14-2985-cv

IN THE

United States Court of Appeals

FOR THE SECOND CIRCUIT

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation,

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

REPLY BRIEF FOR APPELLANT

Bradford L. Smith
David M. Howard
John Frank
Jonathan Palmer
Nathaniel Jones
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052

Guy Petrillo
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017

E. Joshua Rosenkranz
Robert M. Loeb
Brian P. Goldman
Susannah Landes Weaver
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001

Attorneys for Appellant

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FEDERAL STATUTES

FEDERAL RULES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION[1]

The Government's brief confirms this much: Nowhere did Congress say that ECPA should reach private emails stored on providers' computers in foreign countries. Small surprise for a statute written in 1986, before the creation of the global internet, when the notion of storing emails halfway across the globe was barely imaginable.

Congress can and should grapple with the question whether, and when, law enforcement should be able to compel providers like Microsoft to help it seize customer emails stored in foreign countries. Microsoft has outlined many reasons why Congress would be wary of granting that power: It would establish a norm that would allow foreign governments to reach into computers in the United States to seize U.S. citizens' private correspondence, so long as those governments may assert personal jurisdiction over whatever company operates those computers. It would offend foreign sovereigns. And it would jeopardize American economic interests.

The Government counters with some fair observations about law-enforcement concerns that Congress might prioritize instead. Today's Congress

[1] All statutory references are to Title 18 of the U.S. Code, and all emphasis in quotations is added, unless otherwise indicated. Microsoft's Opening Brief and the Government's Response Brief are cited as "OB" and "GB," respectively. Amicus briefs are cited as "___ Br.," according to the name of the lead amicus.

might balance those competing interests by seeking to expand ECPA's warrant power to apply only to U.S. citizens' communications stored abroad. Congress might also grant the extraordinary power the Government claims here to only the federal government, but not to all state and local officials. Or Congress might not expand § 2703 at all. Meanwhile, settled doctrine makes this Court's job simple: Because laws apply only domestically unless Congress clearly provides otherwise, the statute is properly read to apply only to electronic communications stored here, just as other countries' laws regulate electronic communications stored there. *See* § I.

The Government's arguments disregard "the wisdom of the presumption against extraterritoriality," and instead invite "judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 261 (2010). To disguise this end-run around Congress, the Government attempts to shoehorn this case into the *Marc Rich* doctrine, which allows subpoenas to reach business records in a company's custody or control regardless of their location. But the Government does not dispute that *Marc Rich* has *never* been applied to reach private correspondence stored with a custodian in a foreign country, let alone to permit execution of search warrants in a foreign country. Because *Marc Rich* does not speak to the context here, the Government has to recast "warrants" as

"subpoenas," customers' private "contents of electronic communications" as corporate "records," and the "execution of a search warrant" as "compelled disclosure" and "the act of gathering records." For an argument that purports to rest on the "explicit text of the statute," GB 9, the Government rewrites an awful lot of it. *See* § II.

In the end, none of the cases the Government cites addresses the novel scenario presented here. Just as the search-incident-to-arrest doctrine in *Riley* could not be expanded from the contents of cigarette packs to the contents of smartphones, neither can *Marc Rich* be extended from business records to the "qualitative[ly]" and "quantitative[ly]" distinct cache of intimate letters, personal photo albums, and home movies that people around the world now entrust to third-party providers for secure electronic storage. *Riley v. California*, 134 S. Ct. 2473, 2488-89 (2014). Congress never intended to reach, nor even anticipated, private communications stored in a foreign country when it enacted § 2703. This Court should let Congress decide how best to bring ECPA into the 21st century. *See* § III.

ARGUMENT

I. THE GOVERNMENT SEEKS AN IMPERMISSIBLE EXTRATERRITORIAL APPLICATION OF ECPA.

The presumption against extraterritoriality requires a two-step analysis to determine whether a party seeks an impermissible extraterritorial application of a

statute. First, did Congress clearly express its intent for the statute to apply abroad? *See Morrison*, 561 U.S. at 255-65. Here, the answer to that inquiry is easy: The Government does not dispute that Congress never clearly said that ECPA applies extraterritorially. *See* GB 27.

The case thus turns on *Morrison*'s second step: Is the party invoking the statute in fact seeking to apply it abroad? 561 U.S. at 266-73. This is often the more difficult question, because before a court can assess *where* the statute would be applied, it must first determine *what* the relevant conduct is. *Morrison* guides that determination: If the "focus" of the legislation—what it seeks to regulate and protect—occurs abroad in a particular case, then applying the statute in that case would be impermissibly extraterritorial.

The Government's entire argument assumes that the statute's focus is on "compelled disclosure." Only from that premise can the Government even contend that *Marc Rich*'s control-not-location principle applies. As explained in detail below (*see* § II), the Government's reliance on *Marc Rich* is misplaced: It flouts the language of the statute and would effect an unprecedented expansion of that doctrine.

