CONTEMPORARY PRACTICE OF THE UNITED STATES RELATING TO INTERNATIONAL LAW

EDITED BY JEAN GALBRAITH*

In this section:

* Karlos Bledsoe, Emily Friedman, Emily Kyle, Beatrix Lu, Rebecca Wallace, and Howard Weiss contributed to the preparation of this section.

https://doi.org/10.1017/ajil.2019.80 Published online by Cambridge University Press

General International and U.S. Foreign Relations Law

United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data

doi:10.1017/ajil.2019.80

On October 3, 2019, the United States and the United Kingdom reached a bilateral agreement to facilitate more efficient data access between the two countries for law enforcement purposes. The Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime (U.S.-UK Data Access Agreement) was signed by U.S. Attorney General William Barr and UK Home Secretary Priti Patel.[1] This is the first such agreement made by the United States after the passage of the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act, which authorizes and structures future bilateral agreements on data sharing. Pursuant to the CLOUD Act, Congress has 180 days following receipt of a notification regarding the U.S.-UK Data Access Agreement to block its entry into force via a joint resolution, which would require a majority vote in both houses of Congress and either presidential signature or a subsequent congressional override of a presidential veto.

Cross-border data requests for law enforcement purposes have traditionally depended on mutual legal assistance treaties (MLATs). Obtaining data through the processes established in MLATs can take many months.[2] In 2018, Congress passed the CLOUD Act which, among other things, creates "a framework that allows U.S. service providers to disclose U.S.-stored data to certain foreign countries pursuant to lawful foreign orders."[3] Under this framework, the United States may enter into bilateral agreements with "rights-respecting countries that abide by the rule of law" whom the attorney general has determined meet certain specified statutory criteria.[4] Once such a bilateral agreement is in force, it has the effect of "lift[ing] any restrictions under U.S. law on companies disclosing electronic data directly to foreign authorities for covered orders in investigations of serious crimes"—an effect that "would permit U.S.-based global [communications service providers] to respond directly to foreign legal process in many circumstances."[5] Similarly, the bilateral agreements contemplated by the CLOUD Act can lift

[1] 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 (Oct. 3, 2019), *available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf [https://perma.cc/G9EZ-GSUR] [hereinafter U.S.-UK Data Access Agreement].

[2] *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, 708 (2017) (noting that on average, successful requests for data made pursuant to MLATs take ten months once requests are made).

[3] Jean Galbraith, Contemporary Practice of the United States, 112 AJIL 487, 487 (2018). The CLOUD Act also amended a federal statute to make clear that U.S. law enforcement could use warrants to obtain electronic data stored overseas by U.S. companies—an amendment that rendered moot a pending Supreme Court case on the issue. *See id.* at 488–89.

[4] U.S. Dep't of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act 4, 6, 10 (Apr. 2019), *available at* https://www.justice.gov/opa/press-release/file/1153446/download?utm_medium=email&utm_source=govdelivery [https://perma.cc/PK9F-84A5] [hereinafter DOJ White Paper on CLOUD Act]; *see also* Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523(b) (2018), *available at* https://www.justice.gov/dag/page/file/1152896/download [hereinafter CLOUD Act].

[5] DOJ White Paper on CLOUD Act, *supra* note 4, at 4.

restrictions under the law of the partner nation that might otherwise complicate the ability of U.S. law enforcement to gain access to data.[6] The CLOUD framework thus provides an additional, more efficient path to data sharing without eliminating prior protocols such as MLATs.[7] Both the CLOUD Act and the U.S.-UK Data Access Agreement had the strong support of UK law enforcement officials.[8]

As the first international agreement made by the United States pursuant to the CLOUD Act, the text of the U.S.-UK Data Access Agreement may become a model for similar agreements in the future. Article 1 provides definitions, including one on the threshold issue of what constitutes a "serious crime"—a term that was left undefined in the CLOUD Act.[9] The purpose of the U.S.-UK Data Access Agreement, given in Article 2, is:

> [T]o advance public safety and security, and to protect privacy, civil liberties, and an open Internet, by resolving potential conflicts of legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party.[10]

Article 3 sets forth the core requirement that neither country's domestic laws shall prevent one of its companies from responding to appropriate data requests from the other country.[11] Article 4 specifies who are appropriate underlying targets of data requests, making clear that the United Kingdom cannot intentionally target U.S. citizens, legal permanent residents, or persons on U.S. territory, and conversely that the United States cannot intentionally target persons on UK territory.[12] Articles 5 through 10 provide further substantive and procedural

[6] *See id.* at 4–5 (noting, however, that "the United States currently receives many more requests for electronic data than it submits to other countries," presumably because many communications service providers are based in the United States).

