No. 17-2

IN THE

Supreme Court of the United States

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

UNITED STATES OF AMERICA,
Petitioner,

v.

MICROSOFT CORPORATION,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AS *AMICUS CURIAE* IN SUPPORT OF NEITHER PARTY

SIR IAIN MACLEOD
The Legal Adviser
STEPHEN H. SMITH
Assistant Legal Adviser
FOREIGN AND COMMONWEALTH OFFICE
United Kingdom

DONALD I. BAKER
Counsel of Record
W. TODD MILLER
ISHAI MOOREVILLE
BAKER & MILLER PLLC
2401 Pennsylvania Avenue, NW
Suite 300
Washington, DC 20037
(202) 663-7820
dbaker@bakerandmiller.com

Attorneys for the Government of the United Kingdom of Great Britain and Northern Ireland

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

QUESTION PRESENTED

Whether the normal presumption that an ambiguous U.S. statute not be treated as having extraterritorial effect prevents 18 U.S.C. § 2703 from being used by the U.S. Department of Justice to compel a U.S.-based provider of email services to comply with a probable-cause-based warrant for electronic communications within that provider's control, but which the provider has chosen to store abroad.

TABLE OF CONTENTS

	Page
QUESTION PRESENTED	i
TABLE OF AUTHORITIES	v
INTERESTS OF *AMICUS CURIAE*	1
SUMMARY OF ARGUMENT	1
ARGUMENT	3
I. THE STORAGE LOCATION OF ELECTRONIC COMMUNICATIONS SHOULD NOT BE DETERMINATIVE OF WHETHER A NATION MAY COMPEL ACCESS TO SUCH COMMUNICATIONS	3
A. A Solely Location-Based Approach to Law Enforcement Access to Data No Longer Makes Sense in the Digital Age	4
B. The U.K. Has Therefore Enacted a Statute for Obtaining Electronic Communications from Providers Providing Services Within the U.K., Regardless of the Data's Storage Location	5
II. THE SECOND CIRCUIT DECISION HAS DISRUPTED THE U.K.-U.S. MLAT PROCESS	7

TABLE OF CONTENTS—Continued

Page

A. Under the Current U.K.-U.S. MLAT, the U.K. Submits Requests for Electronic Communications Belonging to U.S. Providers to the DOJ..... 7

B. The Second Circuit Decision Means the United States Can No Longer Assist the U.K. In Accessing Electronic Communications Held by U.S. Providers Abroad..... 9

III. THE SECOND CIRCUIT DECISION IMPEDES THE EFFORTS OF THE U.K. AND THE UNITED STATES TO MODERNIZE THEIR MUTUAL EFFORTS TO OBTAIN ELEC-TRONIC COMMUNICATIONS FROM EACH OTHER'S PROVIDERS..... 10

A. The Traditional MLAT Process Can Be Too Slow for Many Modern Criminal Investigations Requiring Electronic Communications 11

B. The U.K. Is Negotiating a New Bilateral Agreement With the United States Regarding Access to Electronic Communications..... 11

CONCLUSION 14

TABLE OF AUTHORITIES

CASES Page(s)

EEOC v. Arabian Am. Oil Co., 499 U.S. 244 (1991) 5

F. Hoffmann-La Roche Ltd v. Empagran S. A., 542 U.S. 155 (2004) 5

In re Search Warrant No. 16-960-M-1, No. 16-960, 2017 U.S. Dist. LEXIS 131230 (E.D. Pa. Aug. 17, 2017) 4, 10

Kiobel v. Royal Dutch Petro. Co., 569 U.S. 108 (2013) 5

Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010) 5

STATUTES

18 U.S.C. § 2703 8

18 U.S.C. § 2703(a) 8

18 U.S.C. § 2711 8

18 U.S.C. § 3512 8

FOREIGN STATUTES AND REGULATIONS

Data Retention and Investigatory Powers Act 2014 (U.K.), available at http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted (as last visited December 12, 2017) 6