But the Government is wrong at a more basic level. ECPA's "focus" is not "compelled disclosure" at all, but rather the protection and regulation of private "communications … in electronic storage." Thus, the location of the stored

communications determines where the statute is applied. *See* § I.A. The international tension sparked by the Warrant here only confirms that conclusion. *See* § I.B.

A simple example illustrates the point. Under both our view and the Government's, FBI agents cannot fax a warrant to the Moscow headquarters of mail.ru—one of the most popular email services in the world—ordering it to deliver a customer's emails stored in Russia to the U.S. embassy in Moscow. In that case, all three steps involved in applying § 2703 would take place abroad: (1) the "service" of a court-issued "warrant," (2) the "execution of [the] search warrant" for the "contents of … electronic communication … in electronic storage in [mail.ru's] electronic communications system," and (3) the ultimate "disclosure" to the Government. § 2703(a), (g).

The Government's position, however, is that it could accomplish *the same thing* by faxing a warrant to mail.ru's branch office in Mountain View, California, directing the company to download the customer's emails from the same computer in Russia and to deliver them to the FBI in San Francisco. In the Government's view, that scenario would involve no extraterritorial application of ECPA at all, because the Government serves the warrant, and mail.ru "discloses" the emails, in the United States, where a court has "personal jurisdiction over" the company. GB 32.

This case thus comes down to whether the foreign location of the middle step—what the statute calls the "execution of a search warrant" to retrieve communications from "electronic storage," § 2703(a), (g)—is irrelevant to the extraterritoriality analysis, simply because the steps that bookend it take place here. Clearly not. No one describes air travel as ground transportation just because it involves taxiing to and from the runway. Likewise, the "import[ation]" of emails from Ireland is not a domestic act just because the warrant is served and the emails are ultimately "disclose[d]" in the United States. *See* GB 4-6.

A. The Government Applies § 2703 Where Emails Are Stored, Not Where Disclosure Is Compelled.

1. The Government does not dispute that when FBI agents copy emails off a foreign computer themselves, they are executing an extraterritorial seizure. OB 31-33. And the Government admits (at 4) that the action it would force Microsoft to take on the Government's behalf is the same: "*collect*[*ing*]" customers' private email communications "from the datacenter[] where they are stored" abroad "and *import*[*ing*] them into the United States." Yet the Government asks this Court to ignore the extraterritorial nature of that action, because Microsoft's "disclosure" of the target email messages would occur domestically, where the Government has "jurisdiction" over the company. GB 4, 31-32.

The Government is simply wrong to assume that because it "compel[s] disclosure" domestically it is not applying § 2703 extraterritorially. As *Morrison*

observed, "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Morrison*, 561 U.S. at 266. And "the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved." *Id*. Accordingly, when a given application of a statute involves a mix of domestic and foreign activity, *Morrison* directs courts to consider the "'focus' of congressional concern," and in particular whether the conduct Congress sought to "regulate," and the object it sought to "protect," is domestic. *Id*. at 266-67 (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 255 (1991) ("*Aramco*")).

Applying this "focus" test to a provision of the Securities Exchange Act, *Morrison* held that "purchase-and-sale transactions are the objects of the statute's solicitude," so the location of those transactions determines where the Act is being applied. *Id*. at 267. Because the statute's "focus" is not the place where "the deception" giving rise to a fraud claim "originated"—there, Florida—"but upon purchases and sales of securities in the United States," no claim could be brought regarding a security traded abroad. *Id.* at 266; *see also City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG*, 752 F.3d 173, 180-81 (2d Cir. 2014) (the statute does not apply even when shares on a foreign exchange are "cross-listed on the NYSE," or "purchased … by placing a so-called 'buy order' in the United States"); *Loginovskaya v. Batratchenko*, 764 F.3d 266, 272 (2d Cir.

2014) (barring suit under the Commodity Exchange Act because "the transaction at issue—the *conduct* underlying the suit—[did not] occur[] within the United States," notwithstanding multiple domestic ties).

2. "Applying the same mode of analysis here" reveals that the "focus of congressional concern" in ECPA is stored electronic communications, so the relevant location is where they are stored. *Morrison*, 561 U.S. at 266.

First, what the statute seeks to protect and regulate are stored communications. Section 2703 appears in the portion of ECPA known as the *Stored* Communications Act. 18 U.S.C., ch. 121. And as the broader statute's name indicates, Congress enacted ECPA to protect the "Privacy" of "Electronic Communications" that providers store on behalf of their customers. To that end, the Stored Communications Act's first provision—§ 2701—does not regulate providers or discuss "disclosure" at all; it criminalizes a form of hacking: "access[ing] without authorization a facility through which an electronic communication service is provided," to "obtain[]" an "electronic communication … in electronic storage" there. Next, § 2702 turns its attention to providers, broadly prohibiting them from "divulg[ing] … the contents of a communication while in electronic storage" to anyone. The statute then exempts specified disclosures, including those required by valid law-enforcement demands for "communication[s] … in electronic storage." §§ 2702(b), 2703(a). The

"electronic storage" of "communications" is the thread that ties these provisions together.

