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

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
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

CORPORATE DISCLOSURE STATEMENT

Microsoft Corporation has no parent corporation and no other publicly held corporation owns 10% or more of its stock.

Respectfully submitted,

ORRICK, HERRINGTON & SUTCLIFFE LLP

s/ E. Joshua Rosenkranz

E. Joshua Rosenkranz
Counsel for Appellant

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

FEDERAL RULES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION

Imagine this scenario. Officers of the local Stadtpolizei investigating a suspected leak to the press descend on Deutsche Bank headquarters in Frankfurt, Germany. They serve a warrant to seize a bundle of private letters that a *New York Times* reporter is storing in a safe deposit box at a Deutsche Bank USA branch in Manhattan. The bank complies by ordering the New York branch manager to open the reporter's box with a master key, rummage through it, and fax the private letters to the Stadtpolizei.

The U.S. Secretary of State fumes: "We are outraged by the decision to bypass existing formal procedures that the European Union and the United States have agreed on for bilateral cooperation, and to embark instead on extraterritorial law enforcement activity on American soil in violation of international law and our own privacy laws." Germany's Foreign Minister responds: "We did not conduct an extraterritorial search—in fact *we* didn't search anything at all. No German officer ever set foot in the United States. The Stadtpolizei merely ordered a German company to produce its own business records, which were in its own possession, custody, and control. The American reporter's privacy interests were fully protected, because the Stadtpolizei secured a warrant from a neutral magistrate."

No way would that response satisfy the U.S. Government. The letters the reporter placed in a safe deposit box in Manhattan are her private correspondence, not the bank's business records. The seizure of that private correspondence pursuant to a warrant is a law enforcement seizure by a foreign government, executed in the United States, even if it is effected by a private party whom the government has conscripted to act on its behalf.

This case presents a digital version of the same scenario, but the shoe is on the other foot. The Electronic Communications Privacy Act of 1986 ("ECPA") allows federal agents and local police to command email providers to execute a "warrant" to seize customers' private emails from the digital lockboxes they secure with a password. Federal agents served such a search warrant on Microsoft's U.S. headquarters, requiring it to search for a customer's private emails, copy them, and turn them over. The emails, however, are located exclusively on a computer in Dublin, Ireland, where they are protected by Irish and European privacy laws. When the Government nevertheless tried to force Microsoft to access the correspondence abroad and import it into the United States, the European Commissioner of Justice reacted as our hypothetical Secretary of State did—with almost the same words.

To avoid just this sort of international discord, courts presume that federal statutes do not apply extraterritorially unless Congress expresses a clear intent for

them to do so. Congress, however, gave no indication in ECPA that it intended to authorize federal and local police to commandeer service providers to execute searches and seizures of private emails located in foreign countries. Nor did Congress express any intention to allow the Government to ignore established avenues for international cooperation, such as Mutual Legal Assistance Treaties, to obtain such evidence.

The district court nevertheless upheld the extraterritorial execution of the warrant here and held Microsoft in contempt for refusing to comply. It ruled that when Congress used the term "warrant," it actually meant a "hybrid" subpoena, indistinguishable from the type that can compel a bank to produce its own transaction records from a foreign branch. So long as no federal agents tread on Irish soil, it concluded, there is no impermissible extraterritorial action. That was wrong, as a matter of both the statute's plain meaning and extraterritoriality principles.

The power to embark on unilateral law enforcement incursions into a foreign sovereign country—directly or indirectly—has profound foreign policy consequences. Worse still, it threatens the privacy of U.S. citizens. The Golden Rule applies as much to international relations as to other human relations. If the Government prevails here, the United States will have no ground to complain when foreign agents—be they friend or foe—raid Microsoft offices in their jurisdictions

and order them to download U.S. citizens' private emails from computers located in this country. That would put all of our private digital information at risk, not just emails, but everything else we store on remote computers collectively called "the cloud"—a veritable "cache of sensitive personal information" saturated with the highest constitutional privacy rights. *Riley v. California*, 134 S. Ct. 2473, 2490-91 (2014).

By requiring Congress to speak clearly when extending U.S. law abroad, the presumption against extraterritoriality ensures that only Congress decides when to subordinate international comity to other governmental interests. Congress did not make—and, indeed, did not even consider—any such tradeoff in ECPA. On the contrary, ECPA's text and history show Congress believed the law would only apply domestically. If the Government wants the unprecedented power it claims here, it should plead its case to Congress. Meanwhile, the warrant issued here cannot reach emails stored in Ireland, and the judgment should be reversed.

JURISDICTIONAL STATEMENT

The magistrate judge had jurisdiction to issue and modify the warrant under 28 U.S.C. § 636(a)(1) and (b)(3). The district court had jurisdiction to review the magistrate judge's order under 28 U.S.C. § 636(b). *See United States v. Williams*, 23 F.3d 629, 634 (2d Cir. 1994). The district court adopted and affirmed the magistrate judge's order on July 31, 2014. Special Appendix ("SA") 29-31, 32.

Microsoft filed a timely notice of appeal on August 11, 2014. Appendix ("A") 337. The court then held Microsoft in contempt on September 8, 2014, for refusing to comply. SA 36. Microsoft amended its notice of appeal on September 9, 2014. A 344-46. This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUE

Congress is presumed to intend that its statutes do not apply abroad unless it clearly says so. In the Electronic Communications Privacy Act of 1986, Congress granted local, state, and federal law enforcement officers the power to conscript a private party—an email provider—to execute a warrant to search for and seize a customer's personal emails. But it said nothing about warrants authorizing the search and seizure of correspondence that resides on foreign computers. And it required a warrant, a legal instrument Congress understood to be a *domestic* law enforcement tool. The question is whether law enforcement may nevertheless invoke ECPA to conscript providers to search and seize private emails in a foreign country.

STATEMENT OF THE CASE[1]

The Government applied for and Magistrate Judge Francis issued a warrant ("Warrant") to seize the contents of an email account belonging to a customer of Microsoft Corporation. Microsoft moved to vacate the Warrant insofar as it sought emails stored outside the United States. The magistrate judge denied the motion (2014 WL 1661004). Microsoft filed objections with the district court (Chief Judge Preska), which adopted and affirmed the magistrate judge's order in a bench ruling. SA 29-30, 32. The district court then held Microsoft in contempt for refusing to comply with the Warrant. SA 36.

The Electronic Communications Privacy Act Extends To Email The Same Privacy Protections That Are Afforded To Other Private Communications

Congress enacted the Electronic Communications Privacy Act of 1986 "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986) ("Senate Report"). At the time, the Fourth Amendment and federal statutes and regulations afforded "[a] letter sent by first class mail … a high level of protection against unauthorized opening." *Id.* at 5. So, too, for "[v]oice communications." *Id.* But there were no established protections for electronic communications. This raised concerns because individuals who used to "lock

[1] All statutory references are to Title 18 of the United States Code unless otherwise indicated. All emphasis in quotations is added, unless otherwise indicated.

away" their private correspondence and documents were beginning to store "a great deal of personal and business information" on "remote computers" and with "providers of electronic mail." *Id.* at 3.

Congress feared courts might strip this private information of protection. In particular, the Supreme Court had already concluded that customers "lack … any legitimate expectation of privacy" in certain types of "information voluntarily conveyed to" third parties—there, bank records of transactions—even with promises of confidentiality. *United States v. Miller*, 425 U.S. 435, 442 (1976) ("The checks are not confidential communications, but negotiable instruments to be used in commercial transactions."). Congress worried that courts would apply that third-party rule to correspondence that individuals entrust to providers of electronic communications. Senate Report 3. Congress understood that risk could "unnecessarily discourage potential customers from using innovative communications systems" and "discourage American businesses from developing new innovative forms of telecommunications and computer technology." *Id*. at 5. "Most importantly," Congress feared that the "precious right" to privacy would "gradually erode as technology advances." *Id.*

To that end, ECPA first broadly prohibits providers of electronic communications services from "knowingly divulg[ing] to any person or entity,"

including law enforcement officers, the "contents of a communication" held on behalf of a customer, § 2702(a), subject to certain exceptions, § 2702(b).

ECPA then describes additional exceptions, in which a law enforcement officer—federal, state, or local—may force a provider to turn over customer communications and related information. § 2703. The statute grants three tiers of protection, commensurate with the customer's expectations of privacy. For the content of recent emails, considered at the time to be the most private, Congress provided the highest level of protection. "A governmental entity may require the disclosure by a provider of electronic communication service of the contents of" those communications "only pursuant to a warrant." § 2703(a). On the other extreme were the provider's "records" of basic customer information, such as their name and when they opened the account. Officers could obtain that far less sensitive information by a standard subpoena. § 2703(c)(2). In the middle was information Congress viewed as confidential but not as sensitive as the communications themselves, such as a customer's transmission log, detailing the sender, recipient and time of an email. § 2703(c)(1). For such information, ECPA created a new hybrid court order—referred to as a "(d) order." § 2703(d). To secure a (d) order, officers must make a higher showing to the court than for a subpoena (which requires no court pre-approval), but less than for a warrant. § 2703(c)(1), (d).