TABLE OF AUTHORITIES—Continued

	Page(s)
Investigatory Powers Act 2016 (U.K.), available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (as last visited December 12, 2017)	5, 6
Part 2, Ch. 1, § 41	6
Part 2, Ch. 1, § 42	6
Part 2, Ch. 1, § 43	6
Part 9, Ch. 2, § 261(10)	6
Regulation of Investigatory Powers Act 2000 (U.K.), available at https://www.legislation.gov.uk/ukpga/2000/23/contents (as last visited December 12, 2017)	5, 6
Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penal-ties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN (as last visited December 12, 2017)	12

TABLE OF AUTHORITIES—Continued

Page(s)

Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en (as last visited December 12, 2017) 12

TREATIES

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. No. 108, 20 I.L.M. 317, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (as last visited December 12, 2017) 12

TABLE OF AUTHORITIES—Continued

Page(s)

Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance in Criminal Matters signed 6 January 1994, U.S.-U.K., Dec. 16, 2004, T.I.A.S. No. 10-201.49, 2004 U.S.T. LEXIS 248, available at https://www.state.gov/documents/organization/190062.pdf (as last visited December 12, 2017)..... 2-3

Mutual Legal Assistance Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland, U.S.-U.K., Jan. 6, 1994, T.I.A.S No. 96-1202, S. Treaty Doc. No. 104-2, 1994 U.S.T. LEXIS 234, available at http://www.state.gov/documents/organization/176269.pdf (as last visited December 12, 2017) .....*passim*

TABLE OF AUTHORITIES—Continued

OTHER AUTHORITIES Page(s)

Att'y Gen. Jeff Sessions, Dept. of Justice, Attorney General Sessions Delivers Remarks at the Global Forum on Asset Recovery Hosted by the United States and the United Kingdom (Dec. 4, 2017) (Washington, DC), available at https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-global-forum-asset-recovery-hosted-united (as last visited December 12, 2017) 13

Council of Europe, Modernisation of the Data Protection "Convention 108" available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true (as last visited December 12, 2017)..... 12

Richard A. Clarke et al., President's Review Group On Intelligence & Communications Technology, Liberty and Security In A Changing World (2013) available at https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world (as last visited December 12, 2017)..... 8, 11

TABLE OF AUTHORITIES—Continued

Page(s)

Statement of Paddy McGuinness, United Kingdom Deputy National Security Adviser, *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Hearing Before the Sen. Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary,* 115th Cong. (May 10, 2017) available at https://www.judiciary.senate.gov/download/05-24-17-mcguinness-testimony (as last visited December 12, 2017) 10

Statement of Richard W. Downing, Acting Deputy Assistant Attorney General, DOJ, *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Sen. Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (May 10, 2017) available at https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf. (as last visited December 12, 2017)..... 7

INTERESTS OF *AMICUS CURIAE*

The United Kingdom ("U.K.") believes that it is important that the Court understand the broader law enforcement context in which the current case occurs.[1]

Prompt access to email and social media traffic ("electronic communications") is necessary for U.K. law enforcement in all types of criminal investigations, including those combating terrorist-type crimes. But the Second Circuit decision disrupts the U.K.'s ability to use the existing U.K.-U.S. Mutual Legal Assistance Treaty ("MLAT") in order to obtain relevant electronic communications from any U.S.-based provider of electronic communications services in the United Kingdom when the provider has stored the relevant communications outside the United States, as is frequently the case.

The U.K. does not take a position on the proper interpretation of the Stored Communications Act.

SUMMARY OF ARGUMENT

U.S.-based providers of electronic communication services ("Providers") have taken a variety of approaches to storing electronic communications: such communications may be broken into shards that are stored in multiple nations simultaneously, or they may be moved around the world from day to day depending on network demands.

---

[1] Pursuant to Supreme Court Rule 37.6, Amicus Curiae states that no counsel for a party authored this brief in whole or in part and that no person or entity other than Amicus Curiae, its members, and its counsel contributed monetarily to the preparation or submission of this brief. Both Petitioner and Respondent have granted their consent to the filing of all amicus briefs.

