UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW

Volume 47 | Number 3 Article 4

Spring 2022

Where in the World is My Data Today? The U.S.-U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigations

Krista Peace

Where in the World is My Data Today? The U.S. – U.K. Bilateral Data Access Agreement Ushers in a New Era of Cross-Border Data Sharing for Criminal Investigations

Krista Peace†

I. Introduction

In an era of constant, global internet communication, access to electronic data evidence for criminal investigations has become an increasingly complex minefield, frustrating law enforcement officials who are often bound by antiquated bureaucratic systems that fail to efficiently or effectively address the "borderless nature

† University of North Carolina School of Law, Class of 2022. Online Editor, North Carolina Journal of International Law.

of the internet."[1] In 2019, the European Commission found that "[m]ore than half of all criminal investigations today require access to cross-border electronic evidence."[2] For decades, the formal process to obtain cross-border evidence for criminal investigations has been through Mutual Legal Assistance Treaty requests.[3]

The world's largest communication service providers ("CSPs") that hold the bulk of the global communications data, such as Google, Facebook, Twitter, Apple, Yahoo, and Microsoft, are all headquartered in the United States.[4] As a result, every year the United States receives an exponentially increasing number of Mutual Legal Assistance Treaty requests from other countries to obtain access to the data for criminal investigations.[5] This has become an inefficient and ineffective system that can take up to two years for the requesting country to gain access to the necessary data.[6] Until recently, this was the only way for other countries to judicially request access to this kind of data.[7]

On October 3, 2019, the United States and the United Kingdom signed a bilateral data access agreement: "Agreement Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious

---

1 *See Recommendation for a Council Decision Authorising the Opening of Negotiations in View of an Agreement Between the European Union and the United States of America on Cross-border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters*, at 1, COM (2019) 70 final (May 2, 2019) [hereinafter European Commission Recommendation].

2 *Id*.

3 *See* Gail Kent, Sharing Investigation Specific Data with Law Enforcement – An International Approach 1 (Feb. 14, 2014) (Stanford Public Law Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413 [https://perma.cc/48YL-FG94].

4 *See id*. at 4; European Commission Recommendation, *supra* note 1, at 1.

5 *See* European Commission Recommendation, *supra* note 1, at 2.

6 *See id*. at 2; Press Release, Department of Justice, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [https://perma.cc/F7GD-4KMU] [hereinafter U.S. UK DOJ Press Release].

7 *See* Kent, *supra* note 3, at 5. *But see* T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUD. CTR. 1, 23 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf [https://perma.cc/GRT9-LFCB] [hereinafter MLAT Guide] (discussing informal channels of exchanging information).

Crime" ("The Agreement").[8] The Agreement is a first-of-its-kind data sharing agreement between the two countries for the purpose of creating a more efficient and effective system through which law enforcement agencies can obtain access to electronic evidence held by CSPs overseas for certain criminal investigations.[9] The overarching goal is the "prevention, detection, investigation, or prosecution of [s]erious [c]rime."[10] Instead of engaging in the lengthy Mutual Legal Assistance Treaty ("MLAT") request process, designated law enforcement bodies will be able to directly serve evidence production orders for certain requests on CSPs based in the other country party to the agreement.[11]

At the signing of the agreement, U.S. Attorney General William Barr stated, "Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats."[12] While The Agreement is the first of its kind, it is expected to serve as a model for U.S. data sharing agreements with other parties in the future.[13] The United States is negotiating a similar agreement with the European Union[14] and recently entered into a similar agreement with Australia.[15]

Analysis will proceed in seven parts. Part II will provide an overview of cross-border evidence-sharing mechanisms for criminal investigations, including a brief history of letters rogatory, the MLAT Process, and the ways in which these systems have become dysfunctional in the twenty-first century. Part III will

---

8 Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, U.K.-U.S., Oct. 3, 2019, 60 I.L.M. 2 [hereinafter The Agreement]; U.S. UK DOJ Press Release, *supra* note 6.

9 *See* U.S. UK DOJ Press Release, *supra* note 6.