[7] STEPHEN P. MULLIGAN, CONG. RESEARCH SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 23 (Apr. 23, 2018), *available at* https://fas.org/sgp/crs/misc/R45173.pdf [https://perma.cc/X49C-FJHE](observing that "[e]xecutive agreements authorized by the CLOUD Act would supplement, not replace, existing avenues of international data sharing" and "[a]ccordingly, requests for assistance would still be available through MLATs (when in effect)").

[8] *See* Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary, 115th Cong. (2017); UK Government Press Release, UK and US Sign Landmark Data Access Agreement (Oct. 4, 2019), *at* https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement [https://perma.cc/2458-WB4C]. The press release issued by the government of the United Kingdom following the signature of the U.S.-UK Data Access Agreement noted that: "The UK has obtained assurances which are in line with the government's continued opposition to the death penalty in all cases." *Id.*; *see also* U.S.-UK Data Access Agreement, *supra* note 1, Art. 8(4) (setting up special requirements where the United States is seeking data access for purposes of a death penalty case and where the United Kingdom is seeking access for purposes of a case that "raises freedom of speech concerns for the United States").

[9] U.S.-UK Data Access Agreement, *supra* note 1, Art. 1(5), 1(14) (establishing that "Covered Offense means conduct that, under the law of the Issuing Party, constitutes a Serious Crime, including terrorist activity" and "Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years"); CLOUD Act, 18 U.S.C. § 2523(a) (failing to define "serious crimes" in the definitions section).

[10] U.S.-UK Data Access Agreement, *supra* note 1, Art. 2.

[11] *Id.* Art. 3.

[12] *Id.* Art. 4; *see also* UK 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, Cm. 178, at 14 (2018), *at* https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-

https://doi.org/10.1017/ajil.2019.80 Published online by Cambridge University Press

rules for data requests, including ones intended to advance privacy interests.[13] As one notable example, Article 5 provides that "[o]rders subject to this Agreement shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the Order."[14] Article 11 stresses "[c]ompatibility and [n]on-exclusivity" with respect to existing MLATs.[15] Articles 12 through 16 describe implementation procedures, including with respect to entry into force, responsibility for costs, and the process for amendments.[16] Finally, Article 17 sets forth an initial five-year term for the agreement, subject to mutually agreed-upon renewal, and separately provides that either party may terminate at any time on one month's notice.[17]

For the U.S.-UK Data Access Agreement to enter into force, the parties must exchange diplomatic notes to that effect.[18] For the United States, this process will take at least 180 days from when Congress receives official notification of the signed agreement and also receives a certification by the attorney general that the UK is an appropriate bilateral partner for purposes of agreements made pursuant to the CLOUD Act.[19] The CLOUD Act further sets forth streamlined procedures for consideration of such executive agreements by the House of Representatives and the Senate, including provisions ensuring that appropriately introduced joint resolutions of disapproval will receive up-or-down votes following committee review.[20] Some privacy advocates have urged the pursuit of such a joint resolution, arguing among other things that the U.S.-UK Data Access Agreement has too low a standard for

of-countering-serious-crime-cs-usa-no62019 [https://perma.cc/XE4S-4W5A] (indicating the restriction on intentional targeting by the United States was limited to those on the UK's territory rather than also including UK citizens because of "EU law which prohibits discrimination in treatment between citizens of different member states.").

[13] U.S.-UK Data Access Agreement, *supra* note 1, Arts. 5–10.

[14] *Id.* Art. 5(2). Earlier in 2019, the United Kingdom passed an act setting forth a domestic process by which such court orders could be obtained. *See* UK Government Press Release, Crime (Overseas Production Orders) Bill Receives Royal Assent (Feb. 12, 2019), *at* https://www.gov.uk/government/news/crime-overseas-production-orders-bill-receives-royal-assent [https://perma.cc/6H7B-QUJ5]. The U.S.-UK Data Access Agreement also provides that the issuing nations may neither issue requests on behalf of third-party nations nor share data with third-party nations, U.S.-UK Data Access Agreement, *supra* note 1, Arts. 5(4), 8(2); that a provider receiving service of process has the right to challenge an order "when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order," *id.* Art. 5(11–12); and that there should be "minimization procedures" whereby the UK will "minimize the acquisition, retention, and dissemination of information concerning U.S. Persons acquired pursuant to an Order," *id*. Art. 7.