This basic structure remains in effect today, with one important change: The warrant protection now covers all email content, regardless of age. While omitting older emails from the warrant requirement made sense in 1986 when customers typically did not store emails with providers after opening them, *see infra* 45 n.4, the distinction between old and recent emails is constitutionally untenable in the modern age of total and indefinite storage. As the Sixth Circuit has held, an email account is a "conglomeration" of "sensitive and intimate" stored messages that "provides an account of its owner's life." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). Accordingly, "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with … a commercial" service provider and "to the extent [ECPA] purports to permit the government to obtain such emails warrantlessly, [ECPA] is unconstitutional." *Id*. at 288 (internal quotation marks omitted).

This case concerns ECPA's warrant provision, § 2703(a). Before ECPA, an officer armed with a warrant could enter an email provider's offices and search for and seize customer communications from its computers, but the typical officer lacked the technical skill to execute such a search. ECPA gave law enforcement a powerful alternative. Instead of executing a warrant themselves, officers could serve the warrant on the provider and compel it to search for and seize its customer's property on the Government's behalf, and then "disclose" the fruits of

that search and seizure to the Government. § 2703(a), (g). When the provider is compelled to assist with a warrant's execution, ECPA provides that "the presence of an officer shall not be required for service or execution of [the] search warrant," although he may be present. § 2703(g). Regardless of which path the Government chooses, it may seize private emails "only pursuant to a *warrant* issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." *Id*. § 2703(a).

Microsoft Operates A Web-Based Email Service

Microsoft operates a web-based email service called Outlook.com. A 35. While email providers like Microsoft used to store small amounts of customers' email for only a short time, and any long-term storage of it was local, Outlook.com allows customers to store a lifetime of emails remotely in Microsoft's datacenters. A 35-36.

As Microsoft's web-based email service spreads around the globe, Microsoft confronts the problem of "network latency": Quality of service worsens and response time slows the further the customer is from the datacenter where his emails are stored. A 36-37. While using the internet often feels lightning quick, that is only because companies have structured their systems to facilitate data transmission efficiently. The more miles of physical cable data must travel, the

slower the service. Maximizing quality of service by minimizing network latency is therefore a business imperative. To address the problem, Microsoft built datacenters closer to its customers and endeavors to store customers' communications at the closest datacenter. A 36-37.

One such datacenter, opened in 2010, is in Dublin, Ireland. Microsoft's Irish subsidiary leases and operates the Dublin datacenter. A 36. When a customer's account is assigned to the Dublin datacenter, her email content (i.e., the message and subject line) resides in that datacenter on a specific computer. That email content is not stored in any form inside the United States. A 37.

Microsoft Complies With Lawful Law Enforcement Demands

With the rise of electronic communications, federal, state, and local governments, as well as foreign law enforcement, have increasingly required technology companies to assist in criminal investigations. Microsoft and other technology companies receive thousands of demands each year from law enforcement agencies. To accommodate its duties to both its customers and law enforcement, Microsoft complies with lawful orders from U.S. authorities.

When Microsoft receives a search warrant for a customer's emails, Microsoft's Global Criminal Compliance team handles the response. A 39. To collect the emails, a compliance team member first must determine the location of the Microsoft computer on which they are stored. For information or

correspondence stored in the United States, the team member collects the data from the domestic server, as the warrant commands. SA 4-5. Likewise, when the Irish Government seeks a customer's information through valid Irish legal process, Microsoft produces data stored in Ireland directly to Irish authorities. A 105-06.

The situation is different, however, when the U.S. Government seeks data stored in Dublin or the Irish Government seeks data stored in the United States. For such data, the Government can invoke the United States-Ireland Mutual Legal Assistance Treaty ("MLAT"), which allows the U.S. and Irish Governments to seek data through the Irish Ministry of Justice and the U.S. Department of Justice, respectively. A 105-06.

The Government Directs Microsoft To Execute A Warrant For Customer Emails Stored In Dublin

In December 2013, federal agents conducting a drug investigation served the Warrant, issued by a magistrate judge in the Southern District of New York, to search for and seize information associated with a Microsoft customer's web-based email account. A 40, 44-48. The "SEARCH AND SEIZURE WARRANT" purports to authorize the search and seizure of property "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation." A 45. An attachment to the Warrant directs Microsoft to seize "[t]he contents of all e-mails stored in the account, including copies of e-mails sent from the account," and "all records or other information stored … including address books, contact and buddy

lists, pictures, and files" "for the period of inception of the account to the present." A 46-47.

Microsoft's compliance team determined that certain information associated with the customer's account, like the customer's address book, is stored in the United States, and turned over this information to the Government. A 40-41, 50. The customer's email *content*, however, is located in Dublin, Ireland. *Id.* Microsoft moved to vacate the warrant to the extent it directed the seizure of the customer's emails located abroad. A 40; *see* A 24.

The Magistrate Judge Denies Microsoft's Motion And The District Court Affirms

The magistrate judge denied Microsoft's motion. SA 26. He reasoned that although Congress used the term "warrant" in § 2703(a), it meant a "hybrid: part search warrant and part subpoena." SA 12. The magistrate judge thus invoked the rule "that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information." SA 13. Accordingly, he concluded, ECPA "does not implicate principles of extraterritoriality." SA 12. Believing the MLAT process to be "burdensome and uncertain," the magistrate judge opined that Congress would not have intended to have the Government rely on it. SA 20-21.

The magistrate judge's ruling prompted international outrage. The European Commissioner for Justice protested: "The effect of the US District Court order is

that it bypasses existing formal procedures that are agreed between the EU and the US, such as the Mutual Legal Assistance Agreement, that manage foreign government requests for access to information and ensure certain safeguards in terms of data protection." A 151. She added, "that the extraterritorial application of foreign laws (and orders to companies based thereon) may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union." A 151. Foreign newspapers blasted the United States with headlines such as: "US Wants to Rule over All Servers Globally." A 153.

Microsoft filed objections to the magistrate judge's order in the district court. In a brief ruling from the bench, the district court adopted and affirmed the memorandum and order of the magistrate judge. SA 31; *see* SA 32. (Accordingly, this brief refers to the magistrate judge's written order as part of the district court's ruling.) The court then held Microsoft in contempt for not complying with the Warrant. SA 36.

SUMMARY OF THE ARGUMENT

I. An Act of Congress does not apply outside the United States unless Congress clearly says so. This "presumption against extraterritoriality" guards against unintended international conflict, and safeguards the Constitution's separation of powers by recognizing that Congress alone is capable of making such

an important policy decision. Particularly since *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), this Court applies this rule strictly.

ECPA's warrant provision says nothing about conscripting service providers to conduct law enforcement searches and seizures abroad. That silence alone means ECPA does not grant that power. Indeed, Congress actually used language showing that it meant § 2703(a) to apply only domestically: The provision requires a "warrant," a tool that has long been understood to be valid only within U.S. territory. As enacted, the provision incorporated the Rules of Criminal Procedure in whole, which expressly limit the territorial reach of warrants. And ECPA gives equal power to state and local law enforcement officers, which Congress would not have authorized had it intended the statute to apply in foreign countries.

Because this Warrant orders a law enforcement seizure in Ireland, it calls for the unauthorized extraterritorial application of § 2703(a). A warrant issued under ECPA compels a provider to execute a law enforcement search and seizure. A warrant is inherently a law enforcement device. The search and seizure of private correspondence from a secure location is a law enforcement activity—whether the correspondence is physical or digital. That is why the Sixth Circuit has held that an order demanding a customer's "sensitive and intimate" emails from a service provider is a seizure, which can be achieved only with a warrant. *Warshak*,

631 F.3d at 284, 288. It makes no difference that the Government has opted to compel Microsoft to execute the Warrant on its behalf. Conscripting Microsoft to effect the search and seizure in Ireland does not make it any less of a law enforcement search and seizure by the U.S. Government. The Government has not disputed that a seizure of electronically stored information occurs where the customer's private emails are located—and there is no dispute that is Ireland.

II. The district court erred in relying on the rule articulated in *Marc Rich & Co., A.G. v. United States*, that the "test for production of documents is control, not location." 707 F.2d 663, 667 (2d Cir. 1983). That rule governs subpoenas for a company's own business records, not warrants for customers' property. There is no basis in the statute's text for the district court's conclusion that Congress actually meant to create a new "hybrid" subpoena when it said warrant. Instead, Congress relied on an existing form of legal process. Section 2703(a) requires a "warrant," not a "subpoena." Other provisions in § 2703 address subpoenas or create new legal instruments. Congress's choice to refer to those distinct forms of process must be respected.