10 The Agreement, *supra* note 8, art. 2, ¶ 1.

11 The Agreement, *supra* note 8, art. 5, ¶ 5.

12 U.S. UK DOJ Press Release, *supra* note 6.

13 *See* Jean Galbraith ed., *Contemporary Practice of the United States Relating to International Law*, 114 AM. J. INT'L L. 124, 128 (2020).

14 *See* Press Release, Department of Justice, Joint US-EU Statement on Electronic Evidence Sharing Negotiations (Sep. 26, 2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations [https://perma.cc/LR7V-D9KE].

15 *See* Press Release, Department of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime (Dec. 15, 2021), https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime [https://perma.cc/YRQ3-DE5J].

discuss the United States' enabling legislation, the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"). Part IV will describe the United Kingdom's enabling legislation, the Crime Overseas Production Act ("COPO Act"). Part V will examine the contents of The Agreement and the new process for obtaining cross-border evidence set forth in it. Part VI will evaluate public concerns for privacy and civil liberties and whether The Agreement appropriately addressed those concerns. Finally, Part VII will conclude.

II. An Overview of Cross-Border Data Sharing for Criminal Investigations

A. Letters Rogatory

Historically, letters rogatory were the primary means for requesting evidence located beyond the United States' territorial jurisdiction.[16] Letters rogatory are formal requests for assistance that are based on principles of comity and respect, but they do not engender any legal obligation to respond to the request or comply.[17] As a result, letters rogatory as a means for obtaining evidence are often inefficient and unreliable.[18] The United States relied on this comity-based mechanism to obtain cross-border evidence until the 1970s.[19]

B. Mutual Legal Assistance Treaties ("MLATs")

1. History

In the late 1970s, the United States began to investigate coordinated international crimes, such as terrorism, money laundering, and drug trafficking and, in doing so, recognized the need for cross-border legal assistance and evidence sharing in order to successfully investigate and prosecute these types of coordinated

---

16 *See* Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 691 (2017).

17 *See* MLAT Guide, *supra* note 7, at 17; *see also* Swire & Hemmings, *supra* note 16 at 692 ("Letters rogatory rely on principles of comity, or respect for foreign sovereignty, rather than on an assertion that the jurisdiction seeking the evidence has a legal right to the evidence.").

18 *See* MLAT Guide, *supra* note 7, at 3.

19 *See* Swire & Hemmings, *supra* note 16, at 695.

crime.[20] In 1977, the United States entered into its first MLAT with Switzerland.[21] Since then, the United States has entered into more than sixty bilateral MLATs with foreign countries, as well as a multilateral MLAT with the European Union and its member states.[22]

The MLAT system was promulgated to "improve the effectiveness of judicial assistance and to regularize and facilitate its procedures."[23] While letters rogatory are based on principles of comity, MLATs are "legally binding negotiated commitments"[24] that essentially "contractually obligate the two countries to provide each other evidence."[25] In the United States, MLATs are negotiated by the U.S. Department of Justice and the U.S. Department of State.[26] After the negotiations, the U.S. Secretary of State submits the proposed MLAT to the President, who in turn submits it to the U.S. Senate for advice and consent.[27] After this process, the President signs the treaty.[28]

This reciprocal treaty-based mechanism was an improvement from letters rogatory in terms of reliability and effectiveness, however, the process of obtaining evidence via an MLAT request is still extremely inefficient.[29] This inefficiency is exacerbated because requests for electronic evidence increase significantly, but funding for the DOJ does not increase to meet the demands of the

---

20 *See id*.

21 *See* U.S. Dep't of State, 7 Foreign Affairs Manual § 962.1, https://fam.state.gov/fam/07fam/07fam0960.html [https://perma.cc/D2PP-NJPU] [hereinafter DOS Foreign Affairs Manual].

22 *See id*.

23 *Id*.

24 MLAT Guide, *supra* note 7, at 5.

25 *See* In re Commissioner's Subpoenas, 325 F.3d 1287, 1290 (11th Cir. 2003), *overruled on other grounds by* Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241 (2004). MLATs only apply to criminal cases and MLAT requests can only be made by government officials and prosecutors. *See* MLAT Guide, *supra* note 7, at 2. The benefits of MLATs may not be used by civil litigants or defense counsel; instead, they must rely on letters rogatory to obtain evidence held abroad. *See id*. at 3. If a prosecutor or a foreign court seeks evidence in a country without an MLAT, they also must rely on letters rogatory to request evidence. *See id*.

