No. 17-2

In The
# Supreme Court of the United States

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

UNITED STATES OF AMERICA,
*Petitioner,*

v.

MICROSOFT CORPORATION,
*Respondent.*

**On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Second Circuit**

## BRIEF FOR THE STATES OF VERMONT, ALABAMA, ARIZONA, ARKANSAS, CONNECTICUT, DELAWARE, HAWAII, IDAHO, ILLINOIS, INDIANA, IOWA, KANSAS, KENTUCKY, LOUISIANA, MAINE, MARYLAND, MASSACHUSETTS, MICHIGAN, MONTANA, NEBRASKA, NEW HAMPSHIRE, NEW MEXICO, NEW YORK, NORTH CAROLINA, OHIO, OREGON, PENNSYLVANIA, SOUTH CAROLINA, SOUTH DAKOTA, TEXAS, UTAH, VIRGINIA, WYOMING AND THE COMMONWEALTH OF PUERTO RICO AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

THOMAS J. DONOVAN
Attorney General of
the State of Vermont
BENJAMIN D. BATTLES*
Solicitor General
JOHN R. TREADWELL
EVAN P. MEENAN
Assistant Attorneys General
109 State Street
Montpelier, VT 05609
(802) 828-5500
benjamin.battles@vermont.gov
**Counsel of Record*

[Additional Counsel Listed On Signature Page]

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

## QUESTION PRESENTED

Whether a United States provider of email services must comply with a probable-cause based warrant issued under 18 U.S.C. § 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

Page

## INTEREST OF THE *AMICI* STATES[1]

This case presents an important legal question that is central to the ability of federal, state, and local law enforcement agencies to investigate and prosecute crime in the digital age.

The *amici* States investigate and prosecute a wide range of criminal conduct, from drug trafficking and burglary to murder and child sexual exploitation. Email and other electronic communication services provided by companies like Microsoft, Google, Yahoo!, Facebook, and Twitter are ubiquitous in today's world. Indeed, the Court recently described these platforms as "integral to the fabric of our modern society and culture." *Packingham v. N. Carolina*, 137 S. Ct. 1730, 1738 (2017). Not surprisingly, these services are sometimes used to plan, perpetrate, and discuss criminal activity. The companies that provide these services control their customers' data and thus often possess evidence that state and local law enforcement agencies need to investigate and prosecute crimes in their jurisdictions.

For their own commercial reasons, many providers choose to store data on foreign servers – even when the provider and the customer who generated the data are both in the United States. In some cases, data generated by a single communication may be fragmented

[1] *Amici* States submit this brief pursuant to Supreme Court Rule 37.4. Counsel of record for all parties received timely notice of *amici* States' intent to file this brief.

and continuously moved from country to country to facilitate the needs of the provider's network. Google, for example, divides data from a single customer file into component "chunks," which are then copied and moved between a worldwide network of data centers.[2] *In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google*, 2017 WL 471564, at *3 (E.D. Pa. Feb. 3, 2017). This can pose a significant obstacle for a criminal investigation. As one court recently observed, in a network like Google's, it can be difficult to pinpoint the location of relevant data at any given time; it is even "possible that the network will change the location of data between the time when the legal process is sought and when it is served." *Id.*

In this case, on the application of the United States, a federal district court issued a warrant under 18 U.S.C. § 2703, a provision of the Stored Communications Act,[3] directing Microsoft Corporation to produce the contents of a customer's email account. The court found probable cause to believe the account was being used in furtherance of narcotics trafficking activities in the United States. In the decision below, the Second Circuit quashed the warrant with respect to information Microsoft had chosen to store on a server

[2] Google Data Centers: Data and Security, http://www.google.com/about/datacenters/inside/data-security/index.html (last visited July 21, 2017). Google's network includes data centers in Belgium, Chile, Finland, Ireland, the Netherlands, Singapore, and Taiwan. Google Data Centers: Locations, http://www.google.com/about/datacenters/inside/locations/index.html (last visited July 21, 2017).