The *Marc Rich* rule stems from a presumption that companies have control over *their own* books. That rule has never been applied to require a caretaker to import a customer's private papers and effects from abroad. Thus, a bank can be compelled to produce the transaction records from a foreign branch, but not the

contents of a customer's safe deposit box kept there. A customer's emails are similarly private and secure and not subject to importation by subpoena.

This Court should reject the Government's invitation to extend *Marc Rich* to cover this law enforcement seizure. It causes international friction enough when a subpoena requires a U.S. company to produce its own records from a foreign country in violation of that country's law. The diplomatic stakes are higher where a company is ordered to seize someone else's private papers in aid of a foreign government's law enforcement investigation. As it is, *Marc Rich* sits in uneasy tension with the presumption against extraterritoriality; it should not be extended to grant the Government the extraordinary power it seeks here.

III. The district court worried that criminal investigations will be hampered if § 2703(a) is limited to U.S. territory. But under the presumption against extraterritoriality, Congress alone is empowered to decide whether the benefits of authorizing extraterritorial conduct exceed the costs. Even if the court could properly make that policy decision on Congress's behalf, its analysis was flawed. To obtain evidence from abroad, the Government has available to it the efficient Mutual Legal Assistance Treaty process and the Budapest Convention's 24/7 hotline to facilitate the immediate preservation of electronic data.

The district court also failed entirely to account for countervailing policy concerns. If the United States asserts unilateral authority to seize private email

correspondence on foreign soil, other countries will claim the same unilateral authority to seize the private emails of U.S. citizens stored on U.S. soil. By encouraging such reciprocal actions, the district court's position would thwart ECPA's primary objective of protecting U.S. citizens' private electronic information. It also puts at risk the U.S. technology sector's continued ability to operate and compete globally by requiring providers to carry out law enforcement activities, possibly in contravention of foreign laws, and discouraging foreign customers. Only Congress is positioned to weigh these competing interests.

STANDARD OF REVIEW

This Court reviews a district court's finding of contempt "under an abuse of discretion standard that is more rigorous than usual, and … conduct[s] a *de novo* review of any rulings of law" on which it was based. *S. New England Tel. Co. v. Global NAPs Inc.*, 624 F.3d 123, 145 (2d Cir. 2010) (internal quotation marks omitted).

ARGUMENT

I. ECPA DOES NOT AUTHORIZE WARRANTS FOR SEIZURES OF CUSTOMER EMAILS IN OTHER COUNTRIES.

Acts of Congress do not apply abroad unless Congress clearly says they do. § I.A. Far from expressing such an intent in ECPA, Congress indicated that warrants issued under ECPA should apply only within the United States. § I.B. Because the Warrant here compels Microsoft to conduct a search and seizure of

private customer data in Ireland on the Government's behalf, it authorizes an impermissible extraterritorial application of ECPA. § I.C.

A. Under The Presumption Against Extraterritoriality, Statutes Have No Application Abroad Unless Congress Clearly Says They Do.

"It is a 'longstanding principle of American law "that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States."'" *Morrison*, 561 U.S. at 255 (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) ("*Aramco*") (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949))). There is a "presumption against extraterritorial application," *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013), which may be "rebutted *only* when the statute's text, history, and purposes evince a clear indication of extraterritoriality," *Liu Meng-Lin v. Siemens AG*, 763 F.3d 175, 178 (2d Cir. 2014) (internal punctuation omitted). "When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255.

The presumption safeguards the Constitution's separation of powers and "helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel*, 133 S. Ct. at 1665. In the "delicate field of international relations," Congress "alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord

are so evident and retaliative action so certain." *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957).

B. Congress Gave No Clear Indication That ECPA's Warrant Provision Should Apply Extraterritorially.

All indications—from the text, context, and legislative amendments—are that in enacting § 2703(a) Congress was focused exclusively on the domestic application of the statute.

Text. There is no hint in ECPA's text that warrants may compel service providers to seize email content in electronic storage in a foreign country. It reads:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

§ 2703(a). The text is silent as to extraterritorial reach. And "silence means no extraterritorial application." *Morrison*, 561 U.S. at 261.

When Congress intends its statutes to apply abroad, it does not hide the ball. Congress normally specifies not only *whether* a statute applies extraterritorially but also *when* it does so (e.g., only when a U.S. citizen or national is involved). Thus, Congress strikes the delicate balance between any need for extraterritorial application and the risk of international friction. For example, the Dodd-Frank Act

gives district courts "*[e]xtraterritorial jurisdiction*" of suits for certain violations of antifraud laws involving "conduct occurring *outside the United States*," but only when they have "a foreseeable substantial effect within the United States." 15 U.S.C. § 80b-14(b)(2). Similarly, Congress extended Title VII to protect U.S. citizens "employ[ed] in a foreign country," but only when employed by *U.S. companies* and not if compliance with Title VII would "violate the law of the foreign country in which such workplace is located." 42 U.S.C. §§ 2000e(f), 2000e-1(b)-(c).

Section 2703(a) is more than just silent, though. In several respects, the statutory text confirms that Congress meant it to apply only within U.S. boundaries. First, the very decision to say that a "warrant" is required to obtain private electronic communications indicates that Congress intended only domestic application. "Warrant" is a legal term of art. "[W]here Congress borrows terms of art in which are accumulated the legal tradition and meaning of centuries of practice, it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed." *Morissette v. United States*, 342 U.S. 246, 263 (1952); *see Sekhar v. United States*, 133 S. Ct. 2720, 2724 (2013).

The "cluster of ideas" that attends the term "warrant" includes the understanding that ordinarily "United States district judges possess no extraterritorial jurisdiction"—no jurisdiction even beyond their own *districts*—and thus may not issue warrants for searches and seizures abroad. *Weinberg v. United States*, 126 F.2d 1004, 1006 (2d Cir. 1942). It has long been understood that "[a] warrant issued by a U.S. court would neither empower a U.S. agent to conduct a search nor would it necessarily compel the intended target to comply. It would be a nullity …, 'a dead letter.'" *United States v. Odeh*, 552 F.3d 157, 170 (2d Cir. 2008) (quoting *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990)); *see United States v. Toscanino,* 500 F.2d 267, 279 (2d Cir. 1974) (holding that the Wiretap Act, upon which ECPA was built, "significantly makes no provision for obtaining authorization for a wiretap in a foreign country" and "has no application outside of the United States"), *abrogated on other grounds by Verdugo-Urquidez*, 494 U.S. 259, *as recognized by Odeh*, 552 F.3d at 167; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) ("there is presently no statutory basis for the issuance of a warrant to conduct searches abroad"). Had Congress meant to apply § 2703 abroad to authorize the Government to compel email providers to seize private communications held overseas, it would not have hidden its intention in a term with so territorial a connotation as "warrant."

Second, Congress incorporated into ECPA the very rule that expressly limits the territorial reach of warrants, Federal Rule of Criminal Procedure 41. As originally enacted, ECPA authorized federal and state law enforcement officers to require providers to turn over private email content "only pursuant to a warrant issued *under the Federal Rules of Criminal Procedure* or equivalent State warrant." Pub. L. No. 99-508 § 201, 100 Stat. 1848 (1986) (creating § 2703(a)). Thus, Congress imported Rule 41 into ECPA, hook, line, and sinker, including the provision that strictly limits issuing judges' authority to issue warrants for property "located within the district." Fed. R. Crim. P. 41(b)(1). So warrants contemplated by § 2703(a) were unequivocally limited to the United States from the outset.[2] As discussed below (at 25-26), Congress changed this language in 2001, but only to make warrants effective "*Nation*wide," not *world*wide.

Third, Congress authorized "*any State or political subdivision thereof*" to seek a warrant, § 2711(4), and any "*State court*" to issue one, § 2703(a). In the domestic context, state and local prosecutors use this warrant power regularly. *See, e.g.*, *State v. Rose*, 330 P.3d 680, 684-85 (Or. Ct. App. 2014); *Preventive Med. Assocs. v. Commonwealth*, 992 N.E.2d 257, 261 (Mass. 2013); *State v. Esarey*, 67 A.3d 1001, 1007 (Conn. 2013). Congress could not have meant to empower a

[2] Rule 41 provides for three specific applications of Rule 41 overseas—all situations that are within U.S. territorial jurisdiction—indicating an intention to exclude other extraterritorial applications. Fed. R. Crim. P. 41(b)(5); *see* 18 U.S.C. § 7(9).

sheriff's deputy in Dublin, Mississippi, to instigate an international crisis by ordering a search and seizure in Dublin, Ireland. "There is, of course, no question that at some point an exercise of state power that touches on foreign relations must yield to the National Government's policy." *Am. Ins. Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003). The "degree of self-restraint and consideration of foreign governmental sensibilities generally exercised by the *U.S. Government*" is not often exercised by other parties. *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 171 (2004) (citation omitted). Against this backdrop, Congress's grant of equal power to federal, state, and local law enforcement demonstrates that it did not expect that authority to reach electronic communications abroad.