26 *See* MLAT Guide, *supra* note 7, at 6.

27 *See id*.

28 *See id*.

29 *See* Swire & Hemmings, *supra* note 16, at 696.

requests.[30]

2. Process

To access electronic data evidence held by U.S. based CSPs, foreign countries that have an MLAT with the U.S. must rely on the lengthy and bureaucratic MLAT request process.[31] First, the law enforcement body seeking the evidence must file a request with their country's designated central authority for review.[32] If the request is approved, the central authority sends the request to the United States' central authority—the U.S. Department of Justice, Criminal Division, Office of International Affairs ("OIA").[33] The OIA is responsible for processing all incoming and outgoing MLAT requests in the U.S.[34] The OIA then reviews the request and works with the requesting country to conform the request to "meet U.S. standards."[35] Once the request is acceptable to the OIA, the OIA sends the request to the proper court or government entity.[36]

There is a "presumption in favor of honoring MLAT requests," but the court must review each request and determine that it complies with the terms of the negotiated MLAT and relevant U.S. law.[37] MLAT requests that are executed in the U.S. are subject to U.S. law, such as rules of privilege and constitutional limits and protections set out in the Fourth Amendment and the Fifth Amendment.[38] If the court has questions about the substance of the request, an inquiry may be directed to the OIA.[39]

If the court finds that the request comports with the terms of the treaty and U.S. law, then the court can serve the request on the U.S.

---

30 *See* U.S. Dep't of Just. FY 2015 Budget Request Mutual Legal Assistance Treaty Process Reform + $24.1 Million in Total Funding 1 (2014) [hereinafter DOJ Budget Request].

31 *See* TIFFANY LIN & MAILYN FIDLER, CROSS-BORDER DATA ACCESS REFORM: A PRIMER ON THE PROPOSED U.S.-U.K. AGREEMENT, A BERKLETT CYBERSECURITY PUBLICATION, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV. 1–2 (2017); MLAT Guide, *supra* note 7, at 3.

32 *See id*. at 2; DOS Foreign Affairs Manual, *supra* note 21.

33 *See* DOS Foreign Affairs Manual, *supra* note 21.

34 *See* MLAT Guide, *supra* note 7, at 3.

35 *See* Lin, *supra* note 31, at 2.

36 *See id*.; MLAT Guide, *supra* note 7, at 3.

37 *See* MLAT Guide, *supra* note 7, at 10.

38 *See id*. at 6–7; Lin, *supra* note 31, at 2.

39 *See* MLAT Guide, *supra* note 7, at 8.

company that holds the electronic data evidence that the country is seeking.[40] Once served, the company submits the evidence to the OIA.[41] The OIA then reviews the evidence to check for human rights issues and data minimization issues.[42] The OIA then transmits the evidence to the designated central authority of the requesting country, which in turn transmits the evidence to the original requesting law enforcement body.[43]

3. MLAT Dysfunction

The MLAT process was created at a time when evidence often had a clearly defined physical location. The system was created as a result of a need for cooperation. As technology has advanced, however, the nature of evidence has too. An event that, on its face, is a purely local crime in one country may implicate electronic evidence stored on a server thousands of miles beyond the borders of that country.[44] Because the U.S. is home to many of the world's largest CSPs such as Google, Facebook, Twitter, Apple, Yahoo, and Microsoft, the OIA often receives MLAT requests for electronic evidence for criminal investigations where the only connection to the U.S. is the fact that the electronic evidence is controlled by a U.S.-based CSP.[45]

As internet communication has increased, so too have the number of MLAT requests for electronic evidence.[46] The increase in MLAT requests has strained resources in the U.S. and led to an increase in wait time for responses to (often time sensitive) requests.[47] In 2019, obtaining data from the U.S. through the MLAT process typically took one year, but could take more than two

---

40 *See* Lin, *supra* note 31, at 2.

41 *See id*. at 3.

42 *See id*.

43 *See id*.

44 *See* Swire *supra* note 16, at 698 (describing a hypothetical burglary taking place in France that involves a French crime, a French victim, and a French suspect, with the only connection to the United States being that the emails about the crime are stored on a server controlled by a U.S.-based CSP).