[3] 18 U.S.C. §§ 2701-2711.

in Ireland. According to the panel, it would be an impermissible extraterritorial application of the Stored Communications Act to require Microsoft to collect and produce information from a foreign server. The court reached this conclusion even though Microsoft could easily access the stored information from its United States offices. This means, as Judge Lynch described in a concurring opinion, that Microsoft, and for that matter any other provider, "can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing – in its own discretion – to store them on a server in another country." App. 52a.

In recent months, in state and federal courts around the country, providers have relied on the decision below to refuse to comply with search warrants issued under the Stored Communications Act and its state law counterparts. Such refusals have been made even when (i) a court has found probable cause that the email account was used in connection with a domestic crime, (ii) the provider can access the requested data from within the United States, and (iii) the suspect and the provider are both in the United States. As discussed below, these refusals have had and will continue to have very real and detrimental impacts on the *amici* States' ability to investigate crimes in their jurisdictions and to protect the safety of their residents.

## SUMMARY OF THE ARGUMENT

This Court should grant the petition for a writ of certiorari. The decision below threatens public safety by interfering with the ability of the federal government, the *amici* States, and local law enforcement agencies to investigate and prosecute serious crimes. This Court's review is necessary to address the Second Circuit's remarkable conclusion that a private company has unfettered discretion to shield evidence of crime from law enforcement, simply by electronically sending that evidence out of the jurisdiction. That conclusion is not compelled by this Court's precedents discussing the extraterritorial application of federal statutes, nor can it be squared with a corporation's obligation to produce relevant documents within its control in response to legal process.



## ARGUMENT

### I. The Second Circuit decision is interfering with the ability of state and local law enforcement agencies to investigate and prosecute crime in their jurisdictions.

This case warrants review now. Although the decision below technically binds only federal courts in the Second Circuit, it is impacting law enforcement agencies nationwide. Several prominent email providers – notably, Google and Yahoo! – are relying on the decision to resist warrants issued under the Stored Communications Act and its state law counterparts any

time compliance would require retrieving data from a foreign server. The decision below is therefore directly interfering with the *amici* States' ability to investigate and prosecute crime in their jurisdictions. The experience of Vermont's Internet Crimes Against Children Task Force is illustrative.

This Vermont task force is part of a network of approximately 61 coordinated task forces representing over 3,500 federal, state, and local law enforcement and prosecutorial agencies. The Vermont Attorney General's Office supervises the task force, whose responsibilities include investigating and prosecuting those who use online communications to sexually exploit children.[4] Since 2008, the task force has prosecuted nearly two hundred cases involving child pornography, luring children to engage in sexual conduct, and sexual assault of children. In the past two years alone, the task force has obtained hundreds of subpoenas and search warrants, many of which were issued under the federal Stored Communications Act and Vermont's Electronic Communication Privacy Act, 13 Vt. Stat. Ann. §§ 8101-8108.

Under the Stored Communications Act, a governmental entity may require a provider to disclose the contents of a wire or electronic communication:

> pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court,

[4] *See* Vt. Internet Crimes Against Children Task Force, www.vt-icac.org (last visited July 24, 2017).

> issued using State warrant procedures) by a court of competent jurisdiction.

18 U.S.C. § 2703(a). If a court issues the warrant, it is served on the provider like an ordinary subpoena. The provider must then review its files and produce data associated with the relevant user account to the requesting law enforcement agency. The agency then searches the data for evidence of the relevant crime. *See generally* 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, 1219 (2004).

When Vermont's task force seeks a warrant under the Stored Communications Act, an officer first prepares an affidavit demonstrating probable cause that a crime has been committed and that data held by the provider would contain evidence of the commission of that crime. *See generally* Vt. R. Crim. P. 41. A senior prosecutor in the Vermont Attorney General's Office Criminal Division then reviews, and if appropriate, approves the warrant application. The officer then appears before a judge and applies for the warrant.