Because of such storage policies, and due to technological change and the global nature of the communications environment, the U.K. does not believe that the geographic storage location of data should be the determining factor for whether or not a nation may gain access to such communications.

Accordingly, the U.K. Investigatory Powers Act, which was enacted in 2016 but has yet to fully enter into force, enables the compulsion of an overseas Provider offering services in the U.K. to provide certain electronic communications sought by a U.K. warrant despite those communications being stored outside of the U.K.

The U.K. also contends that a request for electronic communications stored overseas by a Provider but accessible within the requesting country does not involve an exercise of extraterritorial jurisdiction.

In practice, when the U.K. seeks to obtain electronic evidence from a U.S.-based Provider, it frequently seeks to obtain such communications under the MLAT agreement with the United States that was signed in 1994, and amended in 2004.[2]

---

[2] Mutual Legal Assistance Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland, U.S.-U.K., Jan. 6, 1994, T.I.A.S No. 96-1202, S. Treaty Doc. No. 104-2, 1994 U.S.T. LEXIS 234, available at http://www.state.gov/documents/organization/176269.pdf (as last visited December 12, 2017) [hereinafter U.K.-U.S. MLAT].

The U.K.-U.S. MLAT was later amended by: Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance in Criminal

But the Second Circuit's decision disrupts this cooperative MLAT process because it prevents the U.S. Department of Justice ("DOJ") from being able to compel a U.S. Provider providing services in the U.K. to provide electronic communications stored outside the United States.

Similarly, the Second Circuit's decision is also an impediment to other bilateral agreements that the United States and U.K. are currently pursuing in order to facilitate and regulate reciprocal access to electronic communications controlled from each other's jurisdictions.

ARGUMENT

I. THE STORAGE LOCATION OF ELECTRONIC COMMUNICATIONS SHOULD NOT BE DETERMINATIVE OF WHETHER A NATION MAY COMPEL ACCESS TO SUCH COMMUNICATIONS

The global nature of the modern communications environment renders laws basing access to data purely on location ineffective and likely to lead to unintended and perverse outcomes. Further, for a nation's law enforcement functions to operate effectively, it requires access in limited and regulated circumstances to the electronic communications relating to those in its jurisdiction, wherever those communications are stored.

Matters signed 6 January 1994, U.S.-U.K., Dec. 16, 2004, T.I.A.S. No. 10-201.49, 2004 U.S.T. LEXIS 248, available at https://www.state.gov/documents/organization/190062.pdf (as last visited December 12, 2017).

A. A Solely Location-Based Approach to Law Enforcement Access to Data No Longer Makes Sense in the Digital Age

A large amount of electronic communications services used by the U.K.'s residents are provided by U.S.-based companies. Each Provider has different policies for how and where they store electronic communications around the globe.

Attempting to assign a geographic location to electronic communications stored on an international network is an elusive process, and unlike a traditional document, such communications do not necessarily have a single location.

For example, the record states that "Microsoft generally stores a customer's email information and content at data centers located near the physical location identified by the user as its own when subscribing to the service." Pet. App. 6a. Google has represented that it "breaks individual user files into component parts, or shards, and stores the shards in different network locations in different countries at the same time." *In re Search Warrant No. 16-960-M-1*, No. 16-960, 2017 U.S. Dist. LEXIS 131230, at *3-4 (E.D. Pa. Aug. 17, 2017). Other Providers maintain yet other data storage policies.

If statutory access tests were to rest on the geographic location of storage, such tests would be unrealistic and unworkable.

Further, a system that would require that warrants could be issued only by the country where electronic communications are stored (as urged by Microsoft in this case) could also result in the creation of offshore "data haven" countries that would block legitimate access by foreign nations' law enforcement authorities,

and help wrongdoers evade investigators in the countries where they were resident or doing business. The corporate structure of, or commercial decisions taken by, individual companies should not dictate the jurisdiction enjoyed by a court in the nation in which a company is located to access its data.