45 *See* U.S. DEP'T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT WHITE PAPER 2 (2019) [hereinafter DOJ White Paper].

46 *See* CLOUD Act Resources, Department of Justice, https://www.justice.gov/dag/cloudact [https://perma.cc/CF28-KAUW].

47 *See id*.

years.[48] These delays have led to significant frustration on both sides of the MLAT process.

In 2015, in a request for additional funding, the U.S. Department of Justice ("DOJ") stated that over the past decade MLAT requests have "increased nearly 60 percent, and the number of requests for computer records has increased ten-fold."[49] The DOJ further warned that, "[d]elays and difficulties in obtaining evidence, especially internet records, through the MLAT process is increasingly becoming a source of frustration for many of our foreign partners" and that this could result in "significant adverse consequences."[50] In the request, the DOJ asked for an additional 141 staff positions to help with the MLA process.[51] The request was ultimately denied in the Senate.[52]

The U.K. Minister of State for Security and Economic Crime lamented that this dysfunctional system is extremely problematic, not only because criminal activity continues as law enforcement wait for the data necessary for their investigation, but also because innocent people cannot be cleared from suspicion during the period of time that they wait for the data necessary to remove them from the investigation.[53]

Adding to the dysfunction arising out of the inefficiencies of the MLAT process, former DOJ prosecutor turned whistleblower, Anush Khardori, recently accused certain prosecutors of abusing the lengthy MLAT process as pretext for obtaining statute of limitations extensions.[54] As a result of the time it takes to obtain evidence through the MLAT process, courts may grant an extension on the statute of limitations of up to three years to allow prosecutors the time to obtain the requested evidence.[55]

---

48 *See* THE HOME OFFICE, EXPLANATORY MEMORANDUM TO THE AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA ON ACCESS TO ELECTRONIC DATA FOR THE PURPOSE OF COUNTERING SERIOUS CRIME, 2019, Cm. 178 at 1 (UK) [hereinafter Explanatory Memorandum].

49 *See* DOJ Budget Request, *supra* note 30, at 1.

50 *See id*.

51 *See* DOJ Budget Request, *supra* note 30, at 2.

52 *See* Swire & Hemmings, *supra* note 16, at 717.

53 *See* Explanatory Memorandum, *supra* note 48, at 1.

54 *See* William F. Johnson & Bethany L. Rupert, *Whistleblower Illuminates Abuse of Process in Criminal Cross-Border Matters*, N.Y. L.J. (2020).

55 *See id*.

In the 2016 prosecution of a former Barclays trader Robert Bogucki, just days before the statute of limitations was set to run out, DOJ prosecutors filed an MLAT request with the U.K. for travel records to which they apparently already had access.[56] Bogucki later challenged this as an abuse of process and claimed that the prosecutor only filed the MLAT to stall the statute of limitations.[57] Bugocki's case is not the only one in which prosecutors have been accused of using an MLAT request as pretext for extending the statute of limitations.[58]

4. United States v. Microsoft Corp

In 2013, likely in response to the inefficiency and frustration that accompanies the MLAT request process, prosecutors in the Southern District of New York attempted an alternative route to obtain electronic data evidence stored on servers in Ireland but controlled by a U.S. company—Microsoft Corporation.[59] Instead of following the standard MLAT request process, prosecutors obtained a warrant through § 2703 of the Stored Communications Act ("SCA"). The warrant required Microsoft to "disclose all e-mails and other information associated with the account of one of its customers."[60] Microsoft challenged the warrant in court, arguing that a § 2703 warrant could not compel a U.S. provider to disclose data stored on servers abroad.[61] Eventually, the Supreme Court granted certiorari to decide the issue.[62]

Before the Court could issue an opinion however,[63] Congress addressed the issue with indisputable specificity via the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"). The CLOUD Act amended the SCA with the following provision:

> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information

56 *See id.*

57 *See id.*

58 *Id.*

59 United States v. Microsoft Corp., 138 S. Ct. 1186, 1187, 200 L. Ed. 2d 610 (2018).

60 *Id.*

61 *Id.*

62 *Id.*

63 *Id.*

> pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*."[64]

The CLOUD Act thus rendered the *Microsoft* case moot.[65]

