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 OF *AMICI CURIAE* AMAZON.COM, INC. AND ACCENTURE PLC IN SUPPORT OF APPELLANT

PETER KARANJIA
ERIC J. FEDER
DAVIS WRIGHT TREMAINE LLP
1633 Broadway, 27th Floor
New York, New York 10019
(212) 489-8230

Attorneys for Amici Curiae Amazon.com, Inc. and Accenture plc

CORPORATE DISCLOSURE STATEMENT

Pursuant to FRAP 26.1 and 29(c)(1), undersigned counsel for *amici curiae* provide the following disclosures of corporate identity:

Amicus curiae Amazon.com, Inc. is a publicly held corporation, has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

Amicus curiae Accenture plc is a publicly held corporation, has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

Respectfully submitted,

DAVIS WRIGHT TREMAINE LLP

By: /s/ Peter Karanjia
Peter Karanjia
Counsel for *Amici Curiae*

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES iv

INTEREST OF *AMICI* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. ECPA WARRANTS CANNOT REQUIRE A CLOUD SERVICES PROVIDER TO TURN OVER ITS CUSTOMER'S PERSONAL ELECTRONIC DOCUMENTS LOCATED ABROAD 4

A. The Text, Structure, and Legislative History of ECPA All Show That ECPA Warrants Have No Extraterritorial Effect 4

1. Section 2703 Distinguishes Between *Warrants*, Which May Be Used to Obtain More Sensitive Information Upon a Showing of Probable Cause, and *Subpoenas* 5

2. Section 2703(a)'s Reference to the Federal Rules of Criminal Procedure Incorporates Rule 41 8

3. Rule 41 Expressly Provides For Extraterritorial Effect Only in Limited Situations Inapplicable Here 9

4. The Legislative History Confirms That Congress Did Not Intend to Give Extraterritorial Effect to ECPA Warrants 11

B. The Presumption Against Extraterritorial Application Confirms That ECPA Warrants Cannot Compel a Cloud Services Provider To Turn Over its Customer's Documents Located Abroad 12

1. Because a "Search" and "Seizure" Would Occur Abroad, The District Court's Hybrid ECPA Warrant Would Be Impermissibly Extraterritorial 12

2. Even if There Were No "Search" or "Seizure" Abroad, The Warrant Would Be Impermissibly Extraterritorial 14

3. The Decision Below Will Place Cloud Services Providers In The Untenable Position of Violating Foreign Privacy Laws In Order To Comply With ECPA Warrants.....17

II. BECAUSE THIS CASE INVOLVES A WARRANT RATHER THAN A SUBPOENA FOR A COMPANY'S BUSINESS RECORDS, THE *BANK OF NOVA SCOTIA* CASES HAVE NO BEARING HERE.....18

CONCLUSION.....21

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Boyd v. United States,
116 U.S. 616 (1886).....19, 20, 21

Dean v. United States,
556 U.S. 568 (2009).....11

EEOC v. *Arabian American Oil Co.*,
499 U.S. 244 (1991).....14, 15, 16

Florida v. Jardines,
133 S. Ct. 1409 (2013).....20

Frazier v. Pioneer Americas LLC,
455 F.3d 542 (5th Cir. 2006) 8

Hale v. Henkel,
201 U.S. 43 (1906).....20

In re Grand Jury Proceedings (Bank of Nova Scotia),
740 F.2d 817 (11th Cir. 1984) 4, 19, 21

In re Marc Rich & Co., A.G.,
707 F.2d 663 (2d Cir. 1983) 19

In re Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,
13 F. Supp. 3d 145 (D.D.C. 2014), *vacated on other grounds*,
13 F. Supp. 3d 157 (D.D.C. 2014).....13

In re Terrorist Bombings of U.S. Embassies in E. Africa,
552 F.3d 157 (2d Cir. 2008) 10

