) "formulates the service provider's obligation with words that bear no resemblance to the compelled-production rules the Government invokes." Yet Section 2703(a) could not be clearer: "A governmental entity may

---

[1] Microsoft asserts (Br. 49) that "email content can *never* be obtained by subpoena," citing one lower-court decision holding that the Fourth Amendment requires a warrant for certain searches of the contents of emails, at least when conducted without notice to the account holder. See *United States* v. *Warshak*, 631 F.3d 266 (6th Cir. 2010). But *Warshak*'s Fourth Amendment analysis is beside the point. Section 2703 creates multiple mechanisms for the government to obtain electronic communications. Microsoft offers no reason why Congress would have authorized the government to obtain foreign-stored communications with a subpoena, yet precluded it from doing so with a warrant.

require the disclosure by a provider" of certain electronic materials. 18 U.S.C. 2703(a); see J.A. 24 (requiring that Microsoft "disclose the following information" "within [its] possession, custody, or control"). That language bears an obvious resemblance to the rule that "[a] subpoena may order the witness to produce" materials. Fed. R. Crim. P. 17(c)(1); see Fed. R. Civ. P. 45(a)(1)(A)(iii).

Finally, Microsoft notes (Br. 47) that Section 2703(g) mentions the "execution of a search warrant." As discussed, however, the full provision refers to a provider's disclosure duties while relieving the government of the need to be present during that process. See pp. 6, 10, *supra*. Microsoft also asserts (Br. 48) that a Section 2703 warrant functions as a traditional search warrant "from the *account owner's* perspective." But again, this case involves a provider's disclosure duties, not an account owner's claims. And from a provider's perspective, Microsoft assumes (*ibid.*) that those disclosure duties justify a pre-enforcement motion to quash—a right available to a subpoena recipient but not to the target of a warrant. Pet. App. 3a; see Fed. R. Crim. P. 17(c)(2).

2. Microsoft next attacks the background rule itself, contending (Br. 49-50) that it does not apply to "private papers that a custodian holds in trust for a customer in another country." Like the court of appeals, Pet. App. 34a, Microsoft cites no support for that proposition. Lower courts have concluded that (1) a subpoena requiring a U.S. company to produce records is enforceable regardless of whether the company must retrieve those records from outside the country; and (2) the same disclosure rules apply to a business's own records and the records it stores for clients. See U.S. Br. 33-34,

40-41. It follows from those two premises that a business that stores clients' records abroad is not exempt from compulsory process. Indeed, a carve-out for that scenario would be inconsistent with the underlying principle that an order requiring a person to produce information in the United States is not extraterritorial, so long as the information is within the person's control. See *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir.) ("The test for the production of documents is control, not location."), cert. denied, 463 U.S. 1215 (1983); see also *Hay Grp., Inc.* v. *E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) ("'Production' refers to the delivery of documents, not their retrieval.").

Microsoft also briefly challenges (Br. 50 n.5) the second premise above. Although few "custodian" or "caretaker" cases have arisen, courts have applied ordinary subpoena principles to requests for a client's filing cabinets, mail, or other papers. See *In re Grand Jury Subpoena Served Upon Horowitz*, 482 F.2d 72 (2d Cir.), cert. denied, 414 U.S. 867 (1973); *United States* v. *Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985); *United States* v. *Re*, 313 F. Supp. 442 (S.D.N.Y. 1970); see also *Burdeau* v. *McDowell*, 256 U.S. 465, 476 (1921) (explaining that, if private papers fell into another person's possession, "we know of no reason why a subpoena might not issue for the production of the papers as evidence," as "[s]uch production would require no unreasonable search or seizure"). In fact, *Barr* illustrates Microsoft's preferred physical analogy. There, a subpoena required a mail-receiving service to turn over a client's letters, and the government later obtained a warrant to open and examine those letters. See 605 F. Supp. at 116, 119. Under Section 2703, the government merely combines

those steps by obtaining the warrant as part of the disclosure order: The provider first discloses communications to the government, just as it would under a subpoena, see J.A. 24, and the government then examines the contents of those communications, just as it would under a traditional search warrant, see J.A. 25.

3. Finally, Microsoft suggests (Br. 50-51) that the principles governing compulsory process do not apply because "this Court has never endorsed the *Marc Rich* doctrine." But Congress legislates against the backdrop of "the common law," *Kirtsaeng* v. *John Wiley & Sons, Inc.*, 568 U.S. 519, 538 (2013) (citation omitted), and "the common law" does not require a specific endorsement from this Court. In any event, the Court has acknowledged the broader principle—which *Marc Rich* applies—that court orders do not operate extraterritorially when they require a person over whom the court has jurisdiction to produce domestically information abroad within that person's control. See *Société Nationale Industrielle Aérospatiale* v. *United States Dist. Court*, 482 U.S. 522, 539-540 (1987) (acknowledging in discovery context that trial court had jurisdiction "to order a foreign national party before it to produce evidence physically located within a [foreign] nation").