Context. When Congress enacted ECPA in 1986, it did not even imagine the possibility that a service provider might store emails in another country—much less that it would store them abroad and access them from here. The "World Wide Web" had not yet been invented. Some users sent electronic messages, but the services that brought email to the broad public—Microsoft Mail, America Online, and Compuserve—were still years away. *See generally* G.B. Delta & J.H. Matsuura, *Law of the Internet* § 1.02 (2014). Companies like MCI transmitted messages on their domestic long-distance telephone networks, but international calling rates made such services effectively inaccessible abroad. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 404 (2014)

(hereinafter *Next Generation*); *see* U.S. Congress, Office of Technology Assessment, OTA-CIT-293, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 46-47 (1985). Congress knew only a world where U.S. providers stored the communications of U.S. citizens on computers located on U.S. soil. Kerr, *Next Generation* at 404. "ECPA simply was not written with the territoriality problem in mind." *Id.* at 410.

Amendments. In the intervening decades, as the world around it changed, Congress amended § 2703(a), but only in ways that reinforced its territorial limitations. In 2001, Congress superseded Rule 41(b)'s within-district requirement for warrants issued under § 2703(a) by specifying that the Government may obtain emails pursuant to "a warrant issued ~~under~~ *using the procedures described in* the Federal Rules of Criminal Procedure." USA PATRIOT Act, Pub. L. No. 107-56 § 220(a)(1), 115 Stat. 291 (2001); H.R. Rep. No. 107-236, at 57 (2001). Congress did this because "the cross-jurisdictional nature of the Internet" led to "investigative delays" as officers sought warrants in other districts. H.R. Rep. No. 107-236, at 57. But Congress erased borders only with respect to searches *within* the United States. Congress titled the amendment "*Nationwide* Service of Search Warrants for Electronic Evidence." Pub. L. No. 107-56 § 220(a)(1). It explained that this provision now "[p]ermit[s] a single court having jurisdiction over the offense to issue a search warrant for email that would be valid … anywhere *in the*

United States." 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) (section-by-section bill analysis). If Congress had even the slightest thought that warrants issued under § 2703(a) had always reached (or should now start reaching) *anywhere outside the United States*, this would have been the place to mention it. But Congress said the opposite.

In short, there is "no language in the ECPA itself, nor … any statement in the legislative history" of any iteration of ECPA even remotely suggesting that Congress meant to enact a statute allowing federal or local officers to reach into the territory of a foreign sovereign to extract electronic communications. *Cunzhu Zheng v. Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297, at *3 (N.D. Cal. Dec. 2, 2009).

C. This Warrant Is An Unauthorized Extraterritorial Application Of § 2703(a) Because It Compels Microsoft To Conduct A Law Enforcement Search And Seizure In Ireland.

Three basic propositions confirm that the Warrant here is an invalid extraterritorial application of § 2703(a): (1) a warrant issued under ECPA compels a provider to execute a law enforcement search and seizure; (2) the search and seizure occur in Dublin, where the emails reside; and (3) the execution of a search and seizure in another country is an extraterritorial application of U.S. law.

1. A warrant issued under ECPA compels the provider to execute a law enforcement search and seizure.

Whenever a law enforcement agent searches for and seizes private correspondence from a secure location locked away from the public, it engages in a law enforcement search and seizure. It is a law enforcement search and seizure whether the agent descends on Citibank to seize letters a customer locked away in a safe deposit box or descends on Microsoft to seize letters the customer locked in the digital lockbox of an email account. The nature of the activity does not change depending on whether the letter is written on ink or on magnetic disks. Digital is not different.

That was the very premise of the Sixth Circuit's ruling, discussed above (at 9), that a law enforcement officer must secure a warrant in order to demand emails from a service provider. Customers use email "to send sensitive and intimate information." *Warshak*, 631 F.3d at 284. "Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button." *Id*. An email account is a veritable "cache of sensitive personal information." *Riley*, 134 S. Ct. at 2490. That is why *Warshak* held that ordering a service provider to copy and send the Government such sensitive communications is a law enforcement seizure.

Congress understood that the conduct compelled under § 2703(a) is a law enforcement seizure: That is why Congress required a "warrant," a tool used to

authorize searches and seizures. Just look at the Warrant in this case (reproduced on the next page). It is the standard form AO-93 "SEARCH AND SEIZURE WARRANT" used throughout the federal courts to authorize searches and seizures by law enforcement. A 44. It is addressed, "To: Any authorized law enforcement officer." A 44. It directs: "YOU ARE COMMANDED to execute this warrant" to conduct a "search" for "information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled or operated by Microsoft Corporation." A 44-45.

This Warrant on its face authorizes a federal agent to descend on Microsoft, demand entry, forcibly remove a technician at a terminal, and remotely access any Microsoft computer—in Dublin or anywhere else in the world. *See* § 3109. The Department of Justice insists that federal agents (and presumably local police) may "search the provider's computers themselves."[3] The Government does not dispute that if a federal agent does that, then the resulting act is a law enforcement search and seizure.

[3] U.S. Dep't of Justice, Office of Legal Education, Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 113 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

AO 93 (SDNY Rev. 05/10) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of)
(Briefly describe the property to be searched or identify the person by name and address)) Case No.
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.
✓ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court. JCH
USMJ Initials

☑ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☑ for 30 days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: December 4, 2013 4:30 pm

James C. Francis IV
Judge's signature

City and state: New York, NY

Hon. James C. Francis IV, Magistrate Judge, SDNY
Printed name and title

Of course, the agent is not required to—and usually does not need to—execute a warrant for emails himself. Although federal officers ordinarily must be present for the execution of a search warrant, *see* § 3105, ECPA makes their presence optional ("not … required"), § 2703(g). Thus, here, an agent faxed this Warrant to Microsoft—and Microsoft is responsible for "execut[ing] ... the search warrant," § 2703(g), by seizing the emails and disclosing them to the Government for its review. A 46-47. But that does not change the Warrant into something else. Seizing such email content is a law enforcement seizure regardless of whether the Government does so directly or conscripts a private party to copy the emails and send them for its subsequent review.

For nearly a century it has been established that "a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search." *Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006) (Sotomayor, J.). For example, in considering a federal regulation that required a railroad to test employees for drugs and alcohol, the Court held that a "railroad that complies with [the regulation] does so by compulsion of sovereign authority" and therefore "act[s] as an instrument or agent of the Government." *Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602, 614 (1989). That result flowed inexorably from the Court's holding decades earlier in *Gambino v. United States*: Where individuals "made [an] arrest, search and seizure … solely for the

purpose of aiding the United States in the enforcement of its laws," the search and seizure are treated as if conducted by the Government. 275 U.S. 310, 316-17 (1927) (Brandeis, J.). Similarly, when an employee at a mail carrier opens a letter, the search is treated as the Government's search if it is conducted "with the participation or knowledge of any governmental official," but not if it was "effected by a private individual *not* acting" at the Government's direction. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). As *Warshak* held, and the Supreme Court has since confirmed, *see Riley*, 134 S. Ct. at 2490, this same rule applies with equal force whether the mail is physical or electronic. *See infra* 9.

2. The law enforcement search and seizure occur where the emails are located.

The question, then, is where does the law enforcement search and seizure occur? The Government does not dispute that the email content at issue here is located "exclusively" on a computer "in Dublin, Ireland." A 38, 40. A seizure of electronic mail occurs at the time it is copied and in the place where it is stored. That is because "cop[ying]" an individual's "personal computer records … deprive[s] him of exclusive control of those files," and a "seizure occurs when the Government interferes in some meaningful way with the individual's possession of property." *United States v. Ganias*, 755 F.3d 125, 133, 137 (2d Cir. 2014) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights" (citing *Loretto v. Teleprompter*

Manhattan CATV Corp., 458 U.S. 419, 435 (1982)); *see* Fed. R. Crim. P. 41(e)(2)(B) (equating the "on-site copying" of "electronically stored information" with a "seizure").

Remote access does not change the equation. The search and seizure occur where the evidence is, not where the agent sits. An agent who uses a listening device to insinuate his "uninvited ear" into a phone booth performs a search and seizure without ever stepping foot inside. *Katz v. United States*, 389 U.S. 347, 352-53 (1967). When an agent points a thermal imaging sensor at a house "from the passenger seat of [his] vehicle across the street," the search is in the house, not in the car and not on the exterior wall. *Kyllo v. United States*, 533 U.S. 27, 30, 35 & n.2 (2001).