Because stored communications are the "objects of the statute's solicitude," ECPA would be applied, for purposes of *Morrison*'s focus test, wherever those communications are stored. And, here, it is undisputed that ECPA is being invoked to obtain private electronic communications stored in Ireland. Nothing in § 2701 and § 2702 purports to extend protection to communications in electronic storage abroad. Ireland, like other foreign nations, has its own robust data protection and privacy laws. And just as the Act's protections do not apply to communications stored in other countries, § 2703's law-enforcement exceptions to those protections must also apply only to domestic communications.

The Government focuses instead on the term "disclosure." But under § 2703(a), law enforcement may require the "disclosure" of private electronic communications "*only pursuant to a warrant*"—a historically territorial instrument, which officers may command providers to "execut[e]," § 2703(g), by copying the requested emails out of "electronic storage" on their behalf, rather than execute themselves by forcing their way into the provider's facilities and attempting to navigate complex computer systems. § 2703(a); *see* OB 22, 30-32. The actual "conduct underlying" § 2703(a) is thus the "execution of a search

warrant" for particular communications in "electronic storage." *Loginovskaya*, 764 F.3d at 272-73.

Contrary to the Government's contention (at 21), our argument does not depend on how "the power being exercised … is labeled." Congress's use of the territorial term "warrant" supports reading § 2703 as limited to domestic communications, *see* OB 21-23, but the same conclusion obtains even under the Government's preferred terminology. Where a statute's focus is regulating stored emails, it is still an extraterritorial application of the statute to require that providers "collect" emails from electronic storage abroad and "import" them into the United States. GB 4. Either way, the subsequent act of disclosing those communications to government agents is just the domestic tail of an international dog.

Second, other features of the statute "confirm" Congress's focus on domestic communications. *Morrison*, 561 U.S. at 268. ECPA bans providers from disclosing customer emails, but creates exemptions for authorized disclosures to "governmental entit[ies]," and immunizes providers from liability for those disclosures. §§ 2702, 2703(e). But ECPA defines "governmental entity" as U.S. federal, state, and local governments—*not* foreign governments. § 2711(4). This scheme makes perfect sense if the "electronic storage" regulated by ECPA is limited to storage within the United States: The statute enables *domestic*

authorities to obtain *domestic* communications by serving *domestic* warrants issued by *domestic* courts, all the while protecting providers from *domestic* liability for those disclosures. If Congress meant ECPA to apply to emails stored abroad, it is "reasonable to conclude" that it "would have addressed the subject of conflicts with foreign laws and procedures" by exempting some disclosures to foreign governments for emails stored in *their* territory. *Aramco*, 499 U.S. at 256.

Instead, in 2009, long after the rise of the global internet, Congress amended the statute to enable "request[s] for foreign assistance" to be fulfilled only with the cooperation of *the U.S. Government*. §§ 2711(3)(A)(iii), 3512(a); *see* Foreign Evidence Request Efficiency Act, Pub. L. 111-79, 123 Stat. 2086 (2009). This amendment would be nonsensical if ECPA governed seizures of communications stored outside the United States. Why would a foreign country ask the United States to facilitate its seizure of communications stored in Ireland? The amendment demonstrates Congress's understanding that ECPA governs only domestic emails—as well as its preference for cooperative mechanisms like MLATs. *Contra* GB 48-53.[2]

[2] Although the Government repeatedly notes that Microsoft is a U.S. company, it does not argue that the place of incorporation bears on the extraterritoriality inquiry. With good reason. *See Aramco*, 499 U.S. at 255 ("The EEOC assures us that in its view the term 'employer' means only 'American employer,' but there is no such distinction in this statute."); *Balintulo v. Daimler*

3. The Government's other arguments against applying the presumption are meritless. The Government suggests the location of electronic storage is legally irrelevant because the provider "choose[s]" where to store electronic communications. GB 2, 54. That is like saying a U.S. company whose shares trade on a foreign exchange should be subject to suit under the Securities Exchange Act, notwithstanding *Morrison*, because it "chose" to list them there. The presumption against extraterritoriality takes statutes, and businesses, as it finds them.

The Government then asserts (at 31) that the presumption governs only "substantive provisions of … U.S. law." This Court has already rejected that very argument, noting that "*Morrison* … draws no such distinction." *Loginovskaya*, 764 F.3d at 272; *see also Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (presumption applies to the Alien Tort Statute, a "strictly jurisdictional" provision). Besides, ECPA *is* a substantive law: It protects the privacy of emails, subject to certain tailored exceptions, including § 2703(a). Indeed, contrary to the Government's assertion (at 31-32) that a court has inherent power to compel Microsoft to produce customer emails, the Government can

---

AG, 727 F.3d 174, 189-90 (2d Cir. 2013) (a defendant's "corporate citizenship in the United States" does not make an ATS claim domestic).

require Microsoft to assist it with the "execution of [this] search warrant" *only* because this statute grants it that extraordinary power. § 2703(a), (g).