When a provider relies on an extraterritoriality argument to resist complying with one of these warrants, it interferes with the task force's ability to investigate and prosecute those who use the provider's products to sexually exploit children. It also limits the task force's ability to identify victims who may still be at risk and in desperate need of services. And the only justification

for these social harms is the provider's business decision to locate some of its servers outside the United States.

The Vermont Attorney General's Office, on behalf of the task force, is currently litigating several motions to compel in state court against an email provider that is relying on the decision below to resist warrants issued jointly under the federal Stored Communications Act and Vermont's Electronic Communication Privacy Act, insofar as those warrants require disclosing data stored on foreign servers. This is notwithstanding that in each case: (i) the suspect lives in Vermont; (ii) a court found probable cause to believe a crime occurred in Vermont and that the suspect's email account contains relevant evidence of that crime; (iii) the provider is a United States company doing business in Vermont; (iv) its employees can access and produce the responsive data to the Vermont Attorney General's Office from within the United States; and (v) Attorney General's Office staff will search the responsive data in Vermont.

Law enforcement agencies in other jurisdictions around the country are experiencing similar problems. For example, in Utah, a provider refused to comply with a warrant that sought the contents of an account police knew contained a photograph of the suspect sexually abusing a minor. Similarly, providers have refused to comply with warrants for email data in connection with sexual exploitation investigations in a number of other States, including Massachusetts, Indiana, Illinois, Mississippi, New Hampshire, and Texas.

And in California, a provider refused to comply with a warrant for the contents of a cloud account that could be instrumental in determining the timeline and location of young girl's disappearance and suspected murder.[5]

## II. The decision below conflicts with this Court's precedent.

### A. Neither *Morrison* nor *RJR Nabisco* supports the Second Circuit's extraterritoriality analysis.

As explained in the petition for certiorari, the Second Circuit erred in concluding that compelling Microsoft to comply with the warrant in this case would be an extraterritorial application of the Stored Communications Act. Pet. 13-25. That conclusion is not in any way required by this Court's decisions in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *Id*. The proper "focus" of Section

[5] *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing before the S. Judiciary Subcomm. on Crime and Terrorism* (May 24, 2017) (Written Statement of Christopher Kelly 3-4), *available at* https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights (last visited July 24, 2017); *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing before the H. Judiciary Comm.* (Written Statement of Richard Littlehale 3-4)*, available at* https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/ (last visited July 24, 2017).

2703 is the provider's disclosure of electronic communications to the government, which occurs entirely within the United States. *See* Pet. 14-17.

The result would be no different if user privacy were the "focus" of the relevant statutory provisions. No extraterritorial invasion of privacy is likely to occur when a provider's employee uses a computer in this country to retrieve information from a foreign server, and then discloses that information to a domestic law enforcement agency. *See, e.g.*, Orin S. Kerr, *Search and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005) (arguing that, for purposes of the Fourth Amendment, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer"). This is particularly true when the warrant seeks data generated here by a customer who lives here and is being investigated for crimes committed here.[6] *Cf.* App. 64a-65a & n.7 ("It seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides.") (Lynch, J., concurring).

Locating the relevant privacy interest in this country is also consistent with longstanding Fourth Amendment principles. It is well-established that the Fourth Amendment "protects people not places." *Katz*

[6] While this may or may not describe the facts of this case (the record is unclear), some providers are relying on the decision below to resist warrants even when the only non-domestic aspect of the case is the location of the provider's server.

*v. United States*, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). The extent of a customer's privacy rights to their electronic data should depend upon the customer's reasonable expectations, not upon the provider's business decision to move those data overseas.