In addition, the U.K. does not consider that a request for electronic communications stored overseas for the time being by a Provider, but accessible to that Provider from within the requesting country, involves an exercise of extraterritorial jurisdiction of the sort that this Court has found to be inappropriate as a matter of international law and comity. *See Kiobel v. Royal Dutch Petro. Co.*, 569 U.S. 108 (2013); *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247 (2010); *F. Hoffmann-La Roche Ltd v. Empagran S. A.*, 542 U.S. 155 (2004); *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244 (1991).

B. The U.K. Has Therefore Enacted a Statute for Obtaining Electronic Communications from Providers Providing Services Within the U.K., Regardless of the Data's Storage Location

Reflecting the above, U.K. investigatory powers law provides the ability for U.K. law enforcement to compel any Provider offering telecommunications services in the U.K., including overseas Providers, to provide certain electronic communications sought by a U.K. warrant, even if the data are stored or controlled abroad.[3] These powers are not new and were originally contained in the Regulation

[3] Investigatory Powers Act 2016 (U.K.) available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (as last visited December 12, 2017).

of Investigatory Powers Act 2000 ("RIPA") and subsequently clarified in the Data Retention and Investigatory Powers Act 2014 ("DRIPA").[4] In 2016 the U.K. enacted the Investigatory Powers Act ("IPA").[5] The IPA is a comprehensive statute which, when fully in force, will replace the relevant parts of RIPA and DRIPA and will provide a judicially-supervised basis for the U.K. to obtain electronic communications stored overseas.

The IPA covers any telecommunications operator which provides services to persons within the U.K.,[6] and such an operator can be required to disclose electronic communications without regard to where the communications are stored or processed, so long as it is reasonably practicable for the operator to provide assistance in obtaining the demanded communication.[7]

These powers may therefore be used to compel a U.S. Provider offering telecommunications services in the U.K. to provide certain electronic communications sought by a U.K. warrant, even if those communications are stored abroad, or the Provider claims that it can only access such communications from a location within the United States.

---

[4] Regulation of Investigatory Powers Act 2000 (U.K.) available at https://www.legislation.gov.uk/ukpga/2000/23/contents (as last visited December 12, 2016); Data Retention and Investigatory Powers Act 2014 (U.K.) available at http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted (as last visited December 12, 2017).

[5] *Supra* note 3.

[6] Investigatory Powers Act 2016, Part 9, Ch. 2, § 261(10) (providing definition of telecommunications operator).

[7] *See, e.g.,* Investigatory Powers Act 2016, Part 2, Ch. 1, §§ 41; 42; 43.

II. THE SECOND CIRCUIT DECISION HAS DISRUPTED THE U.K.-U.S. MLAT PROCESS

The U.K. is dependent upon the U.K.-U.S. MLAT to obtain evidential data stored overseas from electronic communications Providers.[8] The principal Providers of such services to people in the U.K. are based in the United States.

As a result of the Second Circuit's decision, many U.S. Providers do not comply with U.S. warrants for communications located outside the United States.[9] Therefore, the U.K. can no longer necessarily rely on the U.K.-U.S. MLAT process to obtain electronic communications where those communications are not stored in the United States. This is true even where the electronic communications sought belong to individuals in the U.K.

A. Under the Current U.K.-U.S. MLAT, the U.K. Submits Requests for Electronic Communications Belonging to U.S. Providers to the DOJ

One of the enumerated exceptions to the bar on disclosure contained in the Stored Communications Act ("SCA") is that a Provider may provide electronic communications pursuant to a warrant, but such

---

[8] *Supra* note 2.

[9] *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Sen. Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (May 10, 2017) (statement of Richard W. Downing, Acting Deputy Assistant Attorney General, DOJ, at 3) available at https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf (as last visited December 12, 2017).

warrants must be obtained by a U.S. governmental entity. 18 U.S.C. § 2703(a).[10] The SCA provides no specific mechanism for U.S. Providers to respond to warrants issued by foreign governments.