B. The International Discord The Warrant Has Created Confirms This Would Be An Extraterritorial Application Of ECPA.

"In all cases applying the presumption against extraterritoriality to statutes, courts must be careful to recall the relevance of this canon—namely, 'to protect against unintended clashes between our laws and those of other nations which could result in international discord.'" *Mastafa v. Chevron Corp.*, 770 F.3d 170, 187 (2d Cir. 2014) (quoting *Aramco*, 499 U.S. at 248); *see* OB 19-20, 55. Thus, in "evaluating the 'relevant' conduct" under the presumption, this Court is "mindful of the Supreme Court's emphasis on … potential foreign policy implications." *Mastafa*, 770 F.3d at 187. Here, the potential for conflict with foreign data protection and privacy laws, and the international outrage over the Government's actions, further confirm that the "relevant" conduct under ECPA is the seizure of private communications from the country in which they are stored.

Morrison cited the "obvious" "probability of incompatibility with the applicable laws of other countries" as a strong signal that Congress did not intend to regulate foreign securities transactions. 561 U.S. at 269. The potential for conflict is similarly "obvious" here: Just as ECPA legislates a balance between protecting individuals' privacy rights and facilitating law enforcement in the United States, "foreign countries regulate [data privacy] within their territorial

jurisdiction." *Id*. "And the regulation of other countries often differs from ours." *Id*. The European Union, for example, has "strict rules designed to maintain the autonomy of [email users]" and "to regulate the transfer and storage of data, preserving the ability of the [email user] to control his personal data." Albrecht Br. 4, 7; DRI Br. 9-13; *see* Charter of Fundamental Rights of the European Union, art. 8(1) (2000) ("the right to the protection of personal data" is a fundamental right). This "obvious" overlap between ECPA and foreign laws provides a compelling reason to presume that Congress did not mean for ECPA to apply to communications stored abroad.

The Government incorrectly suggests (at 45-46) that Microsoft must actually prove that complying with the Warrant would violate Irish or EU law. But the presumption is a prophylactic rule meant to keep U.S. law well short of any conflict. That is why the "presumption applies *regardless* of whether there is a risk of conflict between the American statute and a foreign law." *Morrison*, 561 U.S. at 255.

In any event, as we explained (OB 13-14), the Warrant has already triggered the "unintended clashes" and "international discord" the presumption aims to prevent. *Aramco*, 499 U.S. at 248; *see* Albrecht Br. 11-12. Even more recently, the European Commission took the formal position "that personal data held by private companies in the EU should not, in principle, be directly accessed by or

transferred to foreign enforcement authorities outside of formal channels of cooperation, such as … MLATs."[3] And Europe's Data Protection Authorities issued a joint statement that, "[a]s a rule, a public authority in a non-EU country should not have unrestricted direct access to the data of individuals processed under EU jurisdiction," so "[f]oreign requests must not be served directly to companies under EU jurisdiction."[4] Europe's position is no surprise; in 2006, the U.S. and EU negotiated—and the Senate later ratified—a self-executing treaty that expressly favors bilateral cooperation for data seizures, not unilateral intrusions into each other's territory. *See* DRI Br. 15-19 & 22-25.[5]

Further rebutting the Government's suggestion (at 45) that the "comity concern[s]" raised here are "no[t] genuine," Ireland and Members of the European Parliament filed briefs telling this Court that they view execution of the Warrant as an incursion into sovereign territory, even though no federal agent plans to "use force to enter the Dublin datacenter." GB 20; *see* Ireland Br. 1, 4 (noting Ireland's

[3] European Parliament, Parliamentary Questions, No. E-010602-14 (Mar. 4, 2015), *available at* http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN.

[4] Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, at 3 (Nov. 26, 2014) (emphasis omitted), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf.

[5] Notwithstanding past actions of five European countries, *see* GB 45 & 46 n.21, the 28-member EU's stated position is that non-EU entities should not seize private data from the EU unilaterally.

"genuine and legitimate interest in potential infringements by other states of its sovereign rights with respect to its jurisdiction over its territory," and that "Ireland and the United States are parties to a treaty addressing the *subject of this appeal*."); Albrecht Br. 4, 10 (decrying this "territorial encroachment without justification"); *see also* Colangelo Br. 9-18. Yet in the Government's view, Ireland and the EU have no more interest in private communications stored on a computer in Ireland than Iceland or India do, because the only real action takes place in the United States. That is plainly not so.[6]

The Government does not even respond to Microsoft's observation (OB 23-24) that Congress *never* would have empowered state and local governments to seize private electronic communications stored abroad. Imagine the controversy that will arise when Europe learns that a county sheriff and magistrate, without federal supervision, have launched a raid of electronic communications stored on the Continent.