III. The CLOUD Act

Not only did the CLOUD Act address the warrant issue in *Microsoft*, it also opened a new door to address the root of the issue underlying the conflict—the inefficiencies of the MLAT process. The CLOUD Act created a new avenue to share data for criminal investigations by authorizing the U.S. to enter into a new type of executive agreement with "qualifying foreign governments."[66] These executive agreements allow each country to directly serve production orders for electronic evidence to communication service providers in each other's respective country without going through the MLAT process.[67]

Now, there are three potential avenues through which a country can obtain electronic data evidence from the United States: (1) an executive data sharing agreement under the CLOUD Act, (2) a negotiated MLAT, or (3) in the absence of either of those, letters rogatory.

CLOUD Agreements are predicated on domestic law, so participating countries must enact the appropriate legislation to enable the CSPs based in their country to respond to production orders authorized by an executive agreement that are served by foreign law enforcement agencies.[68] The U.K. passed legislation to do exactly that in 2019.[69]

IV. The Crime (Overseas Production Orders) Act ("COPO Act")

As most CSPs are located outside of the U.K., accessing

---

64 CLOUD Act § 103(a)(1) (emphasis added).

65 United States v. Microsoft Corp., 138 S. Ct. 1186, 1187, 200 L. Ed. 2d 610 (2018).

66 18 U.S.C.A. § 2523; *see also* DOJ White Paper, *supra* note 45.

67 18 U.S.C.A. § 2523; *see also* DOJ White Paper, *supra* note 45.

68 DOJ White Paper, *supra* note 45, at 4.

69 Crime (Overseas Production Orders) Act 2019, c.5 [hereinafter COPO Act] https://www.legislation.gov.uk/ukpga/2019/5/enacted/data.htm [https://perma.cc/Y22Z-524D].

electronic data evidence via the MLAT process has been a source of deep frustration for U.K. law enforcement.[70] In 2019, the U.K. government passed the Crime Overseas Production Orders Act ("COPO Act"). The COPO Act "provided UK law enforcement and prosecution agencies with the power to apply to UK courts for overseas production orders with extra-territorial effect providing there was an international agreement in place between the UK and the other country."[71] The COPO Act requires a CSP to respond to a production order in just seven days unless the issuing judge allows otherwise in particular circumstances.[72] U.K. officials hope that the new agreement will prevent prosecutions from being delayed or abandoned by reducing the previous barriers to obtaining necessary data.[73]

V. The Agreement

A. Process

On October 3, 2019, the U.S. and the U.K. entered into the first bilateral data sharing agreement authorized by the CLOUD and COPO Acts.[74] In contrast with the MLAT request process, under The Agreement, the U.S. and the U.K. can issue orders directly to the CSPs subject to The Agreement.[75] Before the order is sent to a CSP in the other country, the designated authority for the issuing country must review the order to ensure that it complies with The Agreement.[76] In the U.S., the designated authority is any governmental entity designated by the Attorney General.[77] In the U.K., the designated authority is any governmental entity designated by the Secretary of State for the Home Department.[78]

When an issuing party sends an order to a CSP, they must include a point of contact at their designated authority who can

---

70 https://www.legislation.gov.uk/ukpga/2019/5/notes/division/3/index.htm; *see also* Explanatory Memorandum, *supra* note 48, at 1.

71 *Id*. at 6.

72 COPO Act § 5 (5).

73 Explanatory Memorandum, *supra* note 48, at 1.

74 The Agreement, *supra* note 8; U.S. UK DOJ Press Release, *supra* note 6.

75 The Agreement, *supra* note 7, art. 4.

76 *Id*.

77 *Id*. art. 1.

78 *Id*.