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013).....18

McKeel v. Islamic Republic of Iran,
722 F.2d 582 (9th Cir. 1983) 10, 11

Morrison v. Nat'l Australia Bank Ltd.,
561 U.S. 247 (2010).....3, 11, 14, 15, 17

Riley v. California,
134 S. Ct. 2473 (2014).....1, 20, 21

United States v. Bach,
310 F.3d 1063 (8th Cir. 2002) 7

United States v. DiTomasso,
2014 WL 5462467 (S.D.N.Y. Oct. 28, 2014).....13

United States v. Gatlin,
216 F.3d 207 (2d Cir. 2000) 10

United States v. Jones,
132 S. Ct. 945 (2012).....20

United States v. Miller,
425 U.S. 436 (1976).....21

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 7, 13

Zheng v. Yahoo! Inc.,
No. C-08-1068 MMC, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009) 11

International Cases

Entick v. Carrington,
95 Eng. Rep. 807 (C.P. 1765).....19, 20

Federal Statutes

18 U.S.C. § 7(9) 10

18 U.S.C. §§ 2510-2522 ("Electronic Communications Privacy Act") .....*passim*

18 U.S.C. § 2510(17) 6

18 U.S.C. §§ 2701-2712 ("Stored Communications Act") 5

18 U.S.C. § 2703.....*passim*

18 U.S.C. § 2705 7

18 U.S.C. § 2711(3) 10

28 U.S.C. § 1783 14

Pub. L. No. 99-508, 100 Stat. 1848 (1986) 5

Pub. L. No. 102-166, 105 Stat. 1071 (1991) 16

Constitutional Provisions

U.S. Const. amend. IV 7, 13, 15

Legislative Materials

147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) 10

H.R. Rep. No. 99-647 (1986) 12

S. Rep. No. 99-541 (1986) 5

S. Rep. No. 99-541 (1986) 12

Rules

Fed. R. Crim. P. 41 ..... *passim*

FRAP 29(c)(5) 1

Other Authorities

Directive 95/46/EC of the European Parliament and Council of 25 October 1995 (O.J. L281/38), Arts. 7 and 25 18

INTEREST OF *AMICI*[1]

Amici are two of America's leading technology and cloud computing service companies. Cloud computing allows individuals, businesses, organizations, and governments to store and access their documents securely on remote servers via the Internet. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014). *Amici* have made substantial investments in expanding their infrastructure and providing their technology services across the globe in order to provide their customers with faster, more efficient, and better-value services.

Amici are committed to complying with lawful government requests for information. At the same time, they highly value, and work diligently to protect, the privacy and confidentiality of their customers' information. *Amici* therefore have a strong interest in ensuring that the provisions of the Electronic Communications Privacy Act at issue in this case are properly interpreted to protect their customers' legitimate privacy interests and enable innovative cloud technologies to continue to thrive.

---

[1] Pursuant to FRAP 29(c)(5), *amici* state that no counsel for a party authored this brief in whole or in part, and no person or entity other than *amici* and their counsel made a monetary contribution to the preparation or submission of this brief. All parties to this case have consented to the filing of this brief.

SUMMARY OF ARGUMENT

The court below fundamentally misinterpreted the Electronic Communications Privacy Act to conclude that it creates a "hybrid . . . part search warrant and part subpoena" that can compel a cloud services provider to produce its customers' private communications stored anywhere in the world. That interpretation runs counter to ECPA's text, its legislative history, and the strong presumption against extraterritorial application of U.S. statutes.

ECPA draws a bright-line distinction between "warrants" and "subpoenas." Where the government seeks highly sensitive documents belonging to the customer of a cloud services provider, it must obtain a *warrant* supported by probable cause. 18 U.S.C. § 2703(a); Fed. R. Crim. P. 41(d)(1). Further, the warrant must be obtained "using the procedures described in the Federal Rules of Criminal Procedure." *Id.* Those procedures are specifically set forth in Federal Rule of Criminal Procedure 41 which, except in limited situations inapplicable here, indisputably has no application outside the United States. The import of Congress' express incorporation of the Rule in ECPA is unmistakable: Section 2703(a)'s authorization of ECPA warrants has only domestic effect and cannot compel the retrieval and collection of documents entrusted to third-party cloud services providers that are stored abroad.