In short, the presumption against extraterritoriality, along with the *Charming Betsy* canon, *see* OB 34-35, "helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's

[6] Irish law does not allow the Irish government to do what the U.S. Government seeks here. *Contra* GB 46. The case Ireland cites (at 6) merely establishes that Ireland has a *Marc Rich* doctrine too. As discussed below (§ II), that doctrine has no application here.

highly interdependent commercial world." *F. Hoffman-La Roche Ltd. v. Empagram S.A.*, 542 U.S. 155, 164-65 (2004). Until Congress indicates otherwise, reading ECPA to allow each nation exclusive control over emails stored in its territory best maintains that harmony.

II. THE GOVERNMENT'S RELIANCE ON *MARC RICH* IS MISPLACED.

Disregarding *Morrison*'s admonition that "congressional silence" is no "justification for judge-made rules" on applying U.S. law abroad, 561 U.S. at 261, the Government "presume[s]" (GB 27-28) that Congress silently incorporated into ECPA the judge-made rule that a company may not "resist the production of documents on the ground that the documents are located abroad." *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983). As just demonstrated, the Government's position is inconsistent with the presumption *against* extraterritoriality.

But even if it were permissible to reverse the presumption, *Marc Rich* does not help the Government for two reasons. First, the Government's argument about what Congress silently intended is inconsistent with the statute Congress wrote. *See* § II.A. Second, no court has ever applied *Marc Rich* in circumstances remotely resembling these. Far from resting on "50 years of settled law," GB 9, the Government seeks a dramatic expansion of the *Marc Rich* rule for the internet age. *See* § II.B.

A. ECPA Requires The "Execution Of A Search Warrant," Not Compliance With A Subpoena "Hybrid" Or "Equivalent."

Doubling down on the district court's characterization of warrants issued under ECPA as "hybrid" subpoenas, SA 12, the Government insists that such warrants are "functionally similar to subpoenas." GB 18. They should thus be controlled, the Government claims, by all the same rules governing subpoenas (or summonses), including the *Marc Rich* principle that "records" under a party's control must be produced regardless of their location. That argument is incompatible with the statute's text and structure.

Text. The Government's contention flouts the statutory language in at least five ways.

First, the Government argues that "SCA warrants were designed to function as a form of compelled disclosure" because "government officials may use a warrant to 'require the disclosure' of communications." GB 18-19. But the ultimate "disclosure" cannot transform what the *statutory text* calls the "execution of a search warrant," § 2703(g), into what the Government calls "[t]he act of gathering records," GB 34. Rather, Congress spoke of "disclosure" in § 2703 only to create an exception to § 2702's broad prohibition against the "*disclosure* of customer communications or records," not to modify the meaning of "warrant." Repeating "disclosure" in § 2703 was necessary to allow those provisions to dovetail. "[D]isclosure" thus has the same meaning throughout the statute, *contra*

GB 18-19; it is the final step in which a provider may lawfully "divulge" to a governmental entity *whatever* material is yielded by the particular process used, whether a warrant, a subpoena, or § 2703(d) order. § 2702(b)(2).

Second, the Government argues that when Congress used the term "warrant," it meant only to require "a finding of probable cause by a magistrate judge," but that in "execution," a warrant should function as a "subpoena." GB 23-25. But warrants and subpoenas are different instruments, and § 2703 refers to both *separately*. OB 37-39. And the Government does not dispute that the word "warrant" has an established—and distinctly territorial—meaning, nor that § 2703 originally incorporated the Federal Rules of Criminal Procedure in full, including their territorial limitations.[7] OB 21-23. Congress would have said so if it intended to create a "hybrid" process, just as it did in § 2703(d).[8]

Third, the Government contradicts ECPA's plain text when it repeatedly characterizes emails as produceable "records." ECPA defines "records" as "*not including* the contents of communications." §§ 2702(c), 2703(c). Indeed, the

[7] Contrary to the Government's contention (at 22), § 2711(3)'s definition of a "court of competent jurisdiction" to *issue* a warrant says nothing about where the *object* of the warranted search and seizure must be found, and certainly not that it may be abroad.

[8] That § 2703 is modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq., sheds no light on whether Congress intended the warrants authorized under these provisions to apply to information stored abroad. GB 19. The Government points to no case in which a RFPA warrant reached information stored abroad, and we have found none.

purpose of the law was to ensure that emails not be treated like a "bank's … records," which can be produced in response to a subpoena. H.R. Rep. No. 99-647, at 23 n.41 (1986). Instead, they must be treated as "analogous to items stored, *under the customer's control*, in a safety deposit box." *Id*.