Moreover, complying with a warrant lawfully issued under the Stored Communications Act will create little to no risk of international discord when all the relevant connections and conduct are domestic, aside from the location of the servers to which the provider has chosen to send a customer's data. *See In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google*, 2017 WL 471564, at *12 ("No foreign nation's sovereignty will be interfered with in any ascertainable way at the time the two warrants at issue are executed because the searches will be conducted in the United States."). The Second Circuit's concern on this point was misplaced. *See* App. 25a.[7]

---

[7] Since the decision below was issued, a number of magistrate judges have disagreed with the Second Circuit's extraterritoriality analysis. *See, e.g.*, *In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017); *In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search of Content that is Stored at Premises Controlled by Google*, No. 16-mc-80263, 2017 WL 1487625 (N.D.

### B. The decision below conflicts with long-standing precedent concerning the obligation to produce relevant evidence in response to legal process.

Although the technology at issue in this case is new, the underlying legal principle at stake is not. A company should not be permitted to shield evidence of criminal conduct from law enforcement simply by relocating that evidence to one of the company's facilities in another jurisdiction.

The Court made this principle clear more than a hundred years ago. In 1906, the Consolidated Rendering Company was headquartered in Boston, Massachusetts, but operated a meat and rendering plant in Burlington, Vermont. *In re Consol. Rendering Co.*, 80 Vt. 55, 66 A. 790, 792 (1907). The State of Vermont, through a grand jury, was investigating four members of the State's board of cattle commissioners for selling diseased meat. *Id.* The grand jury served Consolidated Rendering with a subpoena to produce records regarding the company's dealings with the cattlemen. *Id*. But before the subpoena issued, the company directed its Burlington bookkeeper to send all the company's relevant records to the Boston office. *Id.* at 795. Despite

---

Cal. Apr. 25, 2017); *In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo*, Nos. 17-M-1234, 1235, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google*, 2017 WL 471564. As of the date this brief was filed, the *amici* States are not aware of any court that has issued a decision agreeing with the Second Circuit's analysis.

this, the Vermont courts found the company in contempt for failing to produce the records in Vermont in response to the subpoena. As explained by the Vermont Supreme Court:

> Taking the books [to another jurisdiction] was merely shifting them from one hand to the other. They were as much in control of the corporation as before. That is the essential thing, and not the precise locality where they happened to be when called for. . . . No corporation, whether foreign or domestic, can evade its testimonial duty, which rests upon it while it is here doing business, by merely sending to . . . another [jurisdiction] documents pertaining to said business which are required as evidence in legal proceedings here, and refuse to produce them when required by authority of law.

*Id.* at 799. This Court affirmed, holding "that a corporation doing business in the state, and protected by its power, may be compelled to produce, before a tribunal of the state, material evidence in the shape of books or papers kept by it in the state, and which are in its custody and control, although, for the moment, outside the borders of the state." *Consol. Rendering Co. v. Vermont*, 207 U.S. 541, 552 (1908).

Although times have changed, the principle of *Consolidated Rendering* remains sound. A company – whether it processes meat or provides email service – should not be allowed to "thwart the government's otherwise justified demand for" relevant evidence of

criminal activity "by the simple expedient of choosing – in its own discretion – to store" that evidence in another jurisdiction. *See* App. 52a (Lynch, J., concurring).

## CONCLUSION

The petition for a writ of certiorari should be granted.

July 27, 2017

Respectfully submitted,

THOMAS J. DONOVAN
Attorney General of
the State of Vermont
BENJAMIN D. BATTLES*
Solicitor General
JOHN R. TREADWELL
EVAN P. MEENAN
Assistant Attorneys General
109 State Street
Montpelier, VT 05609
(802) 828-5500
benjamin.battles@vermont.gov

**Counsel of Record*

STEVE MARSHALL
Attorney General
STATE OF ALABAMA
501 Washington Avenue
Montgomery, AL 36130

MARK BRNOVICH
Attorney General
STATE OF ARIZONA
1275 W. Washington
Street
Phoenix, AZ 85007

LESLIE RUTLEDGE
Attorney General
STATE OF ARKANSAS
323 Center Street
Little Rock, AR 72201