C. Practical Consequences Favor Reversal

Although Microsoft criticizes (Br. 51-52) the government for explaining the detrimental consequences that would stem from the decision below, it repeatedly emphasizes (Br. 29-32, 37-44, 51) its own policy arguments. To the extent the Court considers such arguments, they favor reversal.

1. Microsoft's data-location theory would arbitrarily hamper domestic law enforcement and counterterrorism efforts. Microsoft does not dispute, for example,

that a provider's decision where to store data need not bear any relationship to a user's ties to the United States. See U.S. Br. 42-43. Under its position, Microsoft could move all U.S. citizens' data beyond the SCA's reach if it chose to migrate that data to foreign servers. Although Microsoft asserts (Br. 55) that it stores information domestically "for most crimes the Government investigates," it offers no support for that assertion. And, of course, it could change its storage policies at any moment, as it has already done during this litigation (Br. 57).

Nor does Microsoft dispute that its construction of Section 2703 would be unworkable for other storage practices, such as Google's. See U.S. Br. 43-45. Microsoft observes (Br. 59-60) that electronically stored information has a physical location at any given moment (which the government has never contested). But that does not diminish the fact that Microsoft's data-location theory would make data inaccessible where a provider divides a single account into multiple pieces and frequently moves those pieces around the world. If cloud-computing technology moves in that direction, Section 2703 would become wholly ineffective.[2]

---

[2] Microsoft incorrectly asserts (Br. 60) that courts have rejected Google's claims—which parallel Microsoft's—because Google failed to plead threshold facts about the location of its data. Instead, those courts have concluded that the conduct relevant to the SCA's focus occurs in the United States. See, *e.g.*, *In re Search Warrant to Google, Inc.*, No. 17-cv-05847 (D.N.J. Jan. 8, 2018); *In re Search Warrant No. 16-960-M-1 to Google*, No. 16-960, 2017 WL 3535037 (E.D. Pa. Aug. 17, 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 (D.D.C. July 31,

2. Microsoft's contrary policy arguments depend on a purported international "outcry" (Br. 2). Its speculation remains unsupported, and the Executive Branch remains well positioned to evaluate and mitigate any international concerns on a case-by-case basis. See *Pasquantino* v. *United States*, 544 U.S. 349, 369 (2005) ("In our system of government, the Executive is the sole organ of the federal government in the field of international relations.") (citation and internal quotation marks omitted).

a. Microsoft decries (Br. 1) the "global free-for-all" that will supposedly ensue if this Court were to return to the prevailing view of Section 2703 before the decision below. It warns (Br. 58) that "[i]f we can do it to [other countries], they can do it to us." But the United States cannot stop other countries from asserting the domestic authority to obtain foreign-stored data from providers within their borders, although it may criticize abuses. Indeed, many other countries already assert that authority. See Statement of Brad Wiegmann, Deputy Assistant Att'y Gen., DOJ, Before the Subcomm. on Crime & Terrorism, U.S. Senate Comm. on the Judiciary, Hearing Entitled: *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights* 12 (May 24, 2017), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf (Wiegmann Statement); U.S. Br. 46-47. The United Kingdom, for example, may compel providers "to provide certain electronic communications sought by a U.K. warrant, even if the data are stored or controlled abroad." U.K. Amicus Br. 5.

2017); *In re Search of Information Associated with Accounts Identified as [Redacted]@gmail.com*, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017).

Ireland—the location of the data sought here—similarly reports that its courts have the "power to order production of documents by an Irish registered company by one of its branches situated in a foreign country," under certain circumstances. Ir. Amicus Br. 7. And Microsoft's sole example (Br. 58 n.8) of the supposed real-world consequences of applying Section 2703 involves Brazilian authorities' demand for foreign-stored data under Brazilian law.

Microsoft also asserts (Br. 38) that "[f]oreign sovereigns" have protested the application of Section 2703 to foreign-stored data. But Microsoft has declined to argue that its production of data would violate any foreign law. See *ibid.*; J.A. 140, 149. Although it identifies (Br. 38-39) complaints from individual foreign politicians and select foreign publications, no foreign government, including Ireland, has told this Court that Microsoft's production would violate that nation's laws. See Ir. Amicus Br. 3. And because the application of Section 2703 does not violate any individual nation's laws, it also does not violate customary international law, contrary to Microsoft's passing suggestion. See Resp. Br. 40 (citing *Murray* v. *Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804)).