Fourth, § 2703 bears no resemblance to the compelled production rules to which the Government equates it. Such provisions typically speak of materials "in the responding party's *possession, custody, or control*," *e.g.*, Fed. R. Civ. P. 34(a)(1), 45(a)(1)(A)(iii); Fed. R. Crim. P. 16(a)(1), (b)(1), or more generally of "*producing*" documents, *e.g.*, Fed. R. Crim. P. 17(c); § 3486. Indeed, when *In re Harris*, 27 F. Supp. 480 (S.D.N.Y. 1939), first declared that "[t]he test" for ordering a bank "to produce" its records from abroad "is one of control, not of location"—a phrase *Marc Rich* later used—it cited the recently enacted Civil Rule 34, which had codified the "possession, custody, or control" principle. *Id.* at 481.

Section 2703, in contrast, never mentions "possession, custody, or control." Instead, it names the specific *place* where target communications must be found—"in electronic storage." The Government invokes the prior-construction canon, GB 17 (citing *Cannon v. Univ. of Chicago*, 441 U.S. 667, 696-97 (1979)), but ECPA's "language … is nowhere near identical" to the "compelled disclosure" rules construed in cases like *Marc Rich*, so "that canon has no application here."

Armstrong v. Exceptional Child Ctr., Inc., No. 14-15, 2015 WL 1419423, at *6 (U.S. Mar. 31, 2015).

And fifth, the Government misreads § 2703(g) to suggest that "warrants" under ECPA should be treated like subpoenas because they "are most often served in the same manner as subpoenas—by faxing or otherwise transmitting them to the provider, which then must gather the material required to be disclosed"—without the presence of an officer. GB 23. Far from suggesting that § 2703 simply requires the production of documents, however, § 2703(g) expressly *confirms* that ECPA requires the "execution of a search warrant." *See United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002); OB 40-41. In § 2703(g), Congress stated the one way "execution" could differ from the execution of a traditional warrant: A law-enforcement officer need not be present when the provider executes the warrant on its behalf.[9]

Structure. Equally without merit is the Government's suggestion (at 13) that § 2703 operates as an "upside-down pyramid," in which greater forms of process (like warrants) can do everything that lesser forms (like subpoenas) can and more. The *types of materials* that a warrant or a subpoena can demand do fit such a hierarchy. But the *scope* of each form of process does not nest in the same

[9] Notwithstanding its choice over "the history of *this* litigation," GB 20, the Government does not dispute that federal agents always have the power to execute a valid warrant themselves. *See* OB 28 n.3.

way: Where warrants require particularity, for example, subpoenas may order production from anywhere, sometimes even abroad. *See* OB 38-39. In any event, Congress's focus was on the world as it existed at the time, when electronic communications were stored only domestically. As to such domestically stored communications, ECPA 'nests' in precisely the way the Government says it should. By no means can the Government's inference substitute for a clear statement by Congress that the statute has a global sweep.

Relatedly, the Government contends (at 28-30) that warrants for emails must reach abroad, because subpoenas for emails older than 180 days would. That argument is based on a false premise. *No* email of *any* age can be obtained by subpoena; the statute's 180-day distinction is a dead letter after *Warshak*—a decision the Government has never challenged. *See* OB 9, 45 n.4; A 123; Brennan Center Br. 15-23; H.R. Rep. at 68, 72 (explaining the now-outdated justification for the six-month rule). Recognizing this, the Government asserts the question is instead "what Congress intended when it passed the SCA," prior to *Warshak*. GB 28 n.10. If so, the answer is Congress gave the matter no thought: In 1986, U.S.-based companies did *not* store emails abroad. OB 24-25. The Government may not ask this Court to "'discern' whether Congress *would have* wanted the statute to apply" to foreign electronic storage. *Morrison*, 561 U.S. at 255.

B. *Marc Rich* Does Not Apply To Attempts To Procure Third Parties' Private Papers From Abroad.

Congress cannot be presumed to have intended *Marc Rich* to apply here for a second reason: The principle has only ever applied to subpoenas for a recipient's own business records. Notwithstanding a caretaker's physical "possession, custody, or control," the principle has never required a caretaker to import sealed private documents it merely holds in trust for a customer, such as papers in a foreign safe deposit box or the contents of a package in transit overseas. OB 43.[10] The Government cites no example of such a subpoena. This case should not be the first.

1. Only one of the Government's cases mentions foreign documents at all. *United States v. First Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968); GB 37-38. But the Government misreads the case. The subpoena there requested no documents like private papers locked in a safe deposit box, but only a *bank's* own "documents … relating to any transaction in the name of (or for the benefit of)" the customer. *First Nat'l City Bank*, 396 F.2d at 898. In a footnote describing Germany's narrow "bank secrecy doctrine," the Court referenced "material entrusted to a bank within the framework of [a] confidential relationship." *Id.* at

[10] The Government notes the district court's statement that Microsoft waived the argument that customers own their emails. GB 36 & n.14. But it does not defend that conclusion, much less rebut our demonstration (OB 53 n.7) that this point was preserved.