"provide information on legal or practical issues relating to the [o]rder."[79] When a CSP receives an order under The Agreement, it can raise objections to the designated authority's contact if it does not believe that The Agreement has been properly invoked.[80] If they cannot work out the objection with the other country's designated authority, the CSP can bring in their home country's designated authority to resolve the objections raised.[81] If the home country's designated authority agrees with the CSP that The Agreement has not been properly invoked, they can notify the issuing country's designated authority that the Agreement does not apply to that specific order.[82] If there is no objection, or after an objection is resolved, information subject to an order is sent directly from the CSP to the designated authority in the issuing country.[83]

The Agreement remains in effect for five years unless it is renewed by both parties prior to its expiration.[84] If The Agreement is terminated or it expires without renewal, the data acquired while it was in effect may still be used by the receiving party with the same restrictions applicable under The Agreement.[85] At the end of each year, both countries must issue a report to one another detailing their respective usage of The Agreement.[86]

B. Restrictions

The Agreement includes a series of negotiated restrictions to address conflicting domestic law, limit the scope of The agreement, and to address privacy concerns. First, The Agreement limits the requests "relating to the prevention, detection, investigation, or prosecution of Serious Crime, ..."[87] A "Serious Crime" is defined as "an offense that is punishable by a maximum term of imprisonment of at least three years."[88]

When the U.K. is the issuing party of an order, it may not request

---

79 *Id*. art. 4.

80 *Id*.

81 The Agreement, *supra* note 7, art. 4.

82 *Id*.

83 *Id*. art. 6.

84 *Id*. art. 17.

85 *Id*.

86 The Agreement, *supra* note 7, art. 12.

87 *Id*. art. 2(1).

88 *Id*. art. 1(14).

data on a "U.S. person."[89] This includes U.S. citizens, nationals, permanent residents, unincorporated associations with a substantial number of U.S. citizens, nationals, or permanent residents, and corporations that are incorporated in the U.S, and people located within the U.S.[90] Likewise, the U.S. may not request information on a person located in the UK.[91] The inconsistency in this application is a result of European Union law that prohibits discriminatory treatment of citizens from member states.[92]

In an effort to minimize the "acquisition, retention, and dissemination" of the information acquired from these orders, Article 7 of The Agreement sets out minimalization procedures that the U.K. must abide by in its handling of data acquired via an order.[93] When the designated authority in the U.K. receives information from a U.S. based CSP, they must review the information promptly, store it on a secure system, and "segregate, seal, or delete, and not disseminate" data that they receive that is not relevant to the investigation.[94] The order must identify a "specific person, account, address, or personal device, or any other specific identifier."[95]

Both countries also agreed to a requirement that the central authority of each country will obtain permission from the other if they plan to use data evidence acquired in a case in which their "essential interests" are implicated.[96] For the U.K., this means that their central authority must obtain permission to use data acquired pursuant to The Agreement as evidence in any case that implicates freedom of speech concerns.[97] The U.S. must obtain permission to use data acquired pursuant to The Agreement as evidence in any case where the death penalty is sought.[98]

---

89 *See* Explanatory Memorandum, *supra* note 48, at 12.

90 *See id.; see also* The Agreement, *supra* note 8, art. 1(12).

91 *See* Explanatory Memorandum, *supra* note 48, at 7-8.

92 *Id*.

93 The Agreement, *supra* note 8, art. 7.

94 *Id*. art. 7(3).

95 *Id*. art. 4(5).

96 The Agreement, *supra* note 8, art. 8.

97 *Id*. art. 8; *see also* Letter from Attorney General William Barr, *supra* note 14.

98 The Agreement, *supra* note 8, art. 8; *see also* Letter from William Barr, Attorney Gen., to Priti Patel, Sec'y of State for the Home Dep't of the U.K. (Oct. 3, 2020) [hereinafter "Letter from Barr'].

Additionally, the U.S. agreed to inform the U.K. if it intends to target data or use data acquired pursuant to The Agreement in any proceeding involving keeping a person detained at Guantanamo Bay, attempting to imprison a person at Guantanamo Bay, or for use in a military commission proceeding at Guantanamo Bay.[99]

VI. Civil Liberty and Privacy Concerns

Leading up to the passage of the CLOUD Act, heated public debate ensued around whether the executive agreements authorized in the act would provide proper privacy and civil liberty protections.[100] On one side of the debate, proponents argued that Agreements authorized under the CLOUD Act would protect CSP and internet users' privacy and allow law enforcement agencies to achieve justice.[101] On the other side of the debate, critics argued that CLOUD Act agreements threatened privacy and human rights.[102]

Critics of the CLOUD Act argued that the language detailing what counts as a "qualifying government" is not sufficient, and does not provide binding accountability.[103] Per the CLOUD Act, a "qualifying government" is one that the U.S. Attorney General and the U.S. Secretary of State determine has "adequate substantive and procedural laws on cybercrime and electronic evidence."[104] This can be illustrated either "by being a party to the Convention on Cybercrime, . . . , or through domestic laws that are consistent with" the convention.[105] Other prerequisites include, but are not limited to:

(I) "demonstrates respect for the rule of law and principles of

---

99 *See* Letter from Barr, *supra* note 98.