[15] *Id*. Art. 11.

[16] *Id*. Arts. 12–16.

[17] *Id*. Art. 17; *see also* CLOUD Act, 18 U.S.C. § 2523(e)(1) (providing that the attorney general must renew on five-year bases the determination that the other country is an appropriate partner for purposes of executive agreements made pursuant to the CLOUD Act).

[18] U.S.-UK Data Access Agreement, *supra* note 1, Art. 16. It is unclear whether Brexit, should it occur, would impact the timeline. Following Brexit, the UK might need to undergo an "adequacy determination" by EU officials to determine the adequacy of UK data privacy and security before data is permitted to be moved between the UK and EU member states. Kurt Wimmer & Joseph Jones, *Brexit and Implications for Privacy*, 40 FORDHAM INT'L L.J. 1553, 1558–59 (2017). It is unclear the extent to which, should such an adequacy determination need to occur, an agreement like the U.S.-UK Data Access Agreement might be relevant to that determination.

[19] CLOUD Act, 18 U.S.C. § 2523(d)(2).

[20] *Id.*, § 2523(d)(5)–(6); *see also id.*, § 2523(d)(4) (providing that such a resolution can be introduced in either house by the majority or minority leader or, in the Senate, by the designee of one of these leaders).

https://doi.org/10.1017/ajil.2019.80 Published online by Cambridge University Press

triggering data gathering, including wiretaps, and does not clearly specify that judicial oversight must occur prior to data collection.[21]

Overall, the CLOUD Act set the stage for a shift away from the traditional MLATs, and the U.S.-UK Data Access Agreement begins the implementation of this shift. As the first bilateral CLOUD Act agreement, it may serve as a model for future such agreements. The U.S. attorney general and Australian minister for home affairs announced on October 7, 2019, that the two nations are formally negotiating an agreement under the CLOUD Act.[22] Additionally, in June of 2019, the Council of the European Union formally authorized the European Commission to "open negotiations for an agreement between the Union and the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider."[23]

United States Remains in the Universal Postal Union, Rescinding Its Notice of Withdrawal

doi:10.1017/ajil.2019.84

On September 25, 2019, the Third Extraordinary Congress of the Universal Postal Union (UPU) adopted a proposal on terminal dues rates—a decision that led the United States to remain a member state. The United States had given its one-year notice of withdrawal from the UPU eleven months earlier, citing concerns that the existing system unfairly advantaged

[21] Coalition letter from EPIC et. al. to U.S. Members of Congress (Oct. 29, 2019), *available at* https://www.whistleblower.org/sign-on-letter/sign-on-coalition-statement-re-u-s-u-k-cloud-act-executive-agreement [https://perma.cc/9Y67-P3XT] (observing that "the text of the U.S.-U.K. Agreement requires that orders for content, widely considered the most sensitive electronic data, only meet the standard of 'reasonable justification based on articulable and credible facts, particularly, legality, and severity'" and stating that this "standard is vague . . . and likely is weaker than probable cause in various contexts"). By contrast, Jennifer Daskal and Peter Swire describe the U.S.-UK Data Access Agreement and the underlying CLOUD Act as "positive developments that protect privacy and civil liberties, accommodate divergent norms across borders, and respond to the reality that digital evidence critical even to wholly local crimes is often located across international borders." Jennifer Daskal & Peter Swire, *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, JUST SECURITY (Oct. 8, 2019), *at* https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards.

[22] U.S. Dep't of Justice Press Release, Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019), *at* https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us [https://perma.cc/MH2H-ZVEX].

[23] Council of the European Union, Council Decision Authorising the Opening of Negotiations with a View to Concluding 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, COPEN 268 USA 45, 10128/19 (June 12, 2019), *available at* https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf [https://perma.cc/2XJF-KUZC]; *cf.* European Data Protection Supervisor, Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence (July 10, 2019), *available at* https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf [https://perma.cc/2FY7-YWYB] (assessing some legal issues related to the CLOUD Act and its interaction with the EU's General Data Protection Regulation).