In contrast to the novel and textually unsupported "hybrid" warrant-subpoena the district court created to reach across foreign borders, ECPA's statutory text and legislative history leave no doubt that Section 2703(a) creates a warrant that applies only *domestically*. That inescapable conclusion is underscored by the longstanding presumption against the extraterritorial application of U.S. law. That presumption prevents the necessary and intended effect of the warrant here: a "search" and a "seizure" abroad. Indeed, even absent an extraterritorial search or seizure, the warrant would trigger the presumption against extraterritorial application because it purports to compel conduct abroad—the retrieval and collection of documents stored in Ireland.

The impact of the decision below on foreign sovereign interests underscores the full force of the presumption here. If allowed to stand, the district court's decision would place cloud services providers in the untenable position of either disobeying ECPA warrants in order to comply with foreign privacy laws or violating those laws in order to comply with the warrant. "The probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures.'" *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 269 (2010) (citation omitted). When it enacted Section 2703(a), however, Congress did not do so at all, much less provide the "*clear*

indication" of an intended extraterritorial application essential to rebut the presumption. *Id.* at 255 (emphasis added).

Finally, the district court was wrong to rely on the *Bank of Nova Scotia* line of precedent. Those cases involve subpoenas for a company's *own business records*. The ECPA warrant in this case does not seek Microsoft's own records, but rather the *private correspondence* of a Microsoft customer. The cases involving subpoenas for business records are far afield and cannot justify giving ECPA warrants extraterritorial effect where the statute permits none.

ARGUMENT

I. ECPA WARRANTS CANNOT REQUIRE A CLOUD SERVICES PROVIDER TO TURN OVER ITS CUSTOMER'S PERSONAL ELECTRONIC DOCUMENTS LOCATED ABROAD

A. The Text, Structure, and Legislative History of ECPA All Show That ECPA Warrants Have No Extraterritorial Effect

ECPA requires that the government obtain a warrant to order production of the highly sensitive electronic documents of a cloud services provider's customer. 18 U.S.C. § 2703(a). The warrant must be obtained "using the procedures described in the Federal Rules of Criminal Procedure." *Id.* Except in limited situations inapplicable here, those procedures, set forth in Federal Rule of Criminal Procedure 41, authorize only *domestic* warrants. By specifically incorporating those procedures in ECPA, and by not addressing the legal conflicts

that would necessarily arise from foreign application of ECPA warrants, Congress made clear that ECPA warrants do not have extraterritorial effect.

1. Section 2703 Distinguishes Between *Warrants*, Which May Be Used to Obtain More Sensitive Information Upon a Showing of Probable Cause, and *Subpoenas*

Congress enacted ECPA in 1986, before the Internet as we currently know it existed. Even at that time, Congress was aware that, in order to keep pace with evolving technology, new protections were needed to safeguard personal privacy interests in data stored on and transmitted via electronic networks. *See, e.g.*, S. Rep. No. 99-541, at 5 (1986). Congress enacted Section 2703 in Title II of ECPA specifically in an effort to balance those privacy interests against the needs of law enforcement. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986).[2] Title II establishes three mechanisms for government access to different categories of electronic communications: a warrant, a subpoena, and a court order. *See* 18 U.S.C. § 2703(a), (b), (d).

In Section 2703(a), the warrant provision, Congress authorized the government to require providers of electronic communications services to turn over "the contents of" their customers' unopened emails "*only pursuant to a* ***warrant*** *issued using the procedures described in the Federal Rules of Criminal*

[2] Title II of ECPA was enacted as the Stored Communications Act, 18 U.S.C. §§ 2701-2712. The district court's references to the Stored Communications Act ("SCA") thus refer to the same statute—ECPA.

Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a) (emphasis added).[3] That provision governs the warrant here, which seeks the unopened emails of a subscriber to Microsoft's "web-based" email service. A web-based email service, like Microsoft's Outlook.com or Google's Gmail.com, stores subscriber emails (and any embedded documents) "in the cloud"—*i.e.*, remotely on the service provider's servers. As in this case, those servers may be located abroad, a design feature that helps deliver content as quickly and efficiently as possible to customers in their local jurisdiction.