100 *See ACLU CLOUD Act Coalition Letter*, Mar. 12, 2018, https://www.aclu.org/sites/default/files/field_document/cloud_act_coalition_letter_3-8_clean.pdf [https://perma.cc/K72W-VNE2] [hereinafter ACLU Letter]*; see also Tech Companies Letter of Support for Senate CLOUD Act*, Feb. 6, 2018, https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf [https://perma.cc/G6XG-TL5L] [hereinafter Tech Companies Letter].

101 *See* Tech Companies Letter, *supra* note 100.

102 *See* ACLU Letter, *supra* note 100.

103 *See* Robyn Greene, *Skydiving Without a Parachute*, NEW AM.'S OPEN TECH. INST. 6-7 (Feb. 22, 2018), https://na-production.s3.amazonaws.com/documents/Cloud_Act.pdf [https://perma.cc/GA46-JTUG].

104 18 U.S.C. § 2523(b)(i) (2018).

105 *Id*.

nondiscrimination;

(II) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including—

a. protection from arbitrary and unlawful interference with privacy;

b. fair trial rights;

c. freedom of expression, association, and peaceful assembly;

d. prohibitions on arbitrary arrest and detention; and

e. prohibitions against torture and cruel, inhuman, or degrading treatment or punishment;"[106]

Additional commitments to transparency, privacy, and the use of data are also included in the CLOUD Act.[107]

Critics pointed out that the language of the CLOUD Act notably describes these prerequisites as "factors to be met" when the U.S. Attorney General and the Secretary of State are considering the qualifications of a foreign government.[108] They argue that this gives the executive branch far too much discretion, and presents the risk of an administration entering a CLOUD Act agreement with a country that does not have appropriate laws around privacy, or worse, a government that would abuse this system to target political dissidents.[109] However, any executive agreement certified by the Attorney General and the Secretary of State is subject to a 180-day period in which Congress can enact a joint resolution of disapproval.[110]

Critics of the CLOUD Act agreements also cite the MLAT process as providing appropriate measures to protect against this risk because of the vetting involved on the U.S. side before access to data is obtained.[111] However, the DOJ stated that the CLOUD Act "simply clarified existing U.S. law" and "did not change the

---

106 18 U.S.C. § 2523(b)(1)(B)(ii-iii) (2018).

107 *See* 18 U.S.C. § 2523(d) (stating that the Attorney General must notify Congress of executive agreements they make under subsection (b)); *see also* 18 U.S.C. § 2523(b)(2) (discussing "procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement").

108 18 U.S.C. § 2523(b)(1)(B).

109 ACLU Letter, *supra* note 100 at 2.

110 18 U.S.C. § 2523(d)(2), (4) (2018).

111 *See* ACLU Letter, *supra* note 100 at 1-2.

existing high standards under U.S. law that must be met before law enforcement agencies can require disclosure of electronic data."[112] Importantly, the CLOUD Act does not allow any agreement to require CSPs to decrypt encrypted data.[113]

VII. Conclusion

While the potential for abuse and the risk of privacy infringements exists with the new CLOUD Act Agreements, those risks are not outweighed by the necessity for a cross-border data sharing system that closer aligns with the pace of the digital world we live in today. The MLAT system is outdated and presents a plethora of risks and abuses. Furthermore, the MLAT system has become so slow and dysfunctional that it handicaps criminal investigations and harms international relations. The US-UK Agreement will provide a test case for both countries' governments as well as the CSPs that are subject to the production orders. As the orders authorized in The Agreement are utilized more, weaknesses will be exposed, and future Agreements can be negotiated to address the issues that arise.

112 DOJ White Paper, *supra* note 45, at 3.

113 18 U.S.C. § 2523(b)(3) (2018).