900 n.8. But the Court did *not* hold that such materials must be produced; no such materials were at issue. *See also In re First Nat'l City Bank*, 285 F. Supp. 845, 846 (S.D.N.Y. 1968) (describing the documents as "records [that] *refer*" to particular customers). Moreover, even materials revealed in confidence "relating to [a] transaction" between customer and bank are not private in the relevant sense. *See United States v. Miller*, 425 U.S. 435 (1976). Private correspondence entrusted to a caretaker for safekeeping in a secured lockbox is.

2. Every other case the Government invokes (at 38-40) involved subpoenas for third parties' papers that custodians held *domestically*. And even the domestic cases are off-point. Some, like *Barr* and *Giovanelli*, involved no compulsion at all, but rather caretakers who voluntarily delivered private materials to the Government (in *Giovanelli*, without even a Government request) and never tested the validity of the Government's demands. *United States v. Barr*, 605 F. Supp. 114 (S.D.N.Y. 1985); *United States v. Giovanelli*, 747 F. Supp. 891 (S.D.N.Y. 1989). Neither considers whether a subpoena can compel an unwilling caretaker to produce a third party's private sealed papers.

Horowitz, meanwhile, concerned an accountant who had "free run to look at what he pleased" in his client's papers. *United States v. Horowitz*, 482 F.2d 72, 82 (2d Cir. 1973). Under *Miller*, clients have no reasonable expectation of privacy in papers that are exposed to a caretaker, even in confidence. In contrast, customer

emails are neither unsealed nor given to Microsoft to read. Indeed, in *Horowitz* the district court had *quashed* the subpoena to the extent it sought various personal documents and "strictly personal" letters in the accountant's possession. *Horowitz*, 482 F.2d at 75 & n.2.

United States v. First National City Bank, 568 F.2d 853 (2d Cir. 1977), only proves that a safe deposit box *cannot* be subpoenaed from a bank merely because it is in the bank's "possession, custody, or control." There, the "IRS issued jeopardy levies" to summarily seize assets from a safe deposit box before the taxpayer could secret them away. *Id.* at 855. The district court then issued an "order," supported by probable cause, "that the bank allow the government to search the box" itself. *Id.* at 858. This Court rejected a Fourth Amendment challenge only because, in all respects, the search resembled a standard warranted search and seizure by government agents, notwithstanding that the district court's order, for reasons unknown, referred to a "formal subpoena." *Id.* at 855.

3. It is unsurprising that the Government can point to no case, even in the domestic context, where a subpoena compelled an unwilling bank to produce customer papers locked in a safe deposit box in its "possession, custody, or control." A customer's sealed documents remain in the customer's sole "constructive possession." *United States v. Guterma*, 272 F.2d 344, 346 (2d Cir. 1959); *see* OB 45-47. Surely the Government, which "[s]ince 2009 … has been

shifting its data storage needs to cloud-based services and away from agency-owned, in-house data centers," would agree that it retains exclusive control of the documents *it* stores with cloud providers—and that a foreign government could not demand them just because they are accessible from a cloud provider's foreign computer.[11] Email customers reasonably expect providers *not* to peruse, let alone disclose, their private communications. That is why ECPA and the Fourth Amendment require a warrant to access emails. § 2703(a); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

Citing Microsoft's terms of service, the Government claims that Microsoft's limited right to access its customer's emails (for example, to maintain security) makes it more than a mere caretaker of that private correspondence. GB 41-42. The Sixth Circuit rejected exactly that argument in *Warshak*. Although providers may "reserve[] the right to access [a customer's] emails for certain purposes," that does not "extinguish [the customer's] reasonable expectation of privacy" in emails or cause it to become the provider's property. *Warshak*, 631 F.3d at 286-87. The

[11] Congressional Research Service, *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management* 1, (Jan. 20, 2015), *available at* http://fas.org/sgp/crs/misc/R42887.pdf.

more relevant provision of the Microsoft Services Agreement confirms this: "Who owns my Content that I put on the Services?" "You do."[12]

4. Even if the Government could use a subpoena to compel a caretaker to hand over a customer's private, sealed correspondence stored *within* the United States, however, it cannot do so *outside* the United States without clear congressional authorization.