Just last Term, the Supreme Court applied these same principles to a search of electronic data in the cloud. It observed that "[c]loud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley*, 134 S. Ct. at 2491. When the police access that information from a smartphone on the street "at the tap of a screen," the search occurs on the "remote server," not on the street. *Id*.; *see In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756-57 (S.D. Tex. 2013) (it is that "physical space with a local habitation" where the "search takes place, not in the airy nothing of cyberspace," and not at the remote location from

which Government agents may "obtain and view the information gathered from the Target Computer"). The Government cannot dispute this. Government agents sitting in the United States hack into foreign computers and search them remotely without a warrant. When the target asserts that the search occurred in the U.S.—and therefore required a warrant—the Government has correctly (and successfully) responded that the seizure occurred abroad, where the information resided, not in the United States, where the agents sat. *See United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001).

3. The execution of a search warrant in a foreign country is an extraterritorial application of U.S. law.

Given that execution of the Warrant would effect a law enforcement search and seizure in Ireland, the Government's effort to apply § 2703(a) to emails stored abroad is an extraterritorial application of U.S. law. That conclusion is especially evident in light of the international law norms that the Government's excursion would violate. It is a fundamental principle of international law that a "state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state." Restatement (Third) of the Foreign Relations Law of the United States, § 432(2). This "corollary of state sovereignty" applies in particular to foreign "criminal investigation[s]." *Id.* cmt. b. International law prohibits such law enforcement seizures. *See Alvarez-Machain v.*

United States, 331 F.3d 604, 615 (9th Cir. 2003) (en banc), *rev'd on other grounds by Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004).

U.S. courts are, therefore, especially resistant to Government efforts to extend law enforcement reach abroad. The Supreme Court said it two centuries ago: "The jurisdiction of the nation within its own territory is necessarily exclusive and absolute." *The Schooner Exchange v. McFaddon*, 11 U.S. (7 Cranch) 116, 136 (1812); *see The Appollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) ("It would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories for the purpose of seizing vessels which had offended against our laws."). The en banc Ninth Circuit made a similar point when addressing a seizure carried out by a private party at the behest of the United States: "Few principles in international law are as deeply rooted as the general norm prohibiting acts of sovereignty that offend the territorial integrity of another state." *Alvarez-Machain*, 331 F.3d at 615. This Court, too, has said it unequivocally: "The United States has no right to enforce its laws in another country without that country's consent or acquiescence." *United States v. Blanco*, 861 F.2d 773, 779 (2d Cir. 1988).

The imperative to preserve the territorial integrity of foreign nations is so strong that it provides an independent basis on which to invalidate the Warrant. "It has been a maxim of statutory construction since the decision in *Murray v. The*

Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804), that 'an act of congress ought never to be construed to violate the law of nations, if any other possible construction remains.'" *Weinberger v. Rossi*, 456 U.S. 25, 32 (1982); *see United States v. Yousef*, 327 F.3d 56, 86 (2d Cir. 2003) (the *Charming Betsy* principle applies when "determining whether Congress intended a federal statute to apply to overseas conduct"). Accordingly, while recognizing that "Congress is not bound by international law" and "may legislate with respect to conduct outside the United States, in excess of the limits posed by international law," this Court has held that, as with the presumption against extraterritoriality, Congress must "expressly indicate[] its intent to reach such conduct." *Id.* As discussed above (at 20-26), there is none here.

Because § 2703 authorizes the Government to require a provider to conduct a law enforcement seizure of its customer's private email, the place that the warrant is executed—where the emails are seized—determines whether the statute has extraterritorial application. That intrusion is where the "unintended clashes" and "international discord" may arise. *Aramco*, 499 U.S. at 248. Where, as here, the search and seizure would occur at a datacenter in a foreign country, Congress would have had to decide to apply the statute extraterritorially. In the case of ECPA, Congress did not, so this Warrant cannot reach data stored in Ireland.

II. THE DISTRICT COURT IMPROPERLY TREATED THE WARRANT AS A "HYBRID" SUBPOENA SEEKING MICROSOFT'S OWN RECORDS WITH NO EXTRATERRITORIAL EFFECTS.

In ordering Microsoft to comply with the Warrant, the district court did *not* find that Congress intended for § 2703(a) to apply extraterritorially. Rather, the court held that there is simply no extraterritorial application of U.S. law when Microsoft complies with a warrant issued under § 2703(a) to seize a customer's emails from Ireland. The court began with the premise that a "warrant" issued under § 2703(a) resembles a subpoena seeking a company's business records. SA 30. Based on that analogy, the court invoked the *Marc Rich* rule that when a company receives a subpoena seeking its own records, the company may not "resist the production of documents on the ground that the documents are located abroad." 707 F.2d at 667; *see United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984). The court, therefore, surmised that Congress must have intended this subpoena principle to apply to warrants issued under § 2703(a). SA 30.

The court erred at each step. The premise that Congress thought of this "warrant" under § 2703(a) as a "hybrid" subpoena rather than a warrant is inconsistent with the statute Congress actually wrote. § II.A. In any event, cases about routine document production under a subpoena have no bearing here. The power of a subpoena to reach business records anywhere in the world has only ever applied to a company's own records, not to private documents it holds in trust for

its customers. § II.B. This Court should not extend the principle to a law enforcement search warrant seeking to retrieve a customer's private emails from a foreign country. § II.C.

A. The District Court's Premise That Congress Considered A "Warrant" Under § 2703(a) To Be A "Hybrid" Subpoena Is Inconsistent With The Statute Congress Wrote.

The district court's application of principles governing *subpoenas* to "warrants" issued under § 2703(a)—and, therefore, its entire extraterritoriality analysis—rests on the quicksand foundation of a mistaken premise: "Although section 2703(a) uses the term 'warrant' and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather the order is a hybrid: part search warrant and part subpoena." SA 12. The notion that Congress used the word "warrant" to mean "subpoena" (or "something like a subpoena") is inconsistent with the statute's text.

1. ECPA provides for both warrants and subpoenas, but does so separately and treats them differently. Section 2703(a) requires a "warrant" for the Government to obtain individuals' most private electronic communications. In contrast, the next two subsections ((b) and (c)) authorize the Government to obtain less sensitive information, like subscriber information or a "network address," via "an administrative subpoena … or a Federal or State grand jury or trial subpoena." § 2703(c)(2). By concluding that Congress intended to treat warrants like

subpoenas, the district court failed to "respect Congress' decision to use different terms to describe different categories … of things." *Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1708 (2012).

There is no question that the terms "warrant" and "subpoena" "describe different categories … of things." A warrant constitutes the judicial authorization, founded on a finding of probable cause, of an activity that is uniquely assigned to law enforcement—intruding upon an individual's reasonable expectation of privacy to conduct a search and seizure. *See, e.g.*, *Black's Law Dictionary* 1553 (10th ed. 2014). A search warrant is directed toward a particular place to be searched and person or thing to be seized, rather than a person who might possess or control the sought-after evidence. And "[t]o preserve advantages of speed and surprise, [a warrant] is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion." *United States v. Bailey*, 228 F.3d 341, 348 (4th Cir. 2000).

A subpoena, in contrast, "command[s] a person to appear before a court," and may order the person "to bring specified documents, records, or things." *Black's Law Dictionary* 1654 (10th ed. 2014); *see* Fed. R. Crim. P. 17(c)(1). It does not authorize law enforcement searches or the seizure of a customer's property, nor is it directed to a particular location. Unlike a warrant, "the issuance of a subpoena initiates an adversary process that can command the production of

documents and things only after judicial process is afforded." *Bailey*, 228 F.3d at 348. That process allows the recipient, or the party with a privacy interest in the documents (such as the reporter in our opening hypothetical), to challenge a subpoena.

Congress must be presumed to have been aware of these plain—and plainly different—meanings when it used these terms in sequential provisions of ECPA. The district court erred in indulging exactly the opposite presumption—that Congress imported into the word "warrant" principles that courts had applied only to the very different device called a "subpoena." Nothing in the statute Congress actually wrote suggests that Congress silently combined in § 2703(a) the compulsion of a law enforcement search warrant (already substantially enhanced by the power to conscript the service provider to carry out the search for the Government) and the sweeping geographic scope of a subpoena. Congress would have spoken clearly had it meant to arm the government with such a Frankenstein super-warrant-subpoena hybrid, rather than "hid[ing] elephants in mouseholes." *Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001).