The import of Congress' use of the term "warrant" in Section 2703(a) is unmistakable. In other parts of Section 2703, Congress used the term "subpoena," and authorized the government to use subpoenas to obtain basic subscriber and transactional information such as the customer's name, phone number, and payment method. *See* 18 U.S.C. § 2703(c)(1) and (2) (permitting use

[3] Section 2703(a) applies to only *unopened emails* held in electronic storage for 180 days or less. *See* 18 U.S.C. § 2703(a) (referencing electronic or wire communications "in electronic storage in an electronic communications system for one hundred eighty days or less"); *id.* § 2510(17) (defining "electronic storage" as "any temporary intermediate storage" incidental to transmission of emails and any storage for "backup protection"); *see also* Special Appendix ("SA__") at 6 n.2 (magistrate judge's opinion, affirmed by district court).

of "an administrative subpoena" or "grand jury or trial subpoena").[4] And, as other courts have made clear, "[w]hile warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and . . . intended them to be treated as warrants." *United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002).

The difference between warrants and subpoenas—in the context of ECPA and beyond—is substantial. Under ECPA, subpoenas are used to obtain inherently less sensitive private customer information, and expressly cannot be used to obtain the contents of unopened emails. And, while all warrants require a showing of probable cause, *see* 18 U.S.C. § 2703(a); Fed. R. Crim. P. 41(d)(1), no such requirement applies to a subpoena.[5] Because a warrant may reach into the

---

[4] Congress also authorized the government to use an administrative subpoena (instead of a warrant or court order) to obtain *older* emails, which Congress deemed less sensitive than unopened emails. *See* 18 U.S.C. § 2703(a), (b)(1)(B)(i) (addressing emails and other electronic or wire communications "in electronic storage" for *more than* 180 days). Though the statute itself does not require a warrant for the older emails, courts have held that the Fourth Amendment does. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (government violated Fourth Amendment by compelling Internet Service Provider to turn over customer's email without first obtaining a warrant based on probable cause). Thus, while a warrant backed by probable cause is not *statutorily* required for emails stored for more than 180 days, it is *constitutionally* required.

[5] Instead, customers whose records may be obtained by subpoena generally must be afforded the opportunity to challenge the subpoena before their records are turned over. *See* 18 U.S.C. § 2703(b)(1)(B)(i) (requiring advance notification of customer); *see also id.* § 2705(1)(B) & (2) (permitting delay of advance notification only in limited circumstances, such as where the government can show that "life or physical safety" will be "endanger[ed]").

most sensitive data, it makes sense that it is subject to more stringent restrictions, including both the familiar probable-cause requirement and, as explained below, restrictions on its geographic scope.

2. Section 2703(a)'s Reference to the Federal Rules of Criminal Procedure Incorporates Rule 41

Section 2703(a) specifies that a warrant must be obtained "using *the procedures described in the Federal Rules of Criminal Procedure* . . . by a court of competent jurisdiction." 18 U.S.C. § 2703(a) (emphasis added). That language specifically contemplates Federal Rule of Criminal Procedure 41—the rule, entitled "Search and Seizure," that governs search warrants. *See* Fed. R. Crim. P. 41. In particular, Congress' use of the definite article in Section 2703(a) followed by the reference to the plural "procedures" shows that Congress meant to incorporate *all* the procedures in the Federal Rules of Criminal Procedure that apply to warrants—plainly including Rule 41—unless expressly stated otherwise. *See, e.g.*, *Frazier v. Pioneer Americas LLC*, 455 F.3d 542, 546 (5th Cir. 2006) (interpreting statute providing that "any class action in which . . . *the primary defendants* are," *inter alia*, "States," court reasoned that "[t]he plain text of [the statute], using the definite article before the plural nouns, requires that all primary defendants be states. Had Congress desired the opposite, it would have used 'a' and the singular, or no article") (emphasis added).

A separate express carve-out in Section 2703(a) reinforces this reading. Rule 41 generally requires that a warrant be executed in the presence of a law enforcement officer, *see* Fed. R. Crim. P. 41(f), but Section 2703(g) specifies that "the presence of an officer shall not be required for service or execution of a search warrant" under Section 2703. 18 U.S.C. § 2703(g). Because all of the requirements of Rule 41 are otherwise incorporated by reference into Section 2703(a), that carve-out is essential.