As we explained (OB 48-52), ordinary *Marc Rich* subpoenas (e.g., for bank records) generate international friction even when used to procure a recipient's *own* business records. The international friction is exponentially more intense where the Government demands the seizure of a *customer's* private papers—a law-enforcement seizure of documents on foreign soil, against a target it might not have been able to reach but for its ability to conscript an email provider into service. International friction will only grow as individuals, companies, and governments store more private information in the cloud. As with smartphones, "there is an element of pervasiveness that characterizes" emails and other private documents stored in the cloud. *Riley*, 134 S. Ct. at 2490. The justifications for a pre-internet doctrine allowing worldwide compelled production of a company's "business information," *First Nat'l City Bank*, 396 F.3d at 901, simply do not fit

[12] *See* Windows, http://windows.microsoft.com/en-us/windows/microsoft-services-agreement, ¶ 3.1.

the "sensitive records previously found in the home" that citizens of every nation now store in the cloud, mostly with U.S.-based providers. *Riley*, 134 S. Ct. at 2491.

Moreover, there is no question that other nations view the seizure of individuals' private electronic communications as a serious intrusion. Yet the Government does not dispute Microsoft's observation (OB 50) that the execution of a warrant would offer no ex ante opportunity for parties to raise these questions of international comity, as *Marc Rich* subpoenas generally do. *See, e.g., United States v. Davis*, 767 F.2d 1025, 1033 (2d Cir. 1985). It cannot be that the *more* intrusive form of process affords *less* opportunity for a court to balance the foreign-relations cost against the domestic law-enforcement benefit.

In short, the *Marc Rich* regime cannot account for the practical realities of executing a warrant for a customer's private emails. That disconnect underscores why there is a presumption against extraterritoriality in the first place: Congress alone has the institutional competence to craft a scheme governing the seizure of private communications from foreign countries.

III. ONLY CONGRESS CAN DECIDE WHETHER AND HOW TO MODIFY ECPA.

Ultimately, the Government does not think its "ability to obtain [customers' emails] from a provider [should] turn entirely on whether [they] happen[] to be stored here or abroad." GB 53. The plaintiffs in *Morrison*, *Kiobel*, and *Aramco*

would sympathize. But the Department of Justice is addressing its self-described "policy considerations" to the wrong branch. GB 48. If ECPA no longer serves the Government's law-enforcement needs in the age of the global internet, and if—contrary to the only record evidence, *see* OB 57-58—existing tools of international cooperation like MLATs do not suffice, then the Government may ask Congress to expand the reach of § 2703. Indeed, bipartisan legislation pending in Congress would do just that. *See* Law Enforcement Access to Data Stored Abroad Act, S. 512 & H.R. 1174, 114th Cong. (2015).

Microsoft fully supports legislative efforts to bring ECPA into the 21st century. But only Congress can balance competing concerns that touch on foreign relations, the economy, and privacy. The Department of Justice may have nothing to say, for example, about the risks of encouraging foreign governments to propound demands for the emails of newspaper reporters and other U.S. customers stored on computers in the United States. *See* OB 1-2, 56, 59-60. But Congress surely would.

The Government says it is enough that "[t]here is no reason to believe that Congress intended to exclude" foreign-stored email from § 2703's reach. *E.g.*, GB 51. As noted (*supra* at 17, 22), that turns the presumption against extraterritoriality on its head. The Government also urges this Court to close a "loophole" created by the global internet. GB 51-52, 54. The Supreme Court

rejected a nearly identical argument in a nearly identical context, when a plaintiff contended that the "eas[e]" of sending data abroad created a "'loophole'" in the Patent Act: Any "'loophole,' in [the Court's] judgment, is properly left for Congress to consider, and to close if it finds such action warranted." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 452, 457 (2007). So too here: The "ease" of importing data across international borders is no justification for ignoring those borders.

In any event, there is no loophole. Microsoft endeavors to store customer communications at the data center closest to the customer to minimize network latency. A 36-37. It does not regularly move communications among servers, as the Government suggests (at 51-52), because as amici Computer Scientists explain (at 17), doing so would be inefficient.

* * *

It bears remembering that ECPA itself was enacted as a response to gaps in the Wiretap Act—a law that was "written in [a] different technological and regulatory era," before communications had moved from "the human voice over common carrier networks" to the state-of-the-art "[e]lectronic mail," "videotext," and "paging" services of the 1980s. H.R. Rep. at 17, 22-23. Just as ECPA's drafters sought "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement" in light of then-current technologies,

H.R. Rep. at 19, so too will a new Congress have to revisit that balance in light of today's technologies and global interconnectedness. And whatever statute Congress passes now, it will surely have to revise a generation hence to reflect technological advances we cannot yet imagine. For now, the presumption against extraterritoriality limits ECPA, and the Warrant issued under the statute, to communications stored on U.S. soil.

CONCLUSION

This Court should reverse the district court's judgment.

Respectfully submitted,

s/ E. Joshua Rosenkranz
E. Joshua Rosenkranz
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019
(212) 506-5000

Counsel for Appellant

April 8, 2015

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B)(ii) because this brief contains 6,968 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman 14-point font.

ORRICK, HERRINGTON & SUTCLIFFE LLP

s/ E. Joshua Rosenkranz

E. Joshua Rosenkranz
Counsel for Appellant