In fact, when ECPA's drafters wanted to create a hybrid, they did so explicitly. Section 2703(d) creates a novel "court order for disclosure" that allows the Government to obtain more user information than a subpoena would provide but less than a warrant. This special hybrid with its own ECPA-specific name—a

"(d) order"—has its own unique procedures. And Congress did not label it with a legal term of art that means something different. The district court erred in disregarding Congress's carefully reticulated regime and instead applying rules applicable to subpoenas (like *Marc Rich*) where Congress unambiguously demanded a "warrant."

2. More evidence of Congress's understanding appears at the end of the same section. As noted above (at 30), § 2703(g) provides that "the presence of an officer shall not be required for service or execution of a search warrant." § 2703(g). The impetus behind tacking on § 2703(g) in 2002 confirms that Congress never thought of a warrant under § 2703(a) as some sort of hybrid subpoena. The subsection was a response to a district court ruling that a search of electronic communications was unreasonable because a law enforcement officer "was not present and acting in the warrant's execution," as § 3105 requires, "when the [provider's] employees searched and seized information from [the defendant's email] account." *United States v. Bach*, No. Crim. 02-221 PAM/ESS, 2001 WL 1690055, at *2 (D. Minn. Dec. 14, 2001). The Eighth Circuit reversed, holding that "[t]he Fourth Amendment," unlike § 3105, "does not explicitly require official presence during a warrant's execution." *United States v. Bach*, 310 F.3d 1063, 1066-67 (8th Cir. 2002). With § 2703(g), Congress went one step further "clarif[ying]," as a statutory matter, "that a law enforcement officer does not need

to be present for a warrant executed under" ECPA. H. Rep. No. 107-497 at 79 (2002).

This whole dialogue among the courts and Congress would have been unnecessary if § 2703(a) operated like a musclebound subpoena that obliges providers to produce their customer's documents. No official presence is ever required for the "execution" of a subpoena. Indeed, the Eighth Circuit rejected the argument that the standards governing subpoenas should apply to warrants issued under § 2703(a). The court noted that "[w]hile warrants for electronic data are often served like subpoenas (via fax), *Congress called them warrants and we find that Congress intended them to be treated as warrants*." *Bach*, 310 F.3d at 1066 n.1. And when specifically focused on the operation of § 2703 in 2002, Congress did not say anything different; it did not say that when it authorized the seizure of emails pursuant to a warrant, it really meant a subpoena. To agree with the district court here is to read into the statute a term that Congress did not use and to split with the Eighth Circuit's holding that warrants issued under § 2703(a) must be examined under standards applicable to warrants rather than subpoenas.

B. The Subpoena Rules Applicable To A Company's Own Records Do Not Extend To Caretakers Who Hold Customers' Private Communications In Trust.

Even if the district court's characterization of the warrant as a "hybrid" subpoena comported with the statute, it would be improper to apply the rules

governing subpoenas here. Those rules have never been applied to compel a company to produce from abroad anything but *its own* business records. They should not be extended to require a caretaker who holds private letters and papers in trust for a customer to turn them over to law enforcement, let alone to import those documents from abroad.

1. The district court went astray when it applied the subpoena rule that a grand jury "witness [may not] resist the production of documents on the ground that the documents are located abroad" because "[t]he test for production of documents is control, not location." *Marc Rich*, 707 F.2d at 667; *see* SA 13. *Marc Rich*'s possession-and-control test traces back to this Court's century-old decision in *In re Ironclad Mfg. Co.*, 201 F. 66 (2d Cir. 1912). *Ironclad* involved no question of cross-border subpoenas, but only whether a party to a domestic case could be excused from "produc[ing] the books and papers called for [in a court order] … by the mere bald statement of some officer that he does not know where they are." *Id.* at 68. This Court naturally rejected the dodge, announcing a "presumption that a corporation is in the possession and control of *its own books*." *Id.*

Courts after *Ironclad* applied the possession-and-control standard numerous times to prevent a company from avoiding a document request by putting its own "books and records" out of the country. *See Nat'l Pub. Util. Investing Corp. v.*

United States, 79 F.2d 302, 303 (2d Cir. 1935) (suggesting companies should not be permitted to move their "books and records" out of the country for some "sinister purpose," such as "put[ting] them beyond the reach of tax investigators"); *First Nat'l City Bank of N.Y. v. IRS*, 271 F.2d 616, 618 (2d Cir. 1959). We are aware of no decision applying this principle when a company holds documents abroad for someone else, documents that the company is *not* free to peruse at its pleasure or do with as it pleases.

Under *Marc Rich*, the Government could require Citibank to produce its own business records from its Panamanian branch, *see First Nat'l City Bank*, 271 F.2d at 618-19, or FedEx to produce its own log of shipments sent from Dublin. The Government could not, however, serve a subpoena on Citibank's Park Avenue headquarters compelling the bank to pry open a safe deposit box in Panama, copy its contents, and send that copy to New York. Nor could it direct FedEx to intercept a customer's letter in Ireland and import it by serving a subpoena on its Memphis headquarters. The bank and the carrier may have physical custody over its customers' private papers, but those papers and effects are not the companies' "own books," *Ironclad Mfg.*, 201 F. at 68, and are therefore not properly subject to compelled importation pursuant to a *Marc Rich* subpoena. Instead, the Government would need to employ some other tool to execute what is, in reality, a search and seizure on foreign soil.

2. The same principles that apply in the physical world apply to electronic communications. On the one hand, a transmission log detailing the sender, recipient, and time of an email—like a bank's account ledger or a list of package recipients—constitutes a provider's own business records and contains information communicated to it "in the ordinary course of business." *United States v. Miller*, 425 U.S. 435, 442 (1976). Email customers, like bank account holders or FedEx customers, "lack … any legitimate expectation of privacy" in such non-content information they have "voluntarily conveyed to the banks [or providers or carriers] and exposed to their employees." *Id.*

On the other hand, a customer's private email correspondence is no different from the contents of a safe deposit box or the letter inside a FedEx envelope. Like those physical letters, an electronic message belongs to the customer alone, not the email provider. Email correspondence is personal, even "intimate." *Warshak*, 631 F.3d at 284. An email account can contain "[t]he sum of an individual's private life," including "a record of all his communications," "a thousand photographs," and materials like "a prescription, a bank statement, a video." *Riley*, 134 S. Ct. at 2489. Electronic letters do not become the caretaker's records any more than physical letters do. Rather, an email provider is a mere "intermediary that makes email communication possible," "not the intended recipient of the emails"; it is the "functional equivalent of a post office." *Warshak*, 631 F.3d at

286-88; *see id.* at 288 ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here.").

In ECPA, Congress specifically recognized this distinction between emails and business records. Emails, Congress explained, are "analogous to items stored, *under the customer's control*, in a safety deposit box," as opposed to a "bank's (or remote computing service's) records." H.R. Rep. No. 99-647, at 23 n.41 (1986) (distinguishing *Miller*). That is why Congress granted customers' emails the highest level of privacy protection—expressly *excluding* "the contents of communications" from its definition of a provider's "records," § 2703(c), and instead requiring a "warrant" before the Government could obtain the contents of customers' private email messages, § 2703(a).[4]

Because of customers' privacy interests in their emails, providers exercise only limited control over those emails. Email users protect their personal data with passwords, much as bank customers use locks to secure personal property held in a

[4] Section 2703(a) applies only to unopened emails held by a provider for up to 180 days because at the time of ECPA's enactment, email would be deleted from the provider's computer as soon as it was retrieved by the customer, or at most within "a few months." H.R. Rep. No. 99-647, at 68; *see* Senate Report 3, 8. Emails left behind were considered copies left with the provider for its own processing, like ensuring system integrity or billing customers. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1234 (2004); H.R. Rep. No. 99-647, at 68. Now, of course, customers use email very differently, which is why the Sixth Circuit recognized that the Government must obtain a warrant for all email content, regardless of age. *See Warshak*, 631 F.3d at 288.

safe deposit box and FedEx customers seal letters in an envelope. In doing so, customers "plainly manifest[] an expectation that [their] emails [will] be shielded from outside scrutiny." *Warshak*, 631 F.3d at 284. Email providers, like banks and mail carriers, are only limited custodians of their customers' private correspondence and property. By deciding what papers to safeguard inside and securing them to prevent others from gaining access, customers retain the right of control over the contents of those papers even when they are stored with the provider—the "functional equivalent of the post office." *Id*. at 286; *see Ex parte Jackson*, 96 U.S. 727, 733 (1887) ("Letters and sealed packages … in the mail are as fully guarded from examination and inspection … as if they were retained by the parties forwarding them in their own domiciles," and the Government must obtain a warrant to inspect them "as is required when papers are subjected to search in ones' own household.").