3. Rule 41 Expressly Provides For Extraterritorial Effect Only in Limited Situations Inapplicable Here

Rule 41 authorizes *only domestic* warrants, and provides for extra-territorial application only in exceptional situations inapplicable here (involving U.S. diplomatic properties located abroad).

That domestic focus is evident in various parts of Rule 41. For example, the rule empowers "a magistrate judge with authority in the district . . . to issue a warrant to search for and seize a person or property located *within the district*." Fed. R. Crim. P. 41(b)(1) (emphasis added). The Rule also authorizes magistrate judges to issue warrants for searches and seizures "outside the district," *see* Rule 41(b)(2)-(4), but those provisions address out-of-district searches and seizures that nonetheless occur *within the United States*.[6] By contrast, in the

[6] An extraterritorial warrant issued by a U.S. court under Rule 41 "would be a nullity." *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157,

narrow circumstances in which the Rule permits extraterritorial warrants, it says so *explicitly*, as it must to overcome the strong presumption against extraterritorial application of U.S. law. *See* Fed. R. Crim. P. 41(b)(5) (authorizing "warrant for property outside the jurisdiction of any state or district, but within," *inter alia*, "(B) "the premises . . . of a United States diplomatic or consular mission in a foreign state," and "(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.").[7]

Where Congress "includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."

---

171 (2d Cir. 2008) (footnote omitted); *see also* SA18 (acknowledging "limitations on the territorial reach of a warrant issued under" Rule 41).

In addition, Section 2703(a) authorizes any "court of competent jurisdiction" to issue an ECPA warrant, 18 U.S.C. § 2703(a), but this language authorizes only out-of-district—but still *domestic*—warrants. *See* 147 Cong. Rec. H7197-98 (daily ed. Oct. 23, 2001) ("court of competent jurisdiction" language "[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*") (emphasis added).

[7] While U.S. diplomatic properties in foreign countries may be subject to the "'special' . . . territorial jurisdiction of the United States" for purposes of holding U.S. nationals liable for certain criminal offenses committed on those properties, *see, e.g.*, 18 U.S.C. § 7(9); *McKeel v. Islamic Republic of Iran*, 722 F.2d 582, 588 (9th Cir. 1983), U.S. diplomatic or consular missions in foreign states "do[] not constitute territory of the United States." *United States v. Gatlin*, 216 F.3d 207, 214 n.9 (2d Cir. 2000) (quoting *McKeel*, 722 F.2d at 588), *abrogated in part on other grounds*, *Morrison*, 561 U.S. 247.

Dean v. United States, 556 U.S. 568, 573 (2009) (citation omitted). Here, Congress not only did not include any language in Section 2703(a) indicating any intent to give ECPA warrants extraterritorial effect, but also cross-referenced a Rule of Criminal Procedure that *precludes* extraterritorial reach except in the rarest of circumstances. Absent such circumstances here, Congress plainly did not intend for ECPA warrants to apply abroad. *See Morrison*, 561 U.S. at 265 (statute's "explicit provision for a specific extraterritorial application would be quite superfluous if the rest of the . . . Act already applied to transactions on foreign exchanges.").

4. The Legislative History Confirms That Congress Did Not Intend to Give Extraterritorial Effect to ECPA Warrants

The legislative history confirms that, in enacting Section 2703(a), Congress authorized purely *domestic* application. As other courts have observed, ECPA scarcely "reference[d] in any manner activities occurring outside the United States," and its legislative history "clearly expresses Congress' intent that the ECPA not apply to interceptions outside the United States." *Zheng v. Yahoo! Inc.*, No. C-08-1068 MMC, 2009 WL 4430297, at *3 (N.D. Cal. Dec. 2, 2009). In discussing provisions addressing interceptions, for example, a House report specifically noted that "the Committee does not intend that the Act regulate activities conducted outside the territorial United States." H.R. Rep. No. 99-647, at 32-33 (1986).

Elsewhere in the legislative history, Congress expressly discussed extraterritorial application.[8] But even as it did so in conjunction with other ECPA provisions, nowhere in the statutory text or legislative history did Congress suggest that ECPA warrants should have extra-territorial application. Congress' determination not to provide for extraterritorial effect in Section 2703(a), while specifically incorporating Rule 41, makes clear its intent that ECPA warrants have no such effect.