This means that the U.K. has relied on the MLAT between the U.K. and the United States to seek certain electronic communications from U.S. Providers.[11]

When the U.K. makes a request for electronic communications to DOJ pursuant to the U.K.-U.S. MLAT, the DOJ first must review the request to determine if it complies with the Treaty. If the DOJ deems the request to be compliant, the DOJ then applies for a U.S. warrant, based on the U.K. request, for the purpose of complying with the SCA provision on warrants. *See* 18 U.S.C. § 2703(a).[12]

The MLAT process is generally a slow one, with DOJ averaging about 10 months to respond to an MLAT request from a foreign government.[13]

---

[10] The statute defines "governmental entity" to mean "a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711.

[11] *See supra* note 2.

[12] *See also* 18 U.S.C. § 3512 (which authorizes the U.S. government to seek "a warrant or order for contents of stored wire or electronic communications or for records related thereto" under Section 2703 of the SCA).

[13] Richard A. Clarke et al., President's Review Group On Intelligence & Communications Technology, Liberty and Security In A Changing World 227 (2013) available at https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world (as last visited December 12, 2017) (noting that the United States takes an average of ten months to respond to requests made through the MLAT process).

B. The Second Circuit Decision Means the United States Can No Longer Assist the U.K. In Accessing Electronic Communications Held by U.S. Providers Abroad

Since the Second Circuit decision in this case, the traditional U.K.-U.S. MLAT process has only been successful if the U.S. Provider has chosen to store the desired electronic communications in the United States. And as the U.K. usually does not know where an electronic communication is stored, this means that the already time-consuming and complicated MLAT procedure provides no guarantee of obtaining the communications sought.

Even Providers themselves may not know where certain electronic communications are kept from day to day, and there is nothing to prevent a Provider from moving communications to another country before an MLAT request is processed by DOJ. Again, this further complicates and delays the ability of the U.K. to obtain relevant communications from U.S. Providers.

For example, shortly after the *Microsoft* ruling, an MLAT request was submitted by the U.K. to the United States for certain electronic communications from two email accounts in a case concerning the incitement of a child to engage in sexual activity. It transpired that the accounts were held on servers in two third countries and, as such, requests for those communications had to be withdrawn, because the Provider would not provide such communications located abroad.

Google's approach of storing data in component parts, which involves breaking communications into

shards and storing them in pieces around the world,[14] makes the MLAT process unworkable in these circumstances should the Second Circuit decision stand.

III. THE SECOND CIRCUIT DECISION IMPEDES THE EFFORTS OF THE U.K. AND THE UNITED STATES TO MODERNIZE THEIR MUTUAL EFFORTS TO OBTAIN ELECTRONIC COMMUNICATIONS FROM EACH OTHER'S PROVIDERS

Electronic communications are particularly essential when enforcement authorities are trying to (i) respond to and forestall threatened crimes or (ii) break up ongoing criminal conduct. Effective "forward looking" investigation and prosecution of offenses can often require almost immediate access to relevant electronic communications generated by those planning or executing such offenses, which are not as suitable for the MLAT Process.[15] Accordingly, the U.K. and United States are considering a new approach. The Second Circuit decision impedes those efforts.

---

[14] *See In re Search Warrant No. 16-960-M-1*, No. 16-960, 2017 U.S. Dist. LEXIS 131230, at *3-4 (E.D. Pa. Aug. 17, 2017).

[15] *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Hearing Before the Sen. Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary,* 115th Cong. (May 10, 2017) (statement of Paddy McGuinness, United Kingdom Deputy National Security Adviser, at 1) available at https://www.judiciary.senate.gov/download/05-24-17-mcguinness-testimony (as last visited December 12, 2017).