That was the central rationale in this Court's opinion in *United States v. Guterma*, 272 F.2d 344 (2d Cir. 1959): "The fact that the records [are] physically in the possession of" a caretaker like a bank is "of no consequence" absent "proof … that [the owner] had turned over his personal records to [the caretaker] to become *part of its files and records*." *Id.* at 346. Rather, they remain in the "constructive possession" of the owner and so cannot be seized "through the mere procedural device of compelling a third-party naked possessor to produce and

deliver them." *Id.* at 346 (internal quotation marks omitted). Thus, in *Guterma*, this Court quashed a subpoena that directed a company to produce the personal papers of its chairman, who kept them in a safe in the office. The papers were the chairman's alone—not the company's—to produce or withhold. This same premise underlies the *Warshak* court's holding that the "government may not *compel a commercial ISP to turn over* the contents of a subscriber's emails" by means of a subpoena regardless of whether the ISP technically has possession, custody or control; the government must first obtain "a warrant based on probable cause." *Warshak*, 631 F.3d at 288.

It makes no difference that the caretaker can, in theory, remove the lock on a safe deposit box, "rip open a letter," or bypass a password. *Warshak*, 631 F.3d at 287. As the Government has "concede[d]" elsewhere, a landlord's mere "right to enter the apartment … of another" is insufficient "control" to allow "'the government [to] subpoena the landlord to produce the tenant's personal papers from her apartment.'" *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 611 (5th Cir. 2013). So too, a provider's "naked possess[ion]" of private emails is insufficient "control" to allow the Government to obtain them pursuant to a subpoena. *Guterma*, 272 F.2d at 346. And it is surely not at the level of control that animates *Marc Rich*'s rule.

Here, again, ECPA's text proves the point. Because customers' private email communications are held in trust, ECPA prohibits service providers from "knowingly divulg[ing] … the contents" of email messages to anyone other than the sender, the addressee, or its intended recipients. § 2702(a). This nondisclosure provision contains exceptions, but not for discovery subpoenas. Thus, providers may *never* produce those communications in response to discovery subpoenas even though the communication may be in the providers' "possession, custody, or control." *Viacom Int'l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008). Thus, ECPA's text, once again, defeats the district court's premise—that service providers have the same "control" over emails that banks have over their own business records.

C. *Marc Rich* Should Not Be Extended Because A Law Enforcement Warrant Requiring The Seizure Of A Customer's Private Papers Presents More Grave International Comity Concerns Than Ordering A Company To Disclose Its Own Records.

The *Marc Rich* rule causes enough international "friction" when a subpoena requires a company to produce its *own* records from a foreign country in violation of that country's law. *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 544 n.29 (1987) (*Aérospatiale*). That is why the courts have enumerated various factors, summarized in Restatement § 442, to guide "a careful balancing of the interests involved" in each "particular case" before deciding whether to enforce such a subpoena, so as "to minimize the potential conflict" with

foreign law. *United States v. First Nat'l City Bank*, 396 F.2d 897, 901 (2d Cir. 1968).[5] That is also why the Department of Justice requires U.S. Attorneys to secure prior approval from the Office of International Affairs ("OIA") before serving a subpoena seeking evidence stored abroad. U.S. Dep't of Justice, *United States Attorneys' Manual*, *Criminal Resource Manual*, tit. 9 § 279, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00297.htm (listing factors OIA must consider, including "the availability of alternative methods for obtaining the records … such as mutual assistance treaties" and "the indispensability of the records to the success of the investigation or prosecution"). *Marc Rich* cannot properly be extended to this context.

The district court deemed § 442 of the Restatement "dispositive" here in establishing "that the production of [the] information [requested from an email provider] is not an intrusion on the foreign sovereign," because it provides that courts are "empowered to" order the production of documents from abroad. SA 30. Even on its own terms, that reliance was wrong. The Restatement acknowledges, as does the underlying case law, that even vanilla cross-border

[5] *See also Aérospatiale*, 482 U.S. at 544 n.28 (courts should consider factors such as "the availability of alternative means of securing the information" and "the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located"); *Société Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*, 357 U.S. 197, 205-06 (1958).

subpoenas infringe upon foreign sovereignty to some degree, which is why courts must balance the interests before compelling production. Restatement (Third) of Foreign Relations § 442 (1)(c) & cmt. c. The Restatement simply does not suggest that the power to order production somehow overcomes all concerns with foreign sovereignty to determine when it is appropriate to compel production. Because of its error, the court failed to address *how* the customer could raise such competing challenges in the context of a *warrant*, which, unlike a subpoena, *compels* the provider to disclose the customer's emails without affording the customer any opportunity to challenge production.

Moreover, the district court's holding clashes directly with *Warshak* and *Guterma*, which stand for the proposition that subpoenas do not reach constitutionally protected private communications or "papers and effects" held in trust by a caretaker on behalf of a customer. While the Government previously acquiesced in that ruling, A 123, it now questions it, A 267. This Court need not decide here whether the Government could ever simply subpoena a customer's private communications from a caretaker. As indicated above, the issue can be avoided entirely by honoring the plain words in ECPA that require a *search warrant* before a service provider seizes emails, and by following *Morrison*'s rule in holding that warrants issued under ECPA do not reach abroad.

On the latter point, the district court failed to recognize how much more offensive it is to foreign sovereignty to use a law enforcement warrant to seize a person's private correspondence than it is to compel a company to gather its own records. As discussed above (at 27-35), executing a warrant in a foreign sovereign country to obtain a customer's private documents is a search and seizure in that country, which implicates a different section of the Restatement, § 432(2). Under that section, a law enforcement action taken without the sovereign's permission breaches international law.

The district court dismissed all concerns about unauthorized intrusions on foreign sovereignty because a warrant issued under § 2703(a) "does not involve the deployment of American law enforcement personnel abroad," and "does not require even the physical presence of service provider employees at the location where the data are stored." SA 21-22. But sovereign nations have interests in resisting all foreign intrusions, even if they involve remote computer access rather than boots on the ground. Indeed, most of the Supreme Court's extraterritoriality cases also involved no "deployment of American law enforcement personnel abroad," but merely attempts to impose U.S. norms on foreign conduct. *See, e.g.*, *Morrison*, 561 U.S. 247 (applying U.S. securities laws to foreign transactions); *Kiobel*, 133 S. Ct. 1659 (asserting U.S. jurisdiction over foreign torts).

Surely, the United States would not abide the Stadtpolizei ordering DHL or Citibank's employees at a local facility to impound customers' papers in the U.S. and ship them abroad. Nor would it tolerate a Stadtpolizei order directing a Microsoft employee in Germany to download everything in a customer's U.S.-based email account.

It is no surprise, then, that European leaders are equally furious with the U.S. Government's conduct here (as documented at 13-14). The protection foreign countries afford emails housed within their borders is substantial; Ireland and the European Union have some of the strongest data privacy laws in the world. *See* A 116; European Union Directive 95/46, art. 1 (recognizing and protecting "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"); Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Brussels, Jan. 25, 2012), art. 3(2), at 41 (proposing even more expansive protections).

Marc Rich teeters on unsteady ground as it is. *Morrison* abrogated "many decades" of cases from "various courts of appeals" that endeavored "to 'discern' whether Congress would have wanted the [Securities Exchange Act] to apply" extraterritorially on a case-by-case basis. 561 U.S. at 255. That approach

amounted to "disregard" of the long-standing "presumption against extraterritoriality." *Id.* The same could be said of this Court's case-by-case approach to evaluating international comity concerns raised by requests for production of documents residing abroad. *Marc Rich*, even if correct in outcome, certainly does not follow *Morrison*'s analytical approach. This Court need not decide *Marc Rich*'s continuing validity here.[6] But the substantial question on that point counsels strongly against extending the *Marc Rich* cases any further—and certainly not to authorize the execution of a law enforcement seizure of a customer's private materials from a foreign country.[7]

---

[6] This panel is bound by *Marc Rich.* We reserve the right, however, to challenge its continued validity in further proceedings.

[7] One reason for the district court's erroneous conclusion may be that it decided not to consider the difference between Microsoft's own business records and its customers' private correspondence. The district court incorrectly stated that Microsoft waived this argument. *See* SA 30. The district court "confess[ed]" that it "didn't go back and read your briefs" before the magistrate judge. A 296. Those briefs reveal that Microsoft's entire argument before the magistrate judge was that Microsoft could not be compelled to execute a warrant to conduct a "search and seizure *of customer information* located outside the United States." A 34. When the Government invoked the subpoena analogy based on *Marc Rich*, Microsoft explained that warrants—unlike subpoenas—allow the Government to "trespass upon private property" like "data" belonging to a "customer or subscriber" of an email service, and that the *Marc Rich* line of cases did not apply. A 63-64; *see* A 65 (discussing differences between subpoenas and warrants with respect to the notice that must be given to the "customer or subscriber whose data is sought"). Microsoft also argued that the Sixth Circuit in *Warshak* had held, and the Government had accepted, that a warrant is required to "access … the contents of a person's private electronic communications." A 64-65. That was more than enough to preserve the argument.