KEVIN T. KANE
Chief State's Attorney
STATE OF CONNECTICUT
300 Corporate Place
Rocky Hill, CT 06067

MATTHEW P. DENN
Attorney General
STATE OF DELAWARE
820 N. French Street
Wilmington, DE 19801

DOUGLAS S. CHIN
Attorney General
STATE OF HAWAII
425 Queen Street
Honolulu, HI 96813

LAWRENCE G. WASDEN
Attorney General
STATE OF IDAHO
P.O. Box 83720
Boise, ID 83720

LISA MADIGAN
Attorney General
STATE OF ILLINOIS
100 W. Randolph St.
Chicago, IL 60601

CURTIS T. HILL, JR.
Attorney General
STATE OF INDIANA
200 W. Washington Street
Indianapolis, IN 46204

THOMAS J. MILLER
Attorney General
STATE OF IOWA
1305 E. Walnut Street
Des Moines, IA 50319

DEREK SCHMIDT
Attorney General
STATE OF KANSAS
120 SW 10th Avenue
Topeka, KS 66612

ANDY BESHEAR
Attorney General
COMMONWEALTH
OF KENTUCKY
700 Capitol Avenue
Frankfort, KY 40601

JEFF LANDRY
Attorney General
STATE OF LOUISIANA
1885 N. Third Street
Baton Rouge, LA 70802

JANET T. MILLS
Attorney General
STATE OF MAINE
6 State House Station
Augusta, ME 04333

BRIAN E. FROSH
Attorney General
STATE OF MARYLAND
200 Saint Paul Place
Baltimore, MD 21202

MAURA HEALEY
Attorney General
COMMONWEALTH
OF MASSACHUSETTS
One Ashburton Place
Boston, MA 02108

BILL SCHUETTE
Attorney General
STATE OF MICHIGAN
P.O. Box 30212
Lansing, MI 48909

TIMOTHY C. FOX
Attorney General
STATE OF MONTANA
P.O. Box 201401
Helena, MT 59620

DOUG PETERSON
Attorney General
STATE OF NEBRASKA
2115 State Capitol
Lincoln, NE 68509

GORDON J. MACDONALD
Attorney General
STATE OF NEW HAMPSHIRE
33 Capitol Street
Concord, NH 03301

HECTOR H. BALDERAS
Attorney General
STATE OF NEW MEXICO
408 Galisteo Street
Santa Fe, NM 87501

ERIC T. SCHNEIDERMAN
Attorney General
STATE OF NEW YORK
120 Broadway
New York, NY 10271

JOSH STEIN
Attorney General
STATE OF NORTH CAROLINA
9001 Mail Service Center
Raleigh, NC 27699

MICHAEL DEWINE
Attorney General
STATE OF OHIO
30 E. Broad Street
Columbus, OH 43215

ELLEN F. ROSENBLUM
Attorney General
STATE OF OREGON
1162 Court Street NE
Salem, OR 97301

JOSH SHAPIRO
Attorney General
COMMONWEALTH
OF PENNSYLVANIA
Strawberry Square
Harrisburg, PA 17120

ALAN WILSON
Attorney General
STATE OF SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211

MARTY J. JACKSON
Attorney General
STATE OF SOUTH DAKOTA
1302 E. Highway 14
Pierre, SD 57501

KEN PAXTON
Attorney General
STATE OF TEXAS
P.O. Box 12548
Austin, TX 78711

SEAN D. REYES
Attorney General
STATE OF UTAH
P.O. Box 142320
Salt Lake City, UT 84114

MARK R. HERRING
Attorney General
COMMONWEALTH OF VIRGINIA
202 N. Ninth Street
Richmond, VA 23219

PETER K. MICHAEL
Attorney General
STATE OF WYOMING
2320 Capitol Avenue
Cheyenne, WY 82002

WANDA VASQUEZ-GARCED
Attorney General
COMMONWEALTH OF
PUERTO RICO
P.O. Box 9020192
San Juan, PR 00902