Microsoft emphasizes (Br. 41-42) that the European Union's (EU) General Data Protection Regulation (GDPR), which takes effect in May 2018, could affect future transfers of EU-stored data. Article 48 of the GDPR requires use of the treaty process for data transfers to non-EU nations, "without prejudice to other grounds for transfer pursuant to this Chapter." Commission Regulation 2016/679, art. 48, 2016 O.J. (L 119) 64 (GDPR). That same chapter authorizes transfers pursuant to an "adequacy decision," or a finding that

the non-EU nation sufficiently protects personal data. *Id.* art. 45 (emphasis omitted); European Comm'n Amicus Br. 12. The United States currently operates under an adequacy decision with respect to certain transfers of certain providers, including Microsoft, and may do so under the GDPR. See Commission Implementing Decision (EU) 2016/1250, art. 1(1), (3), 2016 O.J. (L 207) 35; see also GDPR art. 45(9). Or the United States could enter a different agreement with the EU to cover future transfers. See GDPR art. 46(2)(a). Even absent such blanket solutions, Article 49(1)(d) authorizes transfers "necessary for important reasons of public interest," GDPR art. 49(1)(d), including the need to combat serious cross-border crimes "such as illicit drug trafficking," European Comm'n Amicus Br. 15—the crime at issue here, see J.A. 25. Alternatively, Article 49(1) endorses a case-specific balancing test that accounts for the provider's legal obligations in the non-EU country. See European Comm'n Amicus Br. 15.

b. Despite emphasizing hypothetical future conflicts, Microsoft all but ignores the United States' existing international obligations. The Budapest Convention requires that parties possess the power to order a person located in the country to submit data "in that person's possession or control." Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003), 2296 U.N.T.S. 167, art. 18.1(a) (Budapest Convention). Microsoft incorporates by reference (Br. 43) an amicus brief's argument that the Budapest Convention does not apply here, but that argument is mistaken.

The amicus brief contends that production orders for foreign-stored data under Article 18.1(a) of the Budapest Convention would conflict with Article 32. See Int'l

& Extraterritorial Law Scholars Amicus Br. 13. But Article 32 discusses trans-border access of data by "A Party," meaning direct access by one of the member countries. Budapest Convention art. 32. Article 18, by contrast, covers circumstances like these, in which member countries compel production from a non-governmental entity. *Id.* art. 18.1; see U.S. Br. 48. The amicus brief also misapprehends Article 18 itself. See Int'l & Extraterritorial Law Scholars Amicus Br. 15-16. Article 18.1(b) governs requests for certain subscriber information from a "service provider" "offering its services in the territory of the Party." Budapest Convention art. 18.1(b). Article 18.1(a) separately governs requests for all data in the possession of a "person"—including a service provider—"in [a party's] territory." *Id.* art. 18.1(a); see U.S. Br. 48-49. The latter provision applies here.

c. Experience also rebuts Microsoft's fears. Until this litigation commenced, Microsoft and other providers "routinely complied" with Section 2703 warrants seeking foreign-stored data, yet the Department of Justice "is not aware of any instance in which a provider has informed the Department or a court that production pursuant to the SCA of data stored outside the United States would place the provider in conflict with [foreign] law." Wiegmann Statement 10-11; see States Amicus Br. 22. Since the decision below, Section 2703 has continued to apply in full force in many courts outside the Second Circuit, see U.S. Br. 21 n.2, yet Microsoft still fails to offer a single example of a concrete conflict.

If, in an individual case, a provider could demonstrate that compliance with a Section 2703 warrant would violate another country's laws, diplomatic and judicial solutions would remain available. As Microsoft

acknowledges (Br. 40-41), the federal government scrutinizes disclosure requests that might adversely affect foreign relations, and it could pursue alternate channels. See Wiegmann Statement 11. Otherwise, courts could consider whether a specific production would violate foreign law, at least as part of their equitable power to craft appropriate contempt sanctions. See *Societe Internationale pour Participations Industrielles et Commerciales, S. A.* v. *Rogers*, 357 U.S. 197, 211-212 (1958). Although Microsoft attempts to cast doubt on that practice (Br. 53 n.7), it cites only an inapposite decision excluding foreign injuries from a specific statute's substantive reach. See *F. Hoffman-La Roche Ltd.* v. *Empagran S.A.*, 542 U.S. 155, 165-168 (2004).

In the end, Microsoft asks the United States to unilaterally forgo a power that countries around the world exercise, in order to avoid future hypothetical conflicts. The sounder course is to apply the statute as written and address such conflicts on a case-by-case basis, if they arise—which, as of this litigation, they have not.

* * * * *

The judgment of the court of appeals should be reversed.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General

FEBRUARY 2018