III. THE DISTRICT COURT IMPROPERLY RELIED ON POLICY CONCERNS THAT MAY BE ADDRESSED ONLY TO CONGRESS.

The district court bookended its opinion with policy considerations, all directed at hypothesizing what Congress would have done had it in 1986 foreseen the global internet. The court began its opinion with a paean to legislative reform:

> "The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign."

SA 1 (citation omitted). And it ended with the prime policy consideration it thought should drive the renovation efforts: Law enforcement would be impeded "[i]f the territorial restrictions on conventional warrants applied to warrants issued under section 2703(a)." SA 18. This whole policy analysis flouts the presumption against extraterritoriality. § III.A. In any event, the court's policy analysis was flawed. § III.B.

A. Congress Alone Decides When U.S. Law Should Apply Abroad.

The district court seems to have forgotten that its role was not to "improve upon the statutory scheme that Congress enacted into law." *Touche Ross & Co. v. Redington*, 442 U.S. 560, 578 (1979). Particularly in the context of extraterritoriality, the court was not supposed to adapt the statute to the "rise of [a new] medium" or contemplate whether the statute Congress wrote "satisfactorily" addresses "entirely new phenomena" or offers sufficiently "clear legal rules." And

it certainly was not supposed to flip the presumption *against* extraterritoriality in favor of a vision of a sovereign that is not "territorially based."

In applying the presumption against extraterritoriality, the Supreme Court and this Court have been emphatic that it is impermissible to try to "'discern' whether Congress would have wanted the statute to apply" abroad had it considered the matter. *Morrison*, 561 U.S. at 255. Any "effort to cobble together indirect, circumstantial suggestions of extraterritorial application faces powerful headwinds." *Liu Meng-Lin*, 763 F.3d at 180; *see Morrison*, 561 U.S. at 257-58 (rejecting tests designed to "point[] the way to what Congress would have wished"). Congress "alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord are so evident and retaliative action so certain." *Benz*, 353 U.S. at 147. Only Congress can fashion a balanced approach to when and how legislation will apply abroad.

Experience confirms that policy considerations get resolved when courts stick to their assigned roles and let Congress attend to policy. For example, rather than decide whether Congress would have wanted Title VII of the Civil Rights Act to apply abroad, the Court limited it to the United States and noted that "should [Congress] wish to do so, [it] may … amend Title VII and in doing so will be able to calibrate its provisions in a way that we cannot." *Aramco*, 499 U.S. at 259. Congress promptly amended the statute to apply extraterritorially, but limited to

certain U.S. citizen employees of U.S. firms in foreign countries. *See* Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1071, 1077 (1991). The presumption against extraterritoriality thus "provoked Congress into providing just the sort of nuanced specificity and limitations that the Court would have had difficulty divining." Einer Elhauge, *Statutory Default Rules: How to Interpret Unclear Legislation* 206 (2008). So, too, here. If this new phenomenon of globalized communications presents some challenges, it is for Congress to decide how to balance international comity interests and law enforcement needs. Congress might seek to authorize the extraterritorial application of § 2703(a) only for investigations of certain crimes and national security matters. It might extend § 2703(a) to reach emails overseas, but only those belonging to U.S. citizens and permanent residents. Indeed, pending Senate bills would do just that. *See* Law Enforcement Access to Data Stored Abroad Act, S. 2871, 113th Cong. §§ 2(4), (3)(a)(2), (3)(a)(5) (2014). Congress might even grant the Government the power it now claims. But it was improper for the district court to try to "'discern' whether Congress *would have wanted* the statute to apply" abroad had it foreseen that global electronic communications would "throw[] the law into disarray." *Morrison*, 561 U.S. at 255.

B. The District Court's Policy Analysis Was Flawed.

Even if the district court were empowered to decide what policy Congress would have favored, its analysis was flawed. In deciding to extend § 2703 abroad, the district court cited "the practical consequences that would follow" from failing to do so. SA 18. It speculated that law enforcement officers would be unable to collect evidence, citing one law review article for the proposition that the MLAT process "generally remains slow and laborious," and opining that "nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance." SA 19. This analysis is both wrong and incomplete.

Law enforcement agents have been using MLATs and informal processes for decades to pursue all manner of evidence strewn all across the globe. If the Government needs to obtain any private papers from Ireland—mail in an envelope, documents in a safe deposit box, and the like—it relies on the MLAT or other bilateral arrangements to do so. When an international crime syndicate leaves such evidence behind in multiple countries, as they often do, agents engage with multiple governments. There is no reason why digital letters should be treated differently from physical letters or why Ireland's sovereign interests are diminished when letters are not written in ink.

Any complaints the Government has about the MLAT process should be addressed by reforming the MLAT process, rather than distorting § 2703(a)'s text.

But the evidence refutes the district court's concerns. Ireland has implemented its MLAT obligations with "highly effective" legislation that is "efficient and well-functioning." A 116. The MLATs create well-defined procedures to obtain the precise type of private emails at issue here. In fact, some of the processes are superior to the ones in place for physical evidence. To the extent the Government needs such evidence urgently, there are procedures for expedited requests, including communicating and responding to requests by fax or email. *Agreement on Mutual Assistance Between the European Union and the United States of America*, art. 7, June 25, 2003, T.I.A.S. 10-201.1. "[U]rgent requests can be processed in a matter of days," A 262-63. To prevent the destruction of evidence, law enforcement may call a hotline on a "24/7" "around-the-clock" basis," to ensure the immediate preservation of data. A 259-60. "Ireland generally processes requests for freezing cooperation orders within 24 hours from when they are made." A 263. And, as Michael McDowell, former Minister of Justice and Attorney General of Ireland, testified, "[r]efusal by Ireland to execute a proper request duly made for assistance from U.S. authorities is very uncommon." A 115. The Government introduced no evidence to support the district court's suggestion that the MLAT process is slow or inefficient or interferes with the Government's ability to investigate or prosecute crimes.

Moreover, that the court's decision "will have an impact on the ability of law enforcement to combat crime," does not end the inquiry. *Riley*, 134 S. Ct. at 2493. The district court failed to account for the countervailing policy concerns. Nations retain discretion to decline a request for assistance precisely because they retain sovereignty over information located within their territory. Ireland, which has some of the strongest data privacy laws in the world, may have valid reasons for restricting access to private emails located in Irish datacenters, just as the United States would have valid reasons for restricting a foreign government's access to private emails located on U.S. soil. The district court's ruling will encourage foreign governments to sidestep their own MLAT commitments and unilaterally seek data stored in the United States from providers that operate in their jurisdictions. Indeed, Brazil has recently enacted legislation expressly imposing its privacy rules on all internet companies with at least one Brazilian user. *See* A 125-28. As foreign countries increasingly assert unilateral jurisdiction over data stored in the United States, the primary objective of ECPA—protecting U.S. citizens' most private electronic information—will be thwarted.

The Government's unilateral exercise of law enforcement powers in Ireland also puts at risk the U.S. information technology sector's continued ability to operate and compete globally. Foreign leaders have expressed concern about the district court's expansive interpretation of ECPA, and noted that compliance with

extraterritorial U.S. search warrants may cause providers to be "caught in the middle" of a "conflict" between U.S. criminal law and the data protection laws of the countries where the targeted data is stored. A 151; *see* A 140 (noting that "[i]f U.S. authorities circumvent the Mutual Legal Assistance agreement and access data directly (through companies) for criminal investigations, they expose companies operating on both sides of the Atlantic to significant legal risks").

Microsoft has also encountered rising concerns among both current and potential customers overseas about the Government's extraterritorial access to their information. A 110-11. In some instances, potential customers—specifically referencing the decision below—have decided not to purchase services from Microsoft and have opted instead for a provider based outside the United States. A 111. The opinion below threatens to undermine the U.S. technology sector's competitive edge. A 112.

If it was proper for the court to engage in "judicial lawmaking" by considering the burden on law enforcement efforts, it should have considered these countervailing concerns as well. *Cf. Morrison*, 561 U.S. at 261 n.5. The court's heedlessness underscores why there is a presumption against extraterritoriality in the first place. Only Congress has the institutional competence and constitutional authority to balance law enforcement needs against our nation's sovereignty, the privacy of its citizens, and the competitiveness of its industry.

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

December 8, 2014

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B)(i) because this brief contains 13,938 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

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system on December 8, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

ORRICK, HERRINGTON & SUTCLIFFE LLP

s/ E. Joshua Rosenkranz

E. Joshua Rosenkranz
Counsel for Appellant