A. The Traditional MLAT Process Can Be Too Slow for Many Modern Criminal Investigations Requiring Electronic Communications

The existing U.K.-U.S. MLAT process was essentially designed to provide each party's prosecutors with a channel for obtaining information needed to investigate and prosecute crimes that have already been committed, i.e. it was a "backward looking" process for investigations into past-conduct offenses.

As has already been explained, it takes on average about 10 months to obtain communications from a U.S. Provider in response to an MLAT request, and can take even longer.[16] This is not timely enough to be useful to the U.K.'s law enforcement when they are trying to anticipate and head off terrorist and security threats or stop ongoing crimes such as drug trafficking and child abuse. In such situations, where the standard for obtaining a warrant has been satisfied, quick access to relevant electronic communications is absolutely critical, and can make the difference between life and death.

B. The U.K. Is Negotiating a New Bilateral Agreement With the United States Regarding Access to Electronic Communications

The U.K. envisions a new agreement with the United States in which each nation would enjoy reciprocal access to certain communications held by Providers located in each nation's jurisdiction, for which a warrant has been obtained, without incurring the delays of going through the MLAT process. The

[16] *See supra* note 13.

reciprocal access would apply regardless of where communications being sought were actually being stored.

Such an agreement between the U.K. and the United States would be founded on a high level of privacy protection for personal data, respect for freedom of speech and international human rights law. For example, the U.K. is committed to implementing the European Union's General Data Protection Regulation ("the GDPR"),[17] the associated Law Enforcement Directive ("LED"),[18] and the Council of Europe's modernized Convention 108.[19] Those

[17] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en (as last visited December 12, 2017).

[18] Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN (as last visited December 12, 2017).

[19] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. No. 108, 20 I.L.M. 317, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (as last visited December 12, 2017). This Convention is undergoing a modernization process. The UK intends to accede to the modernized version of the Convention. *See* Council of Europe, Modernisation of the Data Protection "Convention 108" available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true (as last visited December 12, 2017).

instruments contain a number of bases and safeguards for the international transfer of data.

However, for this type of agreement to be viable, the United States and the U.K. both must have the domestic power to obtain those communications stored overseas. As described above, the U.K. has this authority under the IPA. The U.S. Attorney General recently made clear that the United States must have the same authority for the framework to function: "In order for this type of framework to function, however, we need to ensure that our warrants continue to be effective even when an American company chooses to store customer data outside of the United States."[20]

The Second Circuit decision is a serious impediment to the effectiveness of U.S. warrants, and therefore the viability of this type of agreement.

[20] Att'y Gen. Jeff Sessions, Dept. of Justice, Attorney General Sessions Delivers Remarks at the Global Forum on Asset Recovery Hosted by the United States and the United Kingdom (Dec. 4, 2017) (Washington, DC), available at https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-global-forum-asset-recovery-hosted-united (as last visited December 12, 2017).

CONCLUSION

In today's global communications environment that does not respect geographic boundaries, the U.K. believes that the location of data should not be solely determinative of access for law enforcement purposes. Such an approach would remove the ability of sovereign nations to protect life and prevent and detect crime within their jurisdiction.

The Second Circuit's decision has hindered the MLAT process and, consequently, the U.K.'s ability to obtain electronic communications relevant to its criminal investigations. It also impedes efforts to modernize law enforcement access to data across borders. The U.K. therefore asks that this Court take into account the aforementioned matters when deciding the present case.

Respectfully submitted,

SIR IAIN MACLEOD
The Legal Adviser
STEPHEN H. SMITH
Assistant Legal Adviser
FOREIGN AND
COMMONWEALTH OFFICE
United Kingdom

DONALD I. BAKER
Counsel of Record
W. TODD MILLER
ISHAI MOOREVILLE
BAKER & MILLER PLLC
2401 Pennsylvania Avenue, NW
Suite 300
Washington, DC 20037
(202) 663-7820
dbaker@bakerandmiller.com

Attorneys for the Government of the United Kingdom of Great Britain and Northern Ireland

December 13, 2017