B. The Presumption Against Extraterritorial Application Confirms That ECPA Warrants Cannot Compel a Cloud Services Provider To Turn Over its Customer's Documents Located Abroad

The presumption against the extraterritorial application of U.S. statutes confirms the plain import of ECPA's statutory text and legislative history.

1. Because a "Search" and "Seizure" Would Occur Abroad, The District Court's Hybrid ECPA Warrant Would Be Impermissibly Extraterritorial

Both a "search" and a "seizure" occur where, as here, the government enlists a private actor to access another person's private electronic documents for collection. *See Warshak*, 631 F.3d at 286 ("[I]f government agents compel an ISP

[8] *See, e.g.*, S. Rep. No. 99-541, at 30 (1986) (discussing mobile interception devices, and stating that "a court can authorize an order within its jurisdiction but within the United States . . . . Nothing in this subsection affects the current law with regard to the use of such devices outside the United States."); *id.* at 33-34 (explaining that a warrant to install a mobile tracking device "remains valid even if the device is moved outside the jurisdiction of the court, even outside the jurisdiction of the United States, provided that the device was installed within the jurisdiction of the court").

to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search."); *In re Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 150 (D.D.C. 2014) ("[A]ny e-mails that are turned over to the government are unquestionably 'seized' within the meaning of the Fourth Amendment.") (citing cases), *vacated on other grounds*, 13 F. Supp. 3d 157 (D.D.C. 2014); *see also United States v. DiTomasso*, 2014 WL 5462467 (S.D.N.Y. Oct. 28, 2014) (users have reasonable expectation of privacy in contents of email communications). On its face, the ECPA warrant in this case ordered a "search and seizure" of the Microsoft customer's personal emails. A44. Those events, of course, would occur in Ireland—the location of the materials to be searched and seized.

The compelled search and seizure in Ireland necessarily trigger the longstanding presumption against the extraterritorial application of U.S. statutes. As the Supreme Court has directed, "[w]hen a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255; *see also id.* ("'[U]nless there is the affirmative intention of the Congress *clearly expressed*' to give a statute extraterritorial effect, 'we must presume it is primarily concerned with domestic conditions.'") (quoting *EEOC* v. *Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) ("*Aramco*")). ECPA's text and legislative history foreclose

any serious argument that Section 2703 "gives [a] *clear* indication" of an intended extraterritorial application. *Id.* (emphasis added).[9] Nor did the government argue otherwise below. *See* Gov't Dist. Ct. Br. at 18-21.

Because the extraterritorial retrieval and collection of documents demanded here necessarily constitute a search and seizure, and because ECPA warrants lack extraterritorial effect, the warrant issued to Microsoft cannot compel the production of emails stored on the company's servers in Dublin.

2. Even if There Were No "Search" or "Seizure" Abroad, The Warrant Would Be Impermissibly Extraterritorial

Although compelled accessing and collection of a subscriber's documents located abroad entail an overseas search and seizure, the Court need not even reach that question in order to find that the presumption against extra-territorial application applies in this case.

Morrison and related cases do not require a question of constitutional dimension to trigger application of the presumption, and no "search" or "seizure" in the Fourth Amendment sense is required for the presumption to apply. Rather, the sole predicates are a U.S. statute and "application" of the statute outside "the

[9] In contrast with *warrants* under Section 2703, Congress expressly contemplated that *subpoenas* may have extraterritorial application. *See*, *e.g.*, 28 U.S.C. § 1783 (authorizing issuance of subpoena requiring, *inter alia*, the "production of a specified document or thing" by "a national or resident of the United States who is in a foreign country"). As discussed below, however, the cases addressing subpoenas are far afield. *See* Point II, *infra*.

territorial jurisdiction of the United States." *Morrison*, 561 U.S. at 255; *see also Aramco*, 499 U.S. at 248. Both are met here: The government is relying on Section 2703(a) to force Microsoft to access and collect subscriber documents stored on a computer server in Ireland. That effort to "apply" or "give . . . effect" to the statute abroad triggers the presumption against extraterritorial application. *See Morrison*, 561 U.S. at 255.

To be clear, it makes no difference if the cloud services provider is a U.S. corporation whose main office is in the United States or that the government intends to review the requested documents in the United States. *See* Gov't Dist. Ct. Br. at 20-21. In *Aramco*, for example, the extraterritoriality presumption applied (and barred a Title VII action) even though the plaintiff was a U.S. citizen bringing a claim against a U.S. corporation involving conduct in Saudi Arabia. *See* 499 U.S. at 246-47.[10]

Nor does it matter that the forced retrieval and collection of documents may be initiated by conduct in the United States (for example, by sending instructions via U.S.-based computers to servers in Ireland). In a case like

[10] Significantly, Congress amended Title VII in the wake of the Supreme Court's decision in *Aramco* to specifically cover U.S. citizens working abroad. *See* Pub. L. No. 102-166, § 109, 105 Stat. 1071 (1991). As a result, the statute now applies extraterritorially only because Congress *expressly* provided for extraterritorial application—something it conspicuously declined to do in ECPA.

this, the entire purpose of that U.S.-based conduct is to facilitate the accessing and collection of private documents stored on a foreign server.[11]

The argument that Microsoft's "own employee in the United States will use proprietary software to access a Microsoft datacenter and retrieve the requested records electronically" (Gov't Dist. Ct. Br. at 15) likewise does not change the analysis. The fact that *some* conduct occurs in the United States does not displace the presumption against extraterritorial application—especially where, as here, the critical conduct occurs abroad. As the Supreme Court explained in *Morrison*, "the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case." *Morrison*, 561 U.S. at 266.

Common sense underscores the point. Consider a situation in which a U.S. investor in Manhattan uses a foreign brokerage account to make an online purchase of securities listed on the London Stock Exchange. She later brings a private action for securities fraud under Section 10(b) of the Securities and Exchange Act of 1934, alleging that the U.K.-based issuer misrepresented the securities. Section 10(b) applies only to "transactions in securities listed on domestic exchanges, and domestic transactions in other securities." *Morrison*, 561

[11] Under those circumstances, the government's contention that the conduct abroad is "incidental" to conduct in the United States is both unsupported and unsupportable. *See* Gov't Dist. Ct. Br. at 19.

U.S. at 267. Under *Morrison*, the presumption against extraterritorial application of Section 10(b) unquestionably would bar the action even though the U.S. investor, ensconced in Manhattan, types in a command that initiates an overseas transaction. So too here.

3. The Decision Below Will Place Cloud Services Providers In The Untenable Position of Violating Foreign Privacy Laws In Order To Comply With ECPA Warrants

The impact on foreign sovereign interests cements application of the presumption against extraterritoriality in this case. As in *Morrison*, "[t]he probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures.'" 561 U.S. at 269 (citation omitted). Foreign privacy laws—especially those in Europe—impose stringent requirements that restrict cloud services providers' ability to retrieve and collect their customers' private documents. *See, e.g.*, Directive 95/46/EC of the European Parliament and Council of 25 October 1995 (O.J. L281/38), Arts. 7 (restricting processing of personal data, including disclosures to third parties) and 25 (restricting transfers of personal data outside the European Economic Area). In those cases, allowing the decision below to stand would leave cloud services providers to confront the Hobson's choice of either (a) disobeying the ECPA warrant in order to comply with the privacy laws of the country where the relevant

documents are located or (b) violating those laws in order to comply with the warrant. "The presumption against extraterritoriality guards against our courts triggering such serious foreign policy consequences, and instead defers such decisions, quite appropriately, to the political branches." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013). Here, of course, Congress gave no indication whatsoever that it intended to enmesh technology companies in such international conflicts.

Moreover, these conflicts are wholly unnecessary. It is undisputed that a well-established cooperative process—under Mutual Legal Assistance Treaties—exists for the government to seek the type of information it claims to need in this case, and does so without placing cloud services providers in that untenable position, forcing conflicts with the laws of other sovereign nations, or distorting the statutory scheme Congress intended to achieve the opposite result. The government was unable to point to any evidence below showing that the MLAT process would be unworkable. *See* Microsoft Br. at 57-58.

II. BECAUSE THIS CASE INVOLVES A WARRANT RATHER THAN A SUBPOENA FOR A COMPANY'S BUSINESS RECORDS, THE *BANK OF NOVA SCOTIA* CASES HAVE NO BEARING HERE

The court below treated the government's request as unremarkable—a routine situation in which the government issues a subpoena calling for documents within a company's custody and control. That is simply not the case.

The *Bank of Nova Scotia* line of cases recognizes that the government may issue a subpoena seeking a company's records located abroad.[12] But there is a fundamental difference between a subpoena for a *company's own business records* and a warrant seeking a *third party's personal documents* entrusted to a service provider for safekeeping. As the Supreme Court ruled long ago, citing historical English precedent that remains remarkably apt here, it is "not the breaking of [a person's] doors, and the rummaging of his drawers, that constitutes the essence of the offense," but rather "the *invasion of* his indefeasible right of personal security, personal liberty, and *private property*." *Boyd v. United States*, 116 U.S. 616, 630 (1886) (emphasis added) (discussing *Entick v. Carrington*, 95 Eng. Rep. 807 (C.P. 1765)).[13] "Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and *compulsory* extortion of a man's . . . *private papers* . . . is within the condemnation of [*Entick*]." *Boyd*, 116

---

[12] *See, e.g.*, SA12-13 (citing, *inter alia*, *In re Marc Rich & Co., A.G.*, 707 F.2d 663 (2d Cir. 1983) (grand jury subpoena seeking foreign corporation's business records located abroad)); *see also* SA30 (citing *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) (same)).

[13] The Supreme Court has relied on *Boyd* in several recent decisions, *see, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014); *Florida v. Jardines*, 133 S. Ct. 1409, 1415 (2013); *United States v. Jones*, 132 S. Ct. 945, 949 (2012), and has described *Entick v. Carrington*—the English case on which *Boyd* heavily relied—as "undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure," *Jones*, 132 S. Ct. at 949 (citation and quotation marks omitted).

U.S. at 630 (emphasis added). Here, as then, "the substance of the offense is the *compulsory production of private papers*." *Hale v. Henkel*, 201 U.S. 43, 76 (1906) (emphasis added).

The compulsory production of private documents the owner has entrusted to a third party for safekeeping is precisely what the government seeks here. With the passage of ECPA, Congress anticipated and squarely addressed this situation as to private papers held by third-party electronic computing and remote storage services. And despite the increasing age of that law, Congress spoke with clarity, distinguishing subpoenas from warrants and, for the compelled production of such private materials, unequivocally requiring a warrant subject to all of the governing procedures in the Federal Rules of Criminal Procedure. Absent any contrary direction from Congress, those Rules preclude extraterritorial application of ECPA warrants.

In *Riley*, the Supreme Court concluded that treating a search of data on a modern smartphone as no different from a search of physical items is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." 134 S. Ct. at 2488. By analogy here, treating an ECPA warrant as no different from a routine subpoena for business records abroad is like saying a ride on horseback is indistinguishable from a mission to Mars. The fundamental difference between subpoenas for a company's own records and ECPA warrants

for a customer's private documents securely stored in the cloud illustrates just how far removed the *Bank of Nova Scotia* cases are from this case. *Cf. United States v. Miller*, 425 U.S. 436, 440 (1976) ("On their face, the documents subpoenaed here are not [the account holder's] 'private papers.' Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are *the business records of the banks*.") (emphasis added). The district court seriously erred in conflating the two.

CONCLUSION

For the reasons stated above, the Court should reverse the judgment below.

Dated: December 15, 2014

Respectfully submitted,

DAVIS WRIGHT TREMAINE LLP

By: /s/ Peter Karanjia

Peter Karanjia
Eric Feder
1633 Broadway
New York, NY 10019
Tel: (212) 489-8230
Fax: (212) 489-8340

Attorneys for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 4,994 words, excluding exempted parts, as determined by the word-counting feature of Microsoft Word.

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 it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

Dated: December 15, 2014

By: s/ Peter Karanjia
Peter Karanjia
Attorney for Amici Curiae

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 15, 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.

By: s/ Eric J. Feder
Eric J. Feder
Attorney for